ISACA.CISA-KR.v2026-05-16.q709

□□□□:	CISA-KR
□□□□:	Certified Information Systems Auditor (CISA Korean Version)
□□□:	ISACA
□□ □□ □□□:	709
□□:	v2026-05-16
# □□ □:	112
# □□ □□□:	7090
https://www.krdump.com/ISACA.CISA-KR.v2026-05-16.q709.html	

NEW QUESTION: 1
□□ □□(CSA)□ □□□ □□ □□□ □□□ □ □□□□.
A. □□□ □□□ □□□□□.
B. □□□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Control self-assessment (CSA) is a process that allows business units to evaluate the effectiveness of internal controls. It is primarily used to establish baselines (Option B) for measuring control effectiveness and risk management.
ISACA CISA Reference: CSA is a recognized internal control mechanism that supports risk assessment and control improvement.
Risk Implication: If CSAs are not conducted properly, organizations may lack visibility into weak controls, increasing exposure to risks.
Alternative Choices:
Option A: CSA does not focus on asset valuation.
Option C: Strategic business goals are assessed separately through governance processes.
Option D: CSA complements, but does not replace, formal audits.

NEW QUESTION: 2
□□□□□ □□ □□□ □□□ □□ □□(ERP) □□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□. □□ □□(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: 3

□□ □ □□ □□□ □□□□ □□ □□□□ □□□(RPA) □□□ □□□ □ □□ □□ □ □ □ □□ □□□□□?

A. □□□ □□□ □□ □□□ □□□□□.

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

C. □□ □□□ □□□□□ □□□□□.

D. □□□ □□□□ □□□□ □□□□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 4

□□□ □□ □□ □□□ □□□□ □□ □□ □□□(IS) □□□ □□□□□□□, □□ □□ □ □□□ □□ □□□ □□□ □□□.

A. □□ □□ □□(DRP) □□ □□□ □□□□□.

B. □□□□ □□□ □□ □□ □□ □□

C. □□ □□ □□□ □3□□□ □□

D. □□ □□ □□□ □□ □□ □□□ □□

Answer: (SHOW ANSWER)

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: 5
□□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□ □□□ □□□□□.
B. □□ □□□□ □□□□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□ □□□□ □□□□□.
D. □□□□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 7
□□ □ POS(□□ □□ □□) □□□□ □□□□□ □□ □□□□□□ □□ □□□□ □□ □□ □□□□ □□□□ □□□ IS □□□□□ □□□□ □□ □□□□□?
A. □□ □□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□ □□□ □□ □□ □□□□□.
C. □□ □□ □□□ □□□ □□□ □□□□□□□.
D. POS □□□□□□ □□ □□□□ □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The best option to provide an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately is A. Electronic copies of customer sales receipts are maintained. Electronic copies of customer sales receipts are records of the transactions that occurred at the POS system, which can be compared with the data transferred to the general ledger. This can help detect any errors, omissions, or discrepancies in the data transfer process and ensure that the sales data is complete and accurate.
The other options are not as effective as A in providing assurance that the interface between the POS system and the general ledger is transferring sales data completely and accurately. B. Monthly bank statements are reconciled without exception. Monthly bank

statements are records of the cash inflows and outflows of the organization, which may not match with the sales data recorded by the POS system and the general ledger.
For example, there may be delays, discounts, returns, or refundsthat affect the cash flow but not the sales revenue. Therefore, reconciling monthly bank statements without exception does not necessarily mean that the sales data is complete and accurate. C. Nightly batch processing has been replaced with real-time processing. Nightly batch processing is a method of transferring data from the POS system to the general ledger in batches at a scheduled time, usually at night. Real-time processing is a method of transferring data from the POS system to the general ledger as soon as the transactions occur. Real-time processing may improve the timeliness and efficiency of the data transfer process, but it does not guarantee that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected. D. The data transferred over the POS interface is encrypted. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality and security of the data transferred over the POS interface, but it does not ensure that the sales data is complete and accurate.
There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2 Sales Audit Overview - Oracle3 Notes on Audit of Ledgers - Guidelines to Auditors - Accountlearning

NEW QUESTION: 8
□□ □ IS □□□□ □□ □□ □□□□ □□□ □□□□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□
B. □□□ □□□ □□
C. □□ □□ □□
D. □□ □□□ □□□□
Answer: C (LEAVE A REPLY)
Operating system parameters are settings or values that affect the behavior or performance of the operating system1. Modifications to the operating system parameters may be necessary to improve the system functionality, security, or efficiency. However, such modifications may also introduce risks or errors that can affect the system stability, compatibility, or integrity. Therefore, modifications to the operating system parameters should be authorized and documented by the appropriate authority2.
A change control log is a record of all changes made to the system, including the date, time, description, reason, authorization, and impact of each change3. A change control log

can help the IS auditor to verify whether modifications to the operating system parameters were authorized by comparing the log entries with the actual system settings and the change approval documents4.

NEW QUESTION: 9
□□ □□□□□ □□□ □□ □□□ □□□□ □□ □□□□□□□ □□□□□. □□ □ □□□□□□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□□□□ □□ □□□ □□ □□ □□□□□ □□□□.
B. □□□□□□□ □□ □□□ □□□□□ □□□□□.
C. □□□ □□ □□□ □□□□ □□ □□□□□□□ □□ □□□□.
D. □□□□□□ □□ □□□ □□ □□□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
Access to the spreadsheet is given only to those who require access is the most important control for maintaining the security of data in the spreadsheet. An IS auditor should ensure that the principle of least privilege is applied to limit the access to sensitive financial data and prevent unauthorized disclosure, modification, or deletion. The other options are less important controls that may enhance the accuracy, availability, or integrity of data in the spreadsheet, but not its security. References:
CISA Review Manual (Digital Version), Chapter 6, Section 6.31
CISA Review Questions, Answers and Explanations Database, Question ID 210

NEW QUESTION: 10
□□ □□□(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 settingsor 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: 11
□□ □ IT □□□□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□ □□□
B. □□ □□(QA) □□□
C. □□□□ □□□
D. □□ □□ □□ □□□(CRO)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
□□ □ □□□□ □□□ □□□ □□□□ □□ □□(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: 13
□□ □ □□□ □□ □□□□ □□ □□□ □□□ □□□□□?
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: 14

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

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

B. □□ □□ □□□□ □□□□□ □□□□□□ □□□□□□.

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

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

Answer: (SHOW ANSWER)

The IS auditor's best recommendation is to ensure that programmers cannot access code after the completion of program edits. This is because programmers who have access to code after editing may introduce unauthorized or malicious changes that could compromise the security, functionality, or performance of the application. By restricting access to code after editing, the organization can ensure that only authorized and tested code is released into production, and prevent any tampering or reoccurrence of the same issue.

References:

1 discusses the importance of controlling access to code after editing and testing, and provides some best practices for doing so.

2 explains how programmers can introduce malicious code into applications, and how to prevent and detect such attacks.

3 describes the role of IS auditors in reviewing and assessing the security and quality of application code.

NEW QUESTION: 15

□□ □ □□ □□□ □□ □□□ □ □□ □□ □□□ □□□□□?

A. □□

B. □□□ □□

C. □□ □□□

D. □□

Answer: C (LEAVE A REPLY)

The best answer is C. Re-performance of controls.

Under ISACA audit principles, evidence obtained directly by the auditor is generally more reliable than evidence provided by management or gathered indirectly. Re-performance allows the auditor to independently execute the control or procedure and verify whether it works as intended, making it stronger than inquiry, observation, or management attestation.

Option A is the least reliable because inquiry depends on what people say. Option B is stronger than simple inquiry but still relies on management representation. Option D can be useful, but observation only shows what happened at a point in time and may not prove consistent operation. Re-performance gives the auditor the highest level of assurance because the evidence is generated through the auditor's own independent work.

References (Official ISACA):
* ISACA, Follow-Up Audits and Follow-Up Process: The Auditor's Impact Litmus Tool
* ISACA, The Top-Five Audit Essentials for Driving Efficiency and Value

NEW QUESTION: 16
□□□ □□□ □□ □□□ □□□□□ □□□ □ □□ □□□ □□□□ □□ □ □□□ □ □□□ □□□?
A. □□ □□□ □□□ □□ □□ □□
B. □□ □□ □□□□ □ □□□□ □□□□ □□
C. □□ □□□□ □□□□ □□ □□
D. □□□ □□ □□□ □□ □□ □□□ □□
Answer: A (LEAVE A REPLY)
Information systems governance is the set of policies, processes, structures, and practices that ensure the alignment of IT with business objectives, the delivery of value from IT investments, the management of IT risks, and the optimization of IT resources1.
Information systems governance is a strategic and high-level function that covers the entire organization and its IT portfolio. Therefore, an IS auditor should review the aspects of information systems governance that are relevant to the organization's vision, mission, goals, and strategies.
One of the aspects that an IS auditor should review when evaluating information systems governance for a large organization is the approval processes for new system implementations. This is because new system implementations are significant IT investments that require careful planning, analysis, design,development, testing, deployment, and evaluation to ensure that they meet the business requirements, deliver the expected benefits, comply with the relevant standards and regulations, and minimize the potential risks2. The approval processes fornew system implementations should involve the appropriate stakeholders, such as senior management, business owners, IT managers,project managers, users, and auditors, who have the authority and responsibility to approve or reject the proposed system implementations based on predefined criteria and metrics3. The approval processes for new system implementations should also be documented, transparent, consisten t, and timely to ensure accountability and traceability4.
Therefore, an IS auditor should review the approval processes for new system implementations to assess whether they are aligned with the information systems governance framework and objectives.
The other possible options are:
Procedures for adding a new user to the invoice processing system: This is an operational task that involves granting access rights and permissions to a specific user for a specific system based on the principle of least privilege. This is not a strategic or high-level function that falls under information systems governance.
Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization.

Approval processes for updating the corporate website: This is a tactical task that involves making changes or enhancements to the content or design of the corporate website based on the business needs and feedback.
This is not a strategic or high-level function that falls under information systems governance. Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization.
Procedures for regression testing system changes: This is a technical task that involves verifying that existing system functionalities are not adversely affected by new system changes or updates. This is not a strategic or high-level function that falls under information systems governance. Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization. References: 1: What is IT Governance? - Definition from Techopedia 2: System Implementation - an overview | ScienceDirect Topics 3: Project Approval Process - Project Management Knowledge 4: 5 Best Practices For A Successful Project Approval Process | Kissflow Project : Principle of Least Privilege (POLP) | Imperva :
How to Update Your Website Content - 7 Step Guide | HostGator Blog : What Is Regression Testing?
Definition and Best Practices | BrowserStack

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

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

NEW QUESTION: 18
□□ □□□ □□ □□□ □□□ □□□□.
A. □□□ □□ □□□ □□□□□ □□□ □□□□□□.
B. □□ □□□ □□□ □□ □□ □□□ □□□□□□.
C. □□□□ □□□□□ □□□□ □ □□□ IT □□□□ □□□□□.

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

NEW QUESTION: 19
□□ □ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □ □□□□?
A. □□□ □□ □□(DLP) □□□□□□ □□□□□.
B. □□ □□□ □□□ □□□□□
C. □□□□ □□ □□ □□ □□□ □□□□□.
D. □□ □□ □□□□ □□
Answer: D (LEAVE A REPLY)
The most effective way to identify exfiltration of sensitive data by a malicious insider is to establish behavioral analytics monitoring. Behavioral analytics is the process of analyzing the patterns and anomalies in user behavior to detect and prevent insider threats. Behavioral analytics can help identify unusual or suspicious activities, such as accessing sensitive data at odd hours, transferring large amounts of data to external devices or locations, or using unauthorized applications or protocols. Behavioral analytics can also help correlate data from multiple sources, such as network logs, user profiles, and access rights, to provide a holistic view of user activity and risk.
Data loss prevention (DLP) software is a tool that can help prevent exfiltration of sensitive data by a malicious insider, but it is not the most effective way to identify it. DLP software can block or alert on unauthorized data transfers based on predefined rules and policies, but it may not be able to detect sophisticated or stealthy exfiltration techniques, such as encryption, steganography, or data obfuscation.
Reviewing perimeter firewall logs is a way to identify exfiltration of sensitive data by a malicious insider, but it is not the most effective way. Perimeter firewall logs can show the traffic volume and destination of data transfers, but they may not be able to show the content or context of the data. Perimeter firewall logs may also be overwhelmed by the amount of normal traffic and miss the signals of malicious exfiltration.
Providing ongoing information security awareness training is a way to reduce the risk of exfiltration of sensitive data by a malicious insider, but it is not a way to identify it. Information security awareness training can help educate users on the importance of protecting sensitive data and the consequences of violating policies and regulations, but it may not deter or detect those who are intentionally or maliciously exfiltrating data.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 300
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription 1 Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog 2 How to Secure Your Company'sLegacy Applications - iCorps

NEW QUESTION: 20

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

A. □□ □ □□□ □□□□□ □□□□ □□

B. □□□□ □□□ □□□□ □□□□ □□

C. □□□ □□ □□□ □□□□□ □□ □□

D. □□□ □□□□□ □□□□ □□□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 21

□□ □□ □□ □□□ □ □□ □□□ □□□ □□ □□□□□.

A. □□□ □□ □□□ □□□ □□□□□.

B. □□□ □□□□ □□□ □ □□□□ □□ □□□ □ □□□□.

C. □□□ □□ □□□ □□□□ □□□ □□□□□.

D. □□ □□□□□ □□□ □□□ □□□ □□□□ □□□□.

Answer: D (LEAVE A REPLY)

Monetary unit sampling (MUS) is a statistical sampling method that is used to determine if the account balances or monetary amounts in a population contain any misstatements. MUS treats each individual dollar in the population as a separate sampling unit, so that larger balances or amounts have a higher probability of being selected than smaller ones. MUS then projects the results of testing the sample to the entire population in terms of dollar values, rather than error rates.

One advantage of MUS is that it increases the likelihood of selecting material items from the population.

Material items are those that have a significant impact on the financial statements and could influence the decisions of users. By giving more weight to larger items, MUS ensures that material misstatements are more likely to be detected and reported. MUS also reduces the sample size required to achieve a desired level of confidence and precision, as compared to other sampling methods that do not consider the value of items.

References:

4: Monetary unit sampling definition - AccountingTools

5: How Does Monetary Unit Sampling Work? - dummies

6: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 22

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

A. □□ □□□□□□□ □□ □□ □□□□□ □□□□

B. □□ □□□ □□□□ □□□□□□ □□

C. □□□□ □□□ □□□□□□ □□

D. □ □□□□□□□ □□ □□□□

NEW QUESTION: 23
□□ □□□ □□ □□□□ □□ □□□□□□□ □□□ □□□ □□ □□□ □□□□□ □ □□□ □□□□ □□□□. □□ □ □ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□□□ □□ □□
B. □□ □□□ □□ □□□ □□ □□□□□□□ □ □□□□.
C. □□□□ □□ □□
D. □□□ □□□ □□□ □□□□□□ □□ □ □□
Answer: B (LEAVE A REPLY)
Consolidating multiple applications on asingle serverincreases the risk that aserver outagewillimpact multiple applicationssimultaneously.
More Applications Affected by Outage (Correct Answer - B)
Asingle point of failurecoulddisrupt multiple services.
Example:If aconsolidated server crashes, all hosted applications gooffline.
Higher OS License Fees (Incorrect - A)
License feesmay increase, butdowntime risk is a greater concern.
Simplified Asset Management (Incorrect - C)
True, butdoes not outweigh the availability risk.
Fewer Vulnerability Scans (Incorrect - D)
Reducing the number of serversdoes not reduce security risks.
References:
ISACA CISA Review Manual
NIST 800-160 (System Security Engineering)

NEW QUESTION: 24
□□□□□ □□ □□□□□ □□□□ □□ □□ □ □□ □□□ □□ □□□ □□ □□□ □□ □□□ □ □□□□?
A. □ □□□□ □□□□ □□□ □□
B. □□ □□□ □□□□ □□□ □□ □ □□ □□□
C. □□ □□□□□□ □□ □□ □□
D. □□ □□□ □□□ □ □□
Answer: C (LEAVE A REPLY)
Access controls for source libraries are the features of a library control software package that would protect against unauthorized updating of source code. Access controls are the mechanisms that regulate who can access, modify, or delete the source code stored in the source libraries. Source libraries are the repositories that contain the source code files and their versions. By implementing access controls for source libraries, the library controlsoftware package can prevent unauthorized or malicious users from tampering with the source code and compromising its integrity, security, or functionality1.
The other options are not as effective as access controls for source libraries in protecting against unauthorized updating of source code. Option A, required approvals at each life

cycle step, is a good practice but may not be sufficient to prevent unauthorized updates if the approval process is bypassed or compromised. Option B, date and time stamping of source and object code, is a useful feature but may not prevent unauthorized updates if the date and time stamps are altered or ignored. Option D, release-to-release comparison of source code, is a helpful feature but may not prevent unauthorized updates if the comparison results are not reviewed or acted upon.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription How to protect your source code from attackers2 How to Stop Unauthorized Use of Open Source Code

NEW QUESTION: 25
□□□ □□ □□□ □□□ □□ □□□□ □□□ □□□ □ □□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□ □□ □□
B. □□ □□
C. □□ □□ □ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
The best answer is C. Local laws and regulations.
ISACA privacy guidance consistently frames data protection policy around compliance with privacy laws, rules, and regulations. ISACA specifically notes that privacy strategies and policies should be reviewed and updated regularly to reflect regulatory changes and ensure compliance. Since data protection obligations are often legally mandated and penalties can be significant, legal and regulatory requirements are the most important consideration when determining review frequency.
Option A. Industry best practices can inform good policy design, but they do not override legal requirements.
Option B. Business objectives matter for alignment, but they are not the strongest driver of review frequency in a privacy context.
Option D. Known international standards can be useful references, but local legal obligations are more binding and more important for determining how often the policy must be revisited.
Therefore, C is the correct answer because compliance with local laws and regulations is the most important driver of how frequently a data protection policy should be reviewed.
References (Official ISACA):
* ISACA Journal, What Is Your Privacy and Data Protection Strategy?.
* ISACA, The Evolving World of Data Privacy: Trends and Strategies.
* ISACA Journal, Privacy Risk Management.
* ISACA Journal, Analyzing Privacy Policies as Data.

NEW QUESTION: 26
□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□ □□, □□ □□□ □□□□□ □□□□□□.
□□ □ □□ □□□ □□ □□□□ □□□□ □□□?
A. □□□ □□□□ □ □□ □□□□ □□□□ □□□□□.
B. □□ □□ □□□(IDS)□ □□ □□□ □□□□ □□□□ □□□□□.
C. □□□ □□□□ □□□ □ □□□□□.
D. □□□ □□ □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
ISACA CISA Review Manual 27th Edition (2019), page 254
Incident Response Process - ISACA1
Incident Response: How to Identify and Fix Security Weaknesses

NEW QUESTION: 27
□□ □ □□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□ □□
B. □□ □□ □□□□
C. □□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)
The most effective method of destroying sensitive data stored on electronic media is physical destruction, which involves breaking, shredding, melting, or incinerating the media

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

NEW QUESTION: 28
□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□ □□□ □□□ □ □□□□ □□ □□□ RACI □□□ □□□□ □□□□. □□ □□□ □□ □ □□ □□ □ □ □□□ □□□□□?
A. □□□
B. □□ □□□
C. □□□
D. □□ □□
Answer: (SHOW ANSWER)
The role within the RACI chart that would provide information on who has oversight of staff performing a specific task is accountable. A RACI chart is a matrix that defines and assigns the roles and responsibilities of different stakeholders for a project, process, or activity. RACI stands for responsible, accountable, consulted, and informed. Accountable is the role that has the authority and oversight to approve or reject the work done by the responsible role. The other options are not the roles that provide information on who has oversight of staff performing a specific task, as they have different meanings and functions. Consulted is the role that provides input or advice to the responsible or accountable roles. Informed is the role that receives updates or reports from the responsible or accountable roles. Responsible is the role that performs or executes the work or task. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 29
□□ □ 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: 30
□□ □□□ □□ □□ □□, □□□ □ □□ □□□ □□ □□□□□ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □ □□ □ □ □□□ □□□.
B. □□□□ □□□□ □□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□□ □□□.
D. □□ □□ □□□ □□□ □□□□ □□□□ □ □□□ □□□.
Answer: C (LEAVE A REPLY)
The primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates is that it establishes accountability for the action plans. Accountability means that the individuals or groups who are responsible for implementing the action plans are clearly identified and held liable for their completion within the specified time frame. Accountability also implies that the action plans are monitored and evaluated to ensure that they are effective and efficient in addressing the audit findings and mitigating the associated risks1. Accountability helps to ensure that the audit recommendations are taken seriously and implemented properly, and that the audit value is realized by the organization2. The other options are less relevant or incorrect because:
A). It facilitates easier audit follow-up is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a secondary or indirect benefit. Auditfollow-up is the process of verifying whether the action plans have been implemented and whether they have resolved the audit findings3. While having clear action plans, owners, and target dates may facilitate easier audit follow-up by providing a basis for tracking and reporting the progress and status of the action plans, it does not necessarily guarantee that the action plans will be implemented or effective.
B). It enforces action plan consensus between auditors and auditees is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of a prerequisite or condition for such an approach. Action plan consensus means that the auditors and auditees agree on the audit findings and recommendations, and on the action plans to address them4. While having action plan consensus may enhance the credibility and acceptance of the

audit approach, it does not necessarily ensure that the action plans will be implemented or effective.
D). It helps to ensure factual accuracy of findings is not the primary benefit of an audit approach that requires reported findings to be issued together with related action plans, owners, and target dates, as it is more of an outcome or result of such an approach. Factual accuracy of findings means that theaudit findings are based on sufficient, reliable, relevant, and useful evidence5. While having factual accuracy of findings may increase the confidence and trust in the audit approach, it does not necessarily ensure that the action plans will be implemented or effective. References: Accountability - ISACA, Audit Value - ISACA, Audit Follow-up - ISACA, Action Plan Consensus - ISACA, Factual Accuracy of Findings - ISACA

NEW QUESTION: 31
□□ □□□ □□□□ □□□□□ □□□□□□ □, □□□□ □□□□ □□□ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□ □□□ □□□□ □ □□□
B. □□□□ □□ □□
C. □□□ □□
D. □□ □ □□ □□
Answer: A (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 32
□□□ □□ □□□□□ □□□□ □□□□ □□□ □□ □□□ □□ □□□ □□□□□?
A. □□
B. □□□
C. □□□
D. □□
Answer: (SHOW ANSWER)
Secure code reviews as part of a continuous deployment program are preventive controls. Preventive controls are controls that aim to prevent or avoid undesirable events or outcomes from occurring, such as errors, defects, or incidents. Secure code reviews are activities that examine and evaluate the source code of a software or application to identify and eliminate any vulnerabilities, flaws, or weaknesses that may compromise its security,

functionality, or performance. Secure code reviews as part of a continuous deployment program can help prevent or avoid security issues or incidents from occurring by ensuring that the code is secure and compliant before it is deployed to production. The other options are not correct types of controls for secure code reviews as part of a continuous deployment program, as they have different meanings and functions. Detective controls are controls that aim to detect or discover undesirable events or outcomes that have occurred, such as errors, defects, or incidents. Logical controls are controls that use software or hardware mechanisms to regulate or restrict access to IT resources, such as data, systems, or networks.
Corrective controls are controls that aim to correct or rectify undesirable events or outcomes that have occurred, such as errors, defects, or incidents. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 33
□□ □ □□□ 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: 34
□□ □ □□□ □□□□ □□□ □□ IT □□□□ □□□□□ □ □□ □□□ □□ □□ □ □□□□?
A. □□ □□
B. □□□ □□□□
C. □□□□□□ □□□□(EA)
D. □□ □□□□ □□□(RPA)
Answer: (SHOW ANSWER)

NEW QUESTION: 35
□□□ □□□ □, 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: 36
□□□ □□ □□□□□ □□□ □□□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□ □□
B. □□□ □□ □□ □□□ □□□□ □□
C. □□□ □□□ □□□ □□□□ □□
D. □□ □□ □□□ □□□ □□
Answer: B (LEAVE A REPLY)
The primary reason for an organization to classify the data stored on its internal networks is to implement data protection requirements1234. Data classification helps organizations understand what data they have, its characteristics, and what security and privacy requirements it needs to meet so that the necessary protections can be achieved3. While determining data retention policy56, complying with the organization's data policies27, and following industry best practices891011 are important aspects of data classification, they are secondary to the fundamental requirement of implementing data protection requirements.
References:
What Is Data Classification and Why Is It Important? - RiskOptics
Data Classification Policy: Definition, Examples, and Free Template - Hyperproof Data Classification Policy: Benefits, Examples, and Techniques - Satori What is a Data Classification Policy? - Digital Guardian Data Classification and Practices - NIST Data Classification as a Catalyst for Data Retention and Archiving ...
What is data classification? - Cloud Adoption Framework
Data Classification - Data Security Policies | ITS Policies ...

IMPLEMENTING DATA CLASSIFICATION PRACTICES - NIST
Best Practices for Data Classification | Forcepoint

NEW QUESTION: 37
□□ □ □□□□ □□ □□ □□□□ □□□□ □□□ □ □□□ □□ □ □□□ □□□□ □□ □□□□□?
A. □□□ □□□ □□□□(XSS)
B. □□□ □□
C. □□ □□
D. □□□ □□ □□□□ □□□
Answer: (SHOW ANSWER)
Social engineering is the manipulation of people to perform actions or divulge confidential information. It is a common technique used by attackers to gain unauthorized access to systems or data. Employees who use public social networking sites may be vulnerable to social engineering attacks, such as phishing, baiting, or pretexting, which pose the greatest risk to the organization's security. The other options are not as serious as social engineering, as they relate to web application vulnerabilities, intellectual property rights, and reputation management, which are less likely to compromise the organization's assets or operations. References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.3 Security Awareness Training1

NEW QUESTION: 38
□□ □□□ □□ □□□□ □□ □□□ □□ □□□□ □□ AI □□□ □□□□ □□□ □ □□□□□. □□ □ □□ □ □□ □□□ □□□□□?
A. □□□ □□□
B. □□ □□
C. □□□ □□
D. □□□ □□
Answer: D (LEAVE A REPLY)
The best answer is D.
ISACA guidance on shadow AI and emerging technology risk highlights data breaches, privacy risk, and data leakage as major concerns when employees use unapproved public AI tools. Public cloud AI use can expose sensitive data through prompts, uploads, or output handling, making data leakage the greatest immediate concern from an audit and control perspective.
Option A is a concern because AI outputs can be inaccurate, but poor reliability usually does not create the same immediate confidentiality exposure as leaking internal data. Option B is less severe. Option C can matter in some use cases, but the most significant enterprise risk identified in ISACA's public guidance is unauthorized disclosure of data.
References (Official ISACA):
* ISACA, From Shadow IT to Shadow AI: Navigating the New Frontier of Enterprise Risk.

* ISACA, Navigating the Hype and Risk of Emerging Technologies.
* ISACA, Collaboration and the New Triad of AI Governance.

NEW QUESTION: 39
□□□ □□ □□ □□□□ □□ □□ □□□ □□ □□□ □□ □ □□□□□ □□□?
A. □□ □□ □□ □□
B. □□ □□ □□□□□ □□
C. □□ □□ □□(ERM) □□
D. □□ □□ □□□□□ □□
Answer: (SHOW ANSWER)
The primary role of an internal audit function in the management of identified business risks is to validate the enterprise risk management (ERM) process and provide assurance on its effectiveness. The internal audit function should evaluate whether the ERM process is aligned with the organization's objectives, strategies, policies and culture, and whether it covers all relevant risks and controls. The internal audit function should also assess whether the ERM process is operating as designed and producing reliable and timely information for decision making. The other options are not the primary role of an internal audit function, but rather the responsibilities of senior management, board of directors or risk owners. References:
ISACA, CISA Review Manual, 27thEdition, chapter 1, section 1.41
ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12072

NEW QUESTION: 40
□□ □□□ □□ □□□□ □□ □□□ □□□□□ □□ □□ □□ □□□□ □□□□ □ □□□□□.
□□ □ □□ □□□ □□ □□ □□□?
A. □□ □□□□ □□□ □□□□□□.
B. □□□ □□□ □□□ □□□□□□.
C. □□□ □□ □□□□□ □□□□□□.
D. □□ □□□ □□□□□□ □□□□□.
Answer: (SHOW ANSWER)
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: 41
□□ □ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□(CSA)□ □□□□□ □□□ □ □□□ □ □□□□?
A. □□ □□ □□
B. CSA□ □□□□□ □□□
C. □□ □□ □□
D. CSA □□□ □□
Answer: D (LEAVE A REPLY)
Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's

independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.41
CISA Review Questions, Answers and Explanations Database, Question ID 215

NEW QUESTION: 42
□□ □□□ □□□□ □□ □□ □ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □ □□ □□□□ □□□□. □□ □ □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□ □□□ □ □□□ □□□□ □□□ □□□ □□□□ □□□□□.
B. □□□ □□□□ □□ □□ □ □□□□□ □□□□□ □□ □□□□.
C. □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□ □ □□□□.
D. □□ □□□ □□□□□ □□□ □□□ □□□□□ □□□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)
The observation that should be of most concern to the auditor when reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents is that employees can share files with users outside the company through collaboration tools. Collaboration tools are software or hardware devices that enable users to communicate, cooperate, and coordinate with each other on a common task or project. Collaboration tools can facilitate information sharing and knowledge exchange among users, but they can also pose security risks if not properly controlled or managed. Employees can share files with users outside the company through collaboration tools, as this can compromise the security and confidentiality of intellectual property and patents, which are valuable and sensitive assets of the organization. Employees may share files with unauthorized or untrusted users who may misuse or disclose the intellectual property and patents, either intentionally or unintentionally. This can cause harm or damage to the organization, such as loss of competitive advantage, reputation, revenue, or legal rights. Training was not provided to the department that handles intellectual property and patents is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Training is anactivity that educates and instructs users on how to use collaboration tools effectively and securely, such as how to access, share, store, and protect information using collaboration tools. Training was not provided to the department that handles intellectual property and patents, as this can affect the awareness and competence of users on collaboration tools, and increase the likelihood of errors or mistakes that may compromise the security or quality of information. However, this observation may not be directly related to collaboration tools, as it may apply to any information system or resource used by the department. Logging and monitoring for content filtering is not enabled is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Logging and monitoring are processes that record and analyze the events or activities that occur on an information

system or network, such as user actions, system operations, data changes, errors, alerts, etc. Content filtering is a technique that blocks or allows access to certain types of information based on predefined criteria or rules, such as keywords, categories, sources, etc. Logging and monitoring for content filtering is not enabled, as this can affect the auditability, accountability, and visibility of collaboration tools, and prevent detection or investigation of security incidents or violations related to information sharing using collaboration tools. However, this observation may not be specific to collaboration tools, as it may affect any information system or network that uses content filtering. The collaboration tool is hosted and can only be accessed via an Internet browser is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. A hosted collaboration tool is a type of cloud-based service that provides collaboration functionality over the Internet without requiring installation or maintenance on local devices. An Internet browser is a software application that enables users to access and interact with web-based content or services. The collaboration tool is hosted and can only be accessed via an Internet browser, as this can affect the availability and reliability of collaboration tools, and introduce security or privacy risks for information sharing using collaboration tools. However, this observation may not be unique to collaboration tools, as it may apply to any cloud-based service that uses an Internet browser.

NEW QUESTION: 43

□□□□□ □□ □□□ □□ □□ □□□ □□□ □□□ IT □ □□ □□□□, □□ □□□ □□□□ □ □ □□ □□□ □□ □□□ □□□ □□□□.

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: 44
□□ □ □□□ □□ □□(DLP) □□□□□ □□ □□□ □□□□□?
A. □□□ □□□ □□□□□ □□□ □□ □□
B. □□ □□ □ □□ □□ □□□ □□□□□ □□ □□□ □□ □□ □□□ □□□□□□.
C. □□□ □□□□ □□ □□ □□ □□□□□ □□
D. □□□ □□□ □□ □□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
The central goal of DLP is to prevent sensitive data-such as PII, PHI, or intellectual property-from leaving the organization through unauthorized channels. DLP solutions monitor, detect, and block potential data exfiltration via email, endpoints, cloud applications, or removable media. While compliance (D) is often a driver, it is a secondary outcome of implementing DLP. Enhancing performance (A) and recovery automation (B) are not objectives of DLP. ISACA positions DLP as a critical control for confidentiality under DSS05 (Managed Security Services).
References (ISACA): COBIT 2019, DSS05 Managed Security Services.

NEW QUESTION: 45
□□ □□□ □□□ □□ □ □□ □□ □□□ □□□□□?
A. □□ □□□
B. □□ □□□
C. □□ □□
D. □□□ □□ □□□
Answer: B (LEAVE A REPLY)
The use of control totals satisfies the control objective of processing integrity. Processing integrity refers to the accuracy, completeness, timeliness, and validity of data processing. Control totals are a method of verifying the correctness of data processing by comparing the total value or count of a batch of transactions before and after processing. For example, if a batch of 100 invoices is entered into an accounting system, the total amount and number of invoices should match before and after processing. If there is a discrepancy, it indicates an error in data entry, transmission, or processing. Control totals help to ensure that no transactions are lost, duplicated, or altered during processing.
References:
Control Objectives and Activities: Examples, Appropriateness
Levels and Types of Control | Principles ofManagement

CISA Review Manual 27th Edition, page 337

NEW QUESTION: 46
□□ □ □□ □□□ □□ □□□ □□□ □ □□ □□□ □□ □□□□□?
A. IS □□ □□ □□□ □□□□ □□□ □□ □□□
B. □□ □□ □□□ □□□ □□ □□□ □□□□□ □
C. IS □□ □□□ IT □□ □□□□□ □□□
D. IT□ □□□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
The most important factor when defining the IS audit scope is to understand the relationship between IT and business risks, as this helps to identify the areas that have the most potential impact on the organization's objectives, performance, and value. By understanding the IT and business risks, the IS auditor can focus the audit scope on the key processes, systems, controls, and issues that need to be assessed and addressed.
References
ISACA CISA Review Manual, 27th Edition, page 256
Ten Factors to Consider when Setting the Scope of an Internal Audit
What Is an Audit Scope? | Auditing Basics | KirkpatrickPrice

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 47
□□ □□ □□ IS □□□□ □ □□ □□□ □□□□□ IS □□□□ □□□□ □□□ □□ □□□□□ □□ □□□□□□.
A. □□ □□□□ □□□□□ □□ □□□□□ □□□□□.
B. □□ □□ □□□ □□ □□ □□□□□□.
C. □□ □□□□ □□ □□□□ □□□□□.
D. □□□□ □□ □□ □□□ □□ □□ □□□□□ □□□□□□□□.
Answer: (SHOW ANSWER)
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 and Explanations Database

NEW QUESTION: 48
□□□□ □□□□ □□□□ □□□ □□□ □□□ □ □□ □□ □□□□ □ □□□ □□ □□□?
A. □□□ □□ □□
B. □□□ □□
C. □□ □□□□ □□
D. □□□ □□ □□(SLA)
Answer: (SHOW ANSWER)
Data classification is the first consideration when deciding whether data should be moved to a cloud provider for storage because it determines the level of protection and security required for the data. Data classification also helps to identify the legal and regulatory requirements that apply to the data, such as privacy, retention and disposal policies. Data storage costs, vendor cloud certification and service level agreements (SLAs) are important factors to consider, but they are secondary to data classification. References: CISAReview Manual (Digital Version) 1, Chapter 5, Section 5.3.2

NEW QUESTION: 49
□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□□ □□□□ □□
B. □□□ □□□□ □□ □□ □□
C. □□ □□ □□
D. □□□□ □□□ □□ □□ □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
□ □□□ □□□ □ □□□□ □□ □□ □□□□ □□ □ □□□ □□□□ □□□ □□□ □□□□□□□. □□ □□□(IS) □□□□ □□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □□ □□□?
A. □□ □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□.
B. □□ □□ □□□ □□□ □□ □□ □□
C. □□ □□ □□□ □□□ □□□ □□ □□ □□
D. □□□ □□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □□
Answer: (SHOW ANSWER)

Identifying business processes associated with personal data exchange with the affected jurisdiction is the most helpful activity in making an assessment of the organization's level of exposure in the affected country.
An IS auditor should understand how the organization's business operations and functions rely on or involve the cross-border transfer of personal data, as well as the potentialimpacts and risks of the new regulation on the business continuity and compliance. The other options are less helpful activities that may provide additional information or context for the assessment, but not its primary focus. References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
CISA Review Questions, Answers and Explanations Database, Question ID 221

NEW QUESTION: 51
IS □□□□ IT □□□ □□□□ □□□ □□□□□□ □□ □□□□ □□ □□ □□ □□□ □□□ □□□ □□□□□□. IS □□□□ □□□ □□□□ □□ □□ □□ □□□□ □ □ □□ □□□□□?
A. □□□ □□□ □□□ □□ □ □□ □□
B. □□□□□□ □□□□□ □□ □ □□ □□□□
C. □□□□ □□□□ □□□□ □□□ □□ □□□
D. □□□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
The exact definition of the service levels and their measurement is the first thing that the IS auditor should review in order to understand the problem of different opinions on the availability of their application servers.
Service levels are the agreed-upon standards or targets for delivering IT services, such as availability, reliability, performance, and security. Service level measurement is the process of collecting, analyzing, and reporting data related to the achievement of service levels. By reviewing the exact definition of the service levels and their measurement, the IS auditor can identify any gaps, inconsistencies, or ambiguities that may cause confusion or disagreement among IT and the business. The other options are not as important as reviewing the exact definition of the service levels and their measurement, as they do not address the root cause of the problem. References: CISA Review Manual, 27th Edition,page 372

NEW QUESTION: 52
□□ □□□□ □□□ □□ □□□ □□□ □□□ □□ □□□ □□□□?
A. □□ □□□□ □□ □□ □□□□□ □□□□ □□□ □ □□ □□□ □□ □□□ □□ □□□ □□□□ □□ □ □□□□.
B. □□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□ □□□□□.
C. □□ □□□□ □ □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□ □□□□ □.

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

Answer: (SHOW ANSWER)

Quantum algorithms, such as Shor's algorithm, can factor large prime numbers exponentially faster than classical computers, threatening the security of RSA and elliptic-curve cryptography. Similarly, Grover's algorithm reduces the effective strength of symmetric key algorithms by half, requiring larger key sizes.

While post-quantum cryptography is being developed, current algorithms may become obsolete once practical quantum computers exist. Options B, C, and D are incorrect because quantum does not inherently improve encryption, nor is training the key issue-it is the fundamental breakage of cryptographic assumptions.

References (ISACA): ISACA Journal - Cryptographic Risks and Quantum Computing; CISA Review Manual, Cryptography.

NEW QUESTION: 53

□□□ □□ □□□ □□(BCP)□ □□□ □□□□ □ □□□ □□ □□□ □□ □□□ □□ □□ □□□ □ □□ □□□(IS) □□□□ □□□□□ □□ □□□ □□□ □□□□□?

A. □□ □□□ □□

B. □□□ □□□ □□

C. □□□ □□□ □□□□□□□□□.

D. □□ □□ □□□□

Answer: A (LEAVE A REPLY)

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: 54

□ □□□ □□ □□ □□□□□□□ □□□□ □□□□□ □□□□ □□□(IaaS) □□□ □□□□ □□□□. □□□ □□□□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □ □□□□?

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

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

NEW QUESTION: 56
□□ □ □□□ □□ □□□□□□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□?
A. □3□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□ □□□□□.
B. □□ □□ □□ □□□ □□ □□□ □□□□□

C. □□ □□ □□□ □□□□□.
D. □□ □□□□ □□□ □□□□ □□□ □□ □□(SLA)□ □□□□□.
Answer: D (LEAVE A REPLY)
The best way for an organization to mitigate the risk associated with third-party application performance is to utilize performance monitoring tools to verify service level agreements (SLAs). Performance monitoring tools are software or hardware devices that measure and report the performance of an application or system, such as speed, availability, reliability, etc. Performance monitoring tools can help mitigate the risk associated with third-party application performance, by allowing the organization to verify whether the third-party provider is meeting the SLAs, which are contracts or agreements that define the expected level and quality of service for an application or system. Performance monitoring tools can also help identify and resolve any performance issues or problems that may arise from the third-party application. Ensuring the third party allocates adequate resources to meet requirements is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be feasible or effective depending on the availability, cost, and suitability of the resources. Using analytics within the internal audit function is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be timely or relevant depending on the frequency, scope, and quality of the analytics. Conducting a capacity planning exercise is a possible way to mitigate the risk associated with third-party application performance, but it is not the best one, as it may not be accurate or reliable depending on the assumptions, methods, and data used for the capacity planning.

NEW QUESTION: 57
□□□□□□ □□ □□ □ □□ □□ □□□□ □□□ □□□ □□ □ □□ □ □□ □□ □ □□□ □□ □□ □□□□□?
A. □□□ □□□ □□□□.
B. □□□□ □□□□□.
C. □□□ □□ □□
D. □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 58

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

NEW QUESTION: 59
□□□ □□ □□ □□(SDLC)□ □□□□ □□ □□□(IS) □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□□□□. □ □□ □□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□□□ □□□□□.
B. □□□□ □□ □□□ □□□ □□□□ □□□□□.
C. □□□□ □□□ □□□ □□□ □□□□□□.
D. □□□□□ □□□ □□ □□□ □□□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □ □□□ □□□□□□. □□□□ □□ □□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□□□ □□□□ □□□□□ □□□□□□ □□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□□ □□□□ □□□ □□□ □□□□□.
C. □□□□□□□ □□□ □□ □□(DLP) □□□ □□□□□□.
D. □□ □□ □ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first course of action that the auditor should recommend after finding that several employees are spending an excessive amount of time using social media sites for personal reasons is to implement policies addressing acceptable usage of social media during working hours. Policies can help define the scope, purpose, rules, and expectations of using social media in the workplace, both for personal and professional reasons. Policies can also specify the consequences of violating the policies, such as disciplinary actions or termination. Policies can help deter employees from misusing social media at work, which could affect their productivity, performance, or security. Policies can also help protect the organization from legal liabilities or reputational damages that could arise from inappropriate or unlawful employee behavior on social media.

NEW QUESTION: 61
□□ □ □□ □□ □ □□□ □□□□ □□ □□□□ □□□□ □□□ □□□□□?
A. □□ □□
B. □□ □□ □□□
C. □□ □

D. □□□ □□

Answer: (SHOW ANSWER)

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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 62

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

A. □□ □□ □□

B. □□ □□□□□□ □□□ □□ □□□□□

C. □□ □□□ □□ □□ □□

D. □□ □□(QA) □□□ □□ □□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 63
□□ □ □□ □□ □□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □□ □□(BIA)
B. □□ □□
C. □□ □□
D. □□ □□ □□□□
Answer: C (LEAVE A REPLY)
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: 64
□□ □□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□□□ □ □□.
A. □□ □□□ □□.
B. □□□□ □□.
C. □□ □□ □□.
D. □□□ □□□.
Answer: (SHOW ANSWER)
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: 65
IS □□□□ □□ □□ □□(CSA) □□□□□ □□ □□□ □□□□□ □□□□□□□. □ □ □ □□□□□□ □□□□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□□ □□□□ □□□ □□□ □□□□ □□□.
B. □□□□ □□□ □□ □□□ □□□□ □□□.
C. □□□□ □□□□ □□□ □□□ □□ □□□.
D. □□□□ □□□ □□ □ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
□□ □ □□□□ □□ □□□ □□□ □□ □□ □□□□□ □□ □□□□□□ □□□□ □□□ □□ □□□?
A. □□□□□□ □□□ □□(HTML) □□ □□
B. □□ □□ □□□□ □□ □□□□
C. □□ □□□ □□ □□□
D. □□ □□□□ □□ □□□ □□□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 67
□□ □ □□ □□ □□□□ □□□ □□ □□ □□□ □□□ □ □□ □□ □□□□ □ □□ □ □□□□□?
A. □□ □□ □□□ □□ 2□ □□ □□□□□□ □□□□□.
B. □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□.
C. □□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
References
1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 68
□□□ □□□ □□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□ □□□□□ □□ □?
A. □□ □□□□ □□
B. □□□ □□ □□
C. □□ □□ □□
D. □□ □□ □□ □ □□ □□
Answer: C (LEAVE A REPLY)
The primary basis for selecting which IS audits to perform in the coming year is the organizational risk assessment. An organizational risk assessment is a formal process for identifying, evaluating, and controlling risks that may affect the achievement of the organization'sgoals and objectives3. An organizational risk assessment can help IS auditors prioritize and plan their audit activities based on the level of risk exposure and impact of each area or process within the organization. An organizational risk assessment can also help IS auditors align their audit objectives and criteria with the organization's strategy and performance indicators.
Senior management's request, prior year's audit findings, and previous audit coverage and scope are also possible bases for selecting which IS audits to perform in the coming year, but not as primary as the organizational risk assessment. These factors are more secondary or supplementary sources of information that can help IS auditors refine or adjust their audit plan based on specific needs or issues identified by management or

previous audits. However, thesefactors may not reflect the current or emerging risks that may affect the organization's operations or performance. References: ISACA CISA Review Manual 27th Edition, page 295

NEW QUESTION: 69
□□□ □□□ □□ □□(ERM) □□□□□ □□ □□□ □□□□ □□□□?
A. □□ □□ □□ □□□(CRO)
B. □□□□□
C. □□□
D. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 70
□□ □ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□□ □□ □□ □□□ □□□□ □□□ □□
B. □□ □□□ □□□□ □□□ □□□ □□□ □□
C. □□□ □□□ □□ □□ □□□ □□□□□□ □□
D. □□□ □□□ □□□□ □□□□□ □□□□□ □□□ □□□.
Answer: B (LEAVE A REPLY)
The primary role of an audit reviewer with regard to evidence is to ensure that evidence is sufficient to support audit conclusions. Evidence is the information obtained by the auditor to provide a reasonable basis for the audit opinion or findings. Evidence should be sufficient, reliable, relevant, and useful to support the audit objectives and criteria. The audit reviewer should evaluate the quality and quantity of evidence collected by the auditor and determine if it is adequate to draw valid conclusions and recommendations. Ensuring unauthorized individuals do not tamper with evidence after it has been captured is a role of the auditor, not the audit reviewer. The auditor is responsible for safeguarding the evidence from loss, damage, or alteration during the audit process. The auditor should also document the source, date, and method of obtaining the evidence, as well as any limitations or restrictions on its use or disclosure. Ensuring appropriate statistical sampling methods were used is a role of the auditor, not the audit reviewer. The auditor is responsible for selecting an appropriate sampling method and technique that can provide sufficient evidence to achieve the audit objectives and criteria. The auditor should also document the sampling plan, population, sample size, selection method, evaluation method, and results. Ensuring evidence is labeled to show it was obtained from an approved source is a role of the auditor, not the audit reviewer. The auditor is responsible for labeling the evidence to indicate its origin, nature, and ownership. The auditor should also ensure that the evidence is obtained from reliable and credible sources that can be verified and corroborated. References: ISACA CISA Review Manual 27th Edition, page 295

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

NEW QUESTION: 72
□□ □ □□ □□□□ □□ □□□ □□□□ □□ □ □□□ □□□□□?
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: 73
□□ □ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□ □□(DES)
B. □□□ □□
C. □□ □ □□□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)
A digital signature is the most appropriate control to ensure integrity of online orders because it provides a way to verify the authenticity and integrity of the data sent by the sender. A digital signature is created by applying a cryptographic algorithm to the data and attaching the result to the data. The receiver can then use the sender's public key to verify that the data has not been altered or tampered with during transmission. A digital signature also provides non-repudiation, which means that the sender cannot deny sending the data.
Data Encryption Standard (DES) is a symmetric encryption algorithm that can provide confidentiality of online orders, but not integrity. DES uses the same key to encrypt and decrypt the data, which means that anyone who has the key can modify the data without detection.
Public key encryption is an asymmetric encryption algorithm that can also provide confidentiality of online orders, but not integrity. Public key encryption uses a pair of keys: a public key and a private key. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their own private key.
However, public key encryption does not prevent anyone from modifying the encrypted data.
Multi-factor authentication is a control that can provide authentication and authorization of online orders, but not integrity. Multi-factor authentication requires the user to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Multi-factor authentication can prevent unauthorized access to online orders, but it does not protect the data from being modified after being sent.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 281 1
ISACA, CISA Review Questions, Answers and Explanations Database - 12 MonthSubscription 2

NEW QUESTION: 74
IT □□□ □□□□ □□□ □□□□ □□□ □□□ □, □□ □□ □□ □ □□ □□ □□ □□□□□?
A. □□□□□ □□
B. □□ □□ □□□(ROI) □□ □□ □□ □□□
C. □□ □□ □□ □□ □□
D. □□ □□ □□□(ROI) □ □□ □□ □□ □□□
Answer: B (LEAVE A REPLY)

The best way to determine whether IT investments are meeting business objectives is to compare the realized 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: 75
□□ □□ □□□ □□ □□□□□□ □□□□ □□□ □□ □□□ □□□□ □□□.
A. IT □□□ □□□□□.
B. IT □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□□□.
D. □□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 76
□□ □ □□□□ □□□□ □□□ □□□ □□ □□□□□□(KPI)□ □□ □□□ □□□□ □?
A. □□□□□□ □□□□ □□□□ □□□□□ □□□□□ □□□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□□□□ □□ □□□ □□□ □□ □□ □□□ □□□□□.
C. □□□□ □□□□□ □□□□ □□□□□ □□□□ □□□□ □□□□□.
D. □□ □□□ □□ □□□□□ □□ □ □□ □□□ □□ □□□ □□□ □ □□□ □□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed in-Depth Explanation:
The primary role of KPIs is to provide measurable insights into the performance of business processes and identify variances that may require corrective actions. KPIs help organizations understand whether their processes are achieving desired outcomes and where improvements are needed.
While Option A discusses workflow optimization, it is a secondary benefit rather than the primary purpose.
Options B and C do not accurately describe the core purpose of KPIs.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 77
□□□□ □□ □□□□□ □□□□ □□ □□ IS □□□□ □□□ □□□□ □□□□□□ □□□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□□□. □□ □ □□□□ □□ □ □□□ □□□□□?
A. □□□□□ □□□□ □□□□ □□□ □□□ □□□□□.
B. □□ □□□□□ □□□□ □ □□ □□
C. □□ □□□□□ □□□□□ □□ □□□ □□ □□ □□
D. □□□□ □□□ □□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
The auditor's best course of action after discovering instances where employees shared license keys to critical pieces of business software is to verify whether the licensing agreement allows shared use. A licensing agreement is a contract between the software provider and the user that defines the terms and conditions of using the software, including the number, type, and scope of licenses granted. Some licensing agreements may allow shared use of license keys among multiple users or devices, while others may prohibit or restrict such use. By verifying the licensing agreement, the auditor can determine whether the employees violated the contract or not, and whether there are any legal or financial risks or implications for the organization.
The other options are not as appropriate as option D, as they may not address the root cause of the issue or provide a comprehensive solution. Recommending the utilization of software licensing monitoring tools may help prevent or detect future instances of license key sharing, but it does not resolve the current situation or ensure compliance with the licensing agreement. Recommending the purchase of additional software license keys may be unnecessary or wasteful if the licensing agreement already allows shared use or if there are unused licenses available. Validating user need for shared software licenses may help identify the reasons or motivations behind license key sharing, but it does not justify or excuse such behavior if it violates the licensing agreement.
References:
* 9: Best License Management Software 2023 | Capterra
* 10: Best 10 Software License Management Tools in 2023 | Zluri
* 11: Top 10 Software License Tracking Tools | Zluri

* 12: Top 5 Software License Tracking Solutions in 2023 - DNSstuff

NEW QUESTION: 78
□□ □ □□□ □□ □□ □□ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□
B. □□□ □□ □□□ □□
C. □□ □□ □□□□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
A self-checking digit is the most effective accuracy control for entry of a valid numeric part number. This method involves adding an extra digit at the end of every number which is calculated from the other digits. This digit is then used to check the accuracy of the entered number1. While hash totals, online review of description, and comparison to historical order pattern can be used as accuracy controls, they are not as effective as a self-checking digit.

NEW QUESTION: 79
□□ □□□(IS) □□□□ □□□□(AI) □ □□□ □□□ □□□□□□□ □□□□ □□□ □. □□ □□□□□ □□□ □□□ □□□ □□ □□ □□□□ □□□ □□□□□□. IS □ □□□ □□□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□?
A. □□□□ □□□ □□□□ □□□ □□□□□□.
B. □□□□ □□ □□□ □□□□□ □□□□□.
C. □□□□ □□□ □□□ □□□□□.
D. □□□ □□□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
□□ □ IS □□□□ □□ □□ □□ □□□ □□□ □ □□ □□ □□□□ □ □□□ □□□ □□?
A. □□ □□□ □□□□ □ □□ □□□□□□□.
B. □□ □□ □□(RPO)□ □□□□ □□□□□.
C. □□ □□ □ □□□ □□□□ □□□□□□□.
D. □□□ □□□ □□ □□□□ □□□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
□□□ DLP □□□□ □□□ □ □□□ □□ □□(DLP) □□□ □□ □□□ □□□□□?
A. □□□□ □□□□ □□□□ □□□□ □□□□□.
B. □□□□ □□□ □□ □□□ □□□□ □□□□□.
C. □□ □ □ □□ □□ □□□ □□□□ □□□□□□.
D. □□□ □□□□ □□□□□□ □□□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
□□ □ □□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□(QA)□ □□□□□.
B. □□□ □□ □□□ □□ □□ □□□ □□□□□□.
C. □□□□ □□□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□ □□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
An integrated audit combines IT, operational, and financial audits into a single coordinated review. The primary benefit is the optimization of audit efforts across functions, eliminating duplication and providing a holistic risk perspective.
Option A: QA enhancement is a byproduct but not the primary benefit.
Option C: Skills improvement occurs, but it's not the main objective.
Option D: Applicability to different areas is true, but not the primary benefit.
ISACA Reference: CISA Review Manual 27th Edition, Domain 1, section on integrated audit benefits and efficiencies.

NEW QUESTION: 83
□□□ □□ IT □□ □□□ □□□ □□□ □□□□ □□ □ □□□ □□ □□□ □□ □□ □ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□ □□□ □□ □ □□□ □□ □□ □□□ IT □ □□ □□□□□ □□□□ □□□□.
B. IT □ □□□□□ □□□ □□ □□□(IJAT)□ □□ □□□□□□.
C. IT □□□□ □□ □ □□ □□□ □□□ □ □□□□.
D. □□ □□□ □□□□ □□ □□ □ □□□□ □□□□ □□ □□□□.
Answer: D (LEAVE A REPLY)
Post-implementation testing is the process of verifying and validating the functionality, performance, and security of a system after it has been deployed to the production environment1. Post-implementation testing is important for ensuring that the system meets the user requirements and expectations, as well as the operational and business objectives. Post-implementation testing also helps to identify and resolve any defects, errors, or issues that may have occurred during the deployment process or that may have been missed during the previous testing stages2.
Therefore, the observation that post-implementation testing is not conducted for all system releases should be of greatest concern to an IS auditor performing an audit of change and release management controls for a new complex system developed by a small in-house IT team. This observation indicates that the system may have quality, reliability, or security problems that could affect the user satisfaction, system performance, or data integrity. This observation also suggests that the change and release management controls are not

adequate or effective, as they do not ensure that all system releases are properly tested and validated before and after deployment.
Option A is not correct because access to change testing strategy and results is not restricted to staff outside the IT team is not a major concern for an IS auditor. While it is good practice to limit access to sensitive or confidential information, such as test data or test cases, to authorized personnel only, access to change testing strategy and results may not pose a significant risk to the system or the organization. Moreover, access to change testing strategy and results may be beneficial for some stakeholders outside the IT team, such as business users, project managers, or auditors, who may need to review or evaluate the testing process or outcomes.
Option B is not correct because some user acceptance testing (UAT) was completed by members of the IT team is not a major concern for an IS auditor. User acceptance testing is the process of verifying and validating that the system meets the user requirements and expectations by involving actual or representative users in the testing process3. While it is preferable to have independent and unbiased users perform UAT, it may not be feasible or practical for some organizations, especially those with small or limited resources. Therefore, some UAT may be completed by members of the IT team, as long as they have sufficient knowledge and experience of the user needs and expectations, and as long as they follow the UAT plan and criteria.
Option C is not correct because IT administrators have access to the production and development environment is not a major concern for an IS auditor. IT administrators are responsible for managing and maintaining the IT infrastructure, including the production and development environments4. Therefore, it is reasonable and necessary for them to have access to both environments, as long as they follow the appropriate policies and procedures for accessing, using, and securing them. Moreover, IT administrators may need to perform tasks such as backup, restore, patching, or troubleshooting in both environments.
References:
What Is Post Implementation Testing?1
Post Implementation Review (PIR) - Definition and Process2
User Acceptance Testing (UAT): Definition and Examples3
What Is an IT Administrator? Definition and Examples4

NEW QUESTION: 84
□□ □ □□ □□□ □□□□ □□□□□ IT □□□□ □□□□□ □□□ □□□□ □□□ □ □□ □□ □□□ □□□ □□□□□?
A. □□□□□□ □□ □□□□ □□ IT □□□□□ □□□□□.
B. □□□□□□ □□□ □□□ □□ □□□□□ □□□□ □ □□□□.
C. □□□□□□ □□ □□ □□(CSA)□ □□□□ □□ □ □□□ □□□.
D. □□□□□□ □□□ IT □□□ □□□□ □□□□ □ □□□ □□□.
Answer: B (LEAVE A REPLY)

The best reason for an IS auditor to emphasize to management the importance of using an IT governance framework is that frameworks can be tailored and optimized for different organizations. An IT governance framework is a set of principles, guidelines, and processes that help an organization align its IT strategy with its business goals, manage IT risks and performance, and deliver value from IT investments. An IT governance framework can be adapted and customized to suit the specific needs, context, and culture of each organization, taking into account factors such as size, industry, maturity, objectives, and stakeholders. An IT governance framework can also help an organization adopt best practices and standards from various sources, such as COBIT2, ITIL3, ISO/IEC 200004, and others.
The other options are not as good as option B, as they may not capture the full scope or benefits of using an IT governance framework. Frameworks enable IT benchmarks against competitors, but this is not the main purpose or advantage of using an IT governance framework. Frameworks help facilitate control self- assessments (CSAs), but this is only one aspect or tool of an IT governance framework. Frameworks help organizations understand and manage IT risk, but this is also only one outcome or objective of an IT governance framework.
References:
1: What is ITIL? Your guide to the IT Infrastructure Library | CIO
2: IT Governance Framework | Components | Framework | Terminology - EDUCBA
3: IT Governance: Definitions, Frameworks and Planning - ProjectManager
4: What Is IT Governance? - Definition from Techopedia
5: What is IT Governance? A formal way to align IT and business strategy | CIO
6: What Is IT Governance? - Definition from WhatIs.com
7: ISO/IEC 20000 Information Technology Service Management Systems Standard - ISO/IEC 20000 Portal
8: COBIT | Control Objectives for Information Technologies | ISACA

NEW QUESTION: 85
□□ □ □□□ □□ □□□ □□□□ □□□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□ □□□□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□ □□ □□ □ □□ □□ □□(KPI) □□ □□
C. □□ □□ □□□ □□□□ □ □□□□ □□ □□□ □□□□□.
D. □□ □ □□□□ □□ □□□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
Conducting periodic testing and incorporating lessons learned is the best way to improve the effectiveness of an incident response team. This allows the team to practice their response procedures, identify any gaps or weaknesses in their response, and learn from their mistakes. It also helps to keep the team's skills sharp and up-to-date. The lessons learned from these tests can then be used to improve the team's procedures and performance12. While understanding information systems technology, disseminating

incident response procedures, and publishing KPI metrics can contribute to the effectiveness of the team, they do not provide the same level of continuous improvement as periodic testing and learning from experience.

NEW QUESTION: 86
□□□□ □□ □□□ □□□ □□□ □□□□□□. □□ □□□ □□ □□□□ □□□ □ □□□ □□ □□□□.
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: 87
□□ □□ □□□ □□□ □□ □□□ □ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□.
A. □□□□ □□□□ □□□□□.
B. □□□□□□, □□□ □ □□□, □□□□□□.
C. □□□□ □□ □□□□ □□ □□□□.
D. □□□ □□ □□ □□□.
Answer: D (LEAVE A REPLY)
ISACA defines sufficient and appropriate evidence as the standard for audit conclusions. Appropriateness relates to relevance (applicability) and reliability (persuasiveness). Evidence that is persuasive and directly applicable to the audit objective provides stronger assurance than evidence that is merely timely, complete, or reasonable. While the other options describe desirable qualities, they do not encompass the full ISACA standard. Thus, the most complete characterization of quality evidence is that it must be persuasive and applicable to the audit's purpose.
References (ISACA): ISACA Audit and Assurance Standards; ISACA ITAF Guidelines on Evidence.

NEW QUESTION: 88
□□ □□□ □□□(EUC) □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□□□ □ □□.
A. □□ □□ □□(BIA)□ □□□□□.

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

NEW QUESTION: 89
□ □□□□ □□□ □□□ □□ □□(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: 90
□□□□□ □□□ □□□ □□ □□ □□ □□ □ □□ □□□ □□ □□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
Segregation of duties is a fundamental concept in cybersecurity and information security. It refers to the practice of dividing critical tasks and responsibilities among different individuals or roles within an organization to reduce the risk of fraud, error, or unauthorized activities1. Segregation of duties is designed to prevent unilateral actions within an organization's workflow, which can result in damaging events that would exceed the organization's risk tolerance2.
There are different types of responses to risk associated with segregation of duties, depending on the level of risk and the cost-benefit analysis. Some of the common responses are:
Risk acceptance: This means acknowledging a risk and deciding to tolerate it without taking any corrective actions. This response is usually chosen when the risk is low or the cost of mitigation is too high3.
Risk mitigation: This means taking steps ahead of time to lessen the effects of a risk and make it less likely to happen. Some examples of mitigation strategies are making backup

plans, setting up early warning systems, and staying away from high-risk areas or activities4.
Risk transference: This means shifting the negative impact of a risk and/or the responsibility for managing the risk response to a third party. Some examples of transference strategies are outsourcing, insurance, or contracts5.
Risk reduction: This means reducing the probability and/or severity of the risk below a threshold of acceptability. Some examples of reduction strategies are implementing controls, policies, or procedures to prevent or detect risks6.
Based on these definitions, the response to risk associated with segregation of duties that would incur the lowest initial cost is A. Risk acceptance. This is because risk acceptance does not require any additional resources or actions to address the risk. However, risk acceptance also implies that the organization is willing to bear the consequences of the risk if it occurs, which could be costly in the long run.
Therefore, the correct answer to your question is A. Risk acceptance.

NEW QUESTION: 91
□□□□ □□ □□□□□ □□□ □□ □□ □□□□□ □□□ □ □□ □□□ □□ □ □ □□□□?
A. □□□□ □□ □□□□□□ □□□□□□ □□□ □□□□□ □□□□ □□□□.
B. □□□□ □□ □ □□□□ □□□□□□ □□□□□ □□ □ □□□□.
C. □□ □□□ □□□□ □□ □□□□□□ □□□ □□□ □□□□□□□.
D. □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □ □□□□.
Answer: D (LEAVE A REPLY)
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21
CISA Review Questions, Answers and Explanations Database, Question ID 213

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 92
□□ □ □□ □□□ □□□ □□□□ IT □□□ □□□□□ □ □□□ □□ □□ □□ □□ □ □□□□□?
A. □□ □□□□ □□□ □□□ □□□ □□ □□(SDO)□ □□□□□.
B. IT □□ □□□ □□□□□ □□ □□□ □□□□ □□□□□.
C. □□ □□□ □□□□□ □□□□ □□□□ □□□□□ □□ □□□ □□□□□ □□□ □□.
D. □□□□ □□□ IT □□ □□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
A governing body monitors IT performance most effectively when IT performance metrics are aligned with business goals. ISACA's COBIT-based governance guidance consistently emphasizes that metrics should help leadership and governing bodies monitor the achievement of enterprise business goals and related IT goals. Metrics are useful for governance only when they are connected to what the enterprise is trying to achieve.
Option D is correct because a governing body is responsible for oversight at the strategic level. Strategic oversight depends on understanding whether IT is supporting business objectives, not just whether technical measures are being collected. ISACA states that metrics help management monitor achievements of business- related and IT-related goals.
Option A is useful at an operational or service management level, but it is narrower than business alignment.
Service delivery objectives matter, yet the governing body's concern is broader enterprise value and strategic alignment.
Option B is not the best answer because manufacturer recommendations may help establish technical asset baselines, but they do not ensure metrics support governance needs or enterprise performance oversight.
Option C is attractive because automated, quantitative data improves reliability and efficiency, but automation alone does not guarantee the metrics are the right ones. Governance requires relevant metrics tied to business outcomes, not just easily measured data.
Therefore, D is the best answer because proper alignment between business goals and IT performance metrics is what most enables a governing body to monitor IT performance meaningfully.
References (Official ISACA):
* ISACA Journal, Performance Measurement Metrics for IT Governance - metrics help management monitor achievement of business-related and IT-related goals.
* ISACA Journal, How to Construct a Governance System From the Board Level to the Code Level - enterprise goals are cascaded into IT alignment goals, metrics and results.

* ISACA, Charting the Course of IT Governance - performance measurement involves defining and monitoring KPIs for IT and communicating performance to stakeholders.
* ISACA, Seven Key Features, Lessons and Tips From a COBIT Journey of 27 Years - COBIT uses goals, metrics and capabilities at enterprise and IT levels.

NEW QUESTION: 93
□□ □ IT □□□ □□□ □□ □ □□□ □□□□ □□ □ □□□□ □□ □□□□□?
A. IT □□□ □□ □□□□ □□□□□□□ □□□□□.
B. □□ □□□ □□ □□ □□□(CIO)□□ □□□□□.
C. □□□□ □□□□□□□ IT □□ □□□ □□□□□.
D. □□□□□□□(CIO)□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes.
By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders. References: CISAReview Manual, 27th Edition, page
97

NEW QUESTION: 94
□□□ □□ □□□ IS □□ □□□ □□□□□□. □□ □ □□ □□ □□ □□ □ □□ □ □□ □□□□□?
A. □□□□□ □□ □□
B. □□ □□□ □□
C. □□ □□ □□
D. □□ □□□ □□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)
The first step for the security incident response team after an IS security attack is reported is to perform a damage assessment. This involves identifying the scope, impact and root cause of the incident, as well as collecting and preserving evidence for further analysis and investigation. Reporting results to management, documenting lessons learned and prioritizing resources for corrective action are important steps, but they should be done after the damage assessment is completed. References: CISA Review Manual (Digital Version), Chapter 6, Section 6.31

NEW QUESTION: 95

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

A. □□□

B. □□□□□

C. IS □□ □□□

D. □□□□ □□□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 96

□ □□□ IT □□□ □□ □□ □□□ □□ □□□ □□ □□ □□ □□□(CIO)□□ □□□ □□. □□□ □□ □□□ □□□ □□ □ □□□□ □□□□□?

A. □□□□ □□ □□ □□ □□□

B. IS □□ □□□ □□

C. IS □□ □□□□ □□ IT □□□ □□□□ □□□□.

D. IS □□ □□□ □□ □□ □□□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

The greatest concern with the IT department and internal IS audit function both reporting to the CIO is the potential compromise of IS audit independence. Auditor independence refers to the impartiality and objectivity of an auditor in conducting an audit, free from conflicts of interest and bias1. It is crucial for ensuring the quality and reliability of financial reporting1. If the IS audit function reports to the CIO, who also oversees the IT department, it could create a conflict of interest that might compromise the impartiality and objectivity of the IS audit function.

References:

Auditor Independence - What is it, Rules, Importance, Examples

NEW QUESTION: 97

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

A. □□□□□□ □□□ □□ □□(SLA)□ □□□□□□□.

B. □□□□□ □□□□ □□ □□□ □□□□□.

C. □□□□□ 5□ □□ □□□□ □□□ □□□□□ □□□□□.

D. □□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98

□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□□ □ □□ □□ □□ □□(CRM) □□□□ □□□ □□□□ □□□□. □□ □ □□□□ □□□□ □ □□□ □□□□□?

A. □ □□□□ □□ □3□ □□□ □□□□□ □□□□ □□□□□□.

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

C. □□ □□□□ □□ □□□□□ □□□□□(DMZ) □□ □□□□□□.
D. □□ □□□□ □□ □□□□□ □□ □□□□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
A web-based CRM system that is directly accessed by customers via the Internet should be hosted in a secure and isolated environment to protect it from external threats and unauthorized access. A web-based CRM system should also be reliable, trusted, and backedup regularly1.
Hosting the system on an external third-party service provider's servers (A) or a hybrid-cloud platform managed by a service provider (B) may not be a concern for the auditor if the service provider has adequate security measures and service level agreements in place. The auditor should verify the security controls and contractual terms of the service provider before trusting them with the CRM data23.
Hosting the system within a demilitarized zone (DMZ) of a corporate network is a common practice to provide an extra layer of security to the CRM system from untrusted networks, such as the Internet. A DMZ is a perimeter network that isolates the CRM system from the internal network and filters the incoming traffic from the external network using a security gateway4567.
Hosting the system within an internal segment of a corporate network (D) is a concern for the auditor because it exposes the CRM system and the internal network to potential attacks from the Internet. The CRM system should not be directly accessible from the Internet without a DMZ or a firewall to protect it. This could compromise the confidentiality, integrity, and availability of the CRM data and the internal network78.

NEW QUESTION: 99
□□□ □□□ □□ □□□□ □□□ □□ □□□ □□ □□ □□□□ □□□ □□□ □ □ □□ □□□□ □ □□ □□ □ □□ □□□ □□ □□□□□?
A. □□ □□□□ □□□ □□□ □□□□□□ □□ □□□ □□
B. □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□□□.
C. □□ □□□□ □□□ □□ □□ □□ □□□□□□ □□ □□□ □□□□□.
D. □□□□ □3□□□ □□□ □□□ □□□□ □
Answer: (SHOW ANSWER)
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)

NEW QUESTION: 100
□□ □□□ □□□□ □□□□□□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □ □□□. □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□□□. □□ □ □□ □□□ □□□□□?
A. □□ □□□
B. □□□ □□□
C. □□ □□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
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 impacton 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 ReviewQuestions, Answers and Explanations Database, Question ID 230

NEW QUESTION: 101
□□ □□□ □□□□ □□ IS □□□□ □□□□ □□ □□□ □□ □□ □ □□□□ □□ □ □□ □□ □□□ □□□ □□ □□□□ □□□□. □□□ □□□ □□□□ □□ IS □□ □□ □□ □ □□ □□□ □□□ □□□ □□□□.
A. □□ □□□ □□□ □□□ □□□□□□□□ □□ □□□□□ □□□□□.
B. □□ □□ □□□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□□□ □□□□□.
D. □□□ □□□ □□□ □□□ □□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The IS auditor's best course of action in this situation is to determine whether the alternative controls sufficiently mitigate the risk. Alternative controls are different from those originally discussed and agreed with the audit function, but they may still achieve the same objective of addressing the audit issue or reducing the risk to an acceptable level. The IS auditor should evaluate whether the alternative controls are appropriate, effective, and sustainable before closing the audit finding or escalating it to senior management. The other options are not appropriate for resolving this situation, as they do not consider whether the alternative controls are adequate or reasonable. Re-prioritizing the original issue as high risk and escalating to senior management is a drastic step that may undermine the relationship between the auditor and management, and it should be done

only after exhausting other means of resolving the issue. Scheduling a follow-up audit in the next audit cycle is unnecessary, as follow-up activities should be performed as soon as possible after management has implemented corrective actions. Postponing follow-up activities and escalating the alternative controls to senior audit management is premature, as follow-up activities should be completed before reporting any findings or recommendations to senior audit management. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 102
□□ □ □□□ □□ □□ □ □□ □□□ □□□ □ □□□□ □□ □□□ □□□□□?
A. □□ □□□
B. □□□ □□ □□(DLP) □□□
C. □ □□□□□□ □□□
D. □□□□ □□
Answer: (SHOW ANSWER)
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: 103
□□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□□□□.
□□ □ □□ □□□□ □□□□ □ □□□ □□□□□? □□ □□□ □□ □□□ □□□□ □□□.
A. □□ □□□ □ □□□□ □□□□.
B. □□ □□□ □□□□□.
C. □□□□ □□□□ □□□□□□.
D. □□ □□□□□□□.
Answer: (SHOW ANSWER)
The most important thing to determine next after concluding that an organization has a quality security policy is whether the policy is well understood by all employees. A security policy is a document that defines the objectives, scope, roles, responsibilities, and rules for information security within an organization. A quality security policy is one that is clear, concise, consistent, comprehensive, and aligned with business goals and requirements. However, a quality security policy is useless if it is not well understood by all employees who are expected to comply with it.Therefore, the IS auditor should assess the level of awareness and understanding of the security policy among employees and identify any

gaps or issues that need to be addressed. The other options are not as important as ensuring that the security policy is well understood by all employees, as they do not directly affect the implementation and effectiveness of the security policy. References: CISA Review Manual, 27th Edition, page 317

NEW QUESTION: 104
□□ □□ □□ □ □□ □□ □□□□ □□ □□□ □□ □□ □□□ □□ □ □□ □□ □ □ □□□ □□□□ □□□ □□□ □□ □□□□□. 1□ □□□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □□ □ □□□ □□□□ □□□ □ □□ □□□ □□ □□□ □□□ □□?
A. □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □□□□□□.
B. □□ □□ □□□ □□□ □□ □□□ □□□□□ □□□ □□□□□.
C. □□ □□□ 6□□□□ □□ □□□ □□□ □□□ □□□□□□.
D. □□ □□ □□ □ □□ □□□ □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
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: 105
□ □□□ □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□ □3□□□ □□□ □ □□□□□. □□ □ □□□□□□□ □□□ □□ □□□ □□□□□ □□□□ □ □□ □ □□ □□□□□ □□□□□?
A. □□□□□□(KPI) □□□□
B. □□ □□
C. □□ □□
D. □□ □□(QA)
Answer: (SHOW ANSWER)
The most important process to help ensure the application provides accurate calculations is quality assurance (QA), which involves verifying that the application meets the specified requirements and standards, and testing the application for functionality, performance, reliability, security, and usability. QA helps to identify and correct any defects or errors in the application before it is deployed to the production environment. Key performance indicator (KPI) monitoring, change management, and configuration management are important processes for managing and maintaining the application after it is implemented, but they do not directly ensure the accuracy of the calculationsperformed by the application. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section

3.3: Practices for Quality Assurance

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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 107

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

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

NEW QUESTION: 109
□□ □□□ □□□(EUC)□□ □□□ □□□ □□□ □□ □□□ □ □□□□ □□□ □□ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□ □3□□□ □□ □□□ □□□□□ □□□□.
B. □□ □□□□□□□ EUC □□□□□ □□□□ □□□□□.
C. □□□ □□ □□ □□□ □□□□□.
D. □□ □□□ □□ EUC □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 110

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

A. □□ □□ □□□□ □□□ □□□ □□ □□□

B. □□ □□□ □□□ □□ □□ □□

C. □□□□ □□□ □□ □□□ □□ □□

D. □□□□ □□ □□ □□

Answer: C (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?

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: 111

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

A. □□ □□□ □□ □□□□ □□□□□□ □□ □□

B. □□□□□□ □□ □□□(DBMS)□ □□□□ □□□□□ □□□ □□□□□ □□□□ □□□□ □□

C. □□□ □□ □□□ □□ □□□□ □□ □□

D. □□ □□□□□□ □□□ □□ □□ □□

Answer: B (LEAVE A REPLY)

The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A

DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.
References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 112
□□□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□ □□ □□□ □□□□:
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: 113

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

A. □□ IT □□ □□ □□

B. □□□□ □□□ □□□ □□

C. □□ □□□□□ □□□□ □□ □□□ □□ □□

D. □□□□ □□□ □□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 114

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

A. □□□ □□ □ □□□ □□□ □□□□ □□□□.

B. □□□ □□ □□□□ □□ □□□ □□□ □□□□.

C. □□ □□□ □□ □□□□ □□ □□□□□□□.

D. □□ □□□ □□□ □□□□□□□.

Answer: C (LEAVE A REPLY)

An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessmentshould 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, butthey 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 assessmentshould 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 and Explanations Database - 12 Month Subscription Data Center Threats and Vulnerabilities1 Datacenter threat, vulnerability, and risk assessment2 Data Centre Risk Assessment3

NEW QUESTION: 115
□□ □ IT □□ □□ □□□□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □□
B. □□ □□ □□ □□□ □□ □□ □□□ □□
C. □□ □□□ □□□ □□
D. IT □□□ □□□□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
□□ □ □□ □□□ □□ □□□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□□?
A. □□ □□
B. IT □□ □□□
C. □□ □□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
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: 117
□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□ □□ □□(PII)□ □□ □□ □□ □ □□□□ □□□ □□□ □□ □□□□□. □□ □□ □□□□□□ □□□ □□□ □□ □ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□□□ □□
B. □□□□□□ □□□
C. □□□□□□ □□
D. □□□□□□ □□□

Answer: A (LEAVE A REPLY)
The best recommendation is database segmentation. If liability depends on the number of individuals whose PII is exposed, the organization should reduce the amount of data that could be compromised in any single breach event. Segmenting databases or separating sensitive data domains limits blast radius and can reduce the number of records exposed in a single incident. ISACA guidance supports isolating high-value assets and tightening internal controls as a way to reduce exposure and improve resilience.
Option A is correct because segmentation limits concentration risk. Instead of keeping all customer data in one broadly exposed logical store, segmentation helps confine access and reduce how many records a single compromise can reach. This directly supports limiting breach impact and, in this case, potential liability tied to the number of affected individuals. This conclusion is an inference from ISACA's risk-reduction principles around isolation, exposure control, and documenting exposure.
Option B is incorrect because database normalization improves data structure and reduces redundancy; it is not primarily a breach-liability reduction control.
Option C is incorrect because database harmonization is about consistency or integration across datasets, not limiting exposure in a breach.
Option D is incorrect because database optimization focuses on performance and efficiency, not on minimizing the number of PII records exposed in a security incident.
Therefore, A is the best answer because segmentation is the option that most directly reduces the scope of exposure in a breach and therefore helps limit liability based on affected individuals.
References (Official ISACA):
* ISACA, Best Practices for Setting Up a Cybersecurity Operations Center - recommends prioritizing assets and isolating high-value asset networks.
* ISACA Journal, Reporting on GDPR Compliance to the Board - emphasizes documenting exposure and relevant risk controls for privacy risk reporting.
* ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - supports governance approaches to limiting privacy exposure. (Referenced conceptually from prior ISACA privacy guidance.)

NEW QUESTION: 118
□□ □□□ □□ □□□□□ □□□□□ □□□□ □□ □ □□ □□□ □□ □ □□□□ □ □□□?
A. □□□ □□ □□□ □□□□□.
B. □□□ □□ □□(DLP) □□□ □□□□□.
C. □□□□□ □□□ □□□ □□□ □□□□ □□□ □□□□□□.
D. □□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The first step to successfully implement a corporate data classification program is to approve a data classification policy. A data classification policy is a document that defines

the objectives, scope, principles, roles, responsibilities, and procedures for classifying data based on its sensitivity and value to the organization. A data classification policy is essential for establishing a common understanding and a consistent approach for data classification across the organization, as well as for ensuring compliance with relevant regulatory and contractual requirements.
Selecting a data loss prevention (DLP) product (option B) is not the first step to implement a data classification program, as it is a technical solution that supports the enforcement of the data classification policy, not the definition of it. A DLP product can help prevent unauthorized access, use, or disclosure of sensitive data by monitoring, detecting, and blocking data flows that violate the data classification policy.
However, before selecting a DLP product, the organization needs to have a clear and approved data classification policy that specifies the criteria and rules for data classification.
Confirming that adequate resources are available for the project (option C) is also not the first step to implement a data classification program, as it is a project management activity that ensures the feasibility and sustainability of the project, not the design of it. Confirming that adequate resources are available for the project involves estimating and securing the necessary budget, staff, time, and tools for implementing and maintaining the data classification program. However, before confirming that adequate resources are available for the project, the organization needs to have a clear and approved data classification policy that defines the scope and objectives of the project.
Checking for the required regulatory requirements (option D) is also not the first step to implement a data classification program, as it is an input to the development of the data classification policy, not an output of it.
Checking for the required regulatory requirements involves identifying and analyzing the applicable laws, regulations, standards, and contracts that govern the protection and handling of sensitive data. However, checking for the required regulatory requirements is not enough to implement a data classification program; the organization also needs to have a clear and approved data classification policy that incorporates and complies with those requirements.
Therefore, option A is the correct answer.
References:
Data Classification: What It Is and How to Implement It
Create a well-designed data classification framework
7 Steps to Effective Data Classification | CDW
Data Classification: The Basics and a 6-Step Checklist - NetApp
Private and confidential February 2021 - Deloitte US

NEW QUESTION: 119
□ □□□□ □□□ □□ □□□ □□ □□ □□□□ □□□ □□ □□ □□□□□ □□□ □□□. □□ □ □□ □ □□□ □□□□ □□□□□?

A. □□ □□□ □□ □□□ □□□□□ □□□□ □ □□□□.
B. □□ □□ □□□□ □□□□□ □□□ □□ □□□□□□.
C. □ □□□□ □□ □□ □□□□ □□□ □□ □□ □□□ □ □□□□.
D. □ □□□□□ □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
A distributed security administration system is a system that allows different administrators to manage the security of different parts of the network or organization. This can provide more flexibility, scalability, and efficiency than a centralized system, where one administrator is responsible for the entire security. However, a distributed security administration system also presents some potential challenges and risks, such as: Inconsistency and conflict among different security policies and standards Lack of coordination and communication among different administrators Difficulty in monitoring and auditing the overall security status and performance Increased complexity and cost of security management and maintenance Therefore, the greatest potential concern for implementing a distributed security administration system is that the security procedures may be inadequate to support the change. Security procedures are the rules and guidelines that define how security is implemented and enforced in an organization. They include policies, standards, processes, roles, responsibilities, controls, and metrics. Security procedures should be aligned with the business objectives, risks, and requirements of the organization, as well as the best practices and regulations in the industry. Security procedures should also be reviewed and updated regularly to reflect the changes in the environment, technology, and threats.
If the security procedures are not adequate to support the change from a centralized to a distributed security administration system, the organization may face increased security risks, such as unauthorized access, data breaches, compliance violations, reputation damage, and financial losses. Therefore, it is essential to ensure that the security procedures are revised and adapted to suit the new system, and that they are communicated and enforced effectively across the organization.
References:
1: Security in Distributed System - GeeksforGeeks
2: Distributed System Security Architecture - Wikipedia
3: Distributed Systems Security: Issues, Processes and Solutions

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

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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 122
□□□□ □□ □□□ □□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□□□ □ □□□□□. □□ □□ □□ □□□ □□□□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 123
IT □□□□ □□ □□□ □□□ □□□ □□□ IS □□□□ □□ □□□ □□□ □□□ □ □□□□ □□□□. □□ □ □□□□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □□□ □□□□□□.
B. □□□□□□ □□□□□ □□□□□□.
C. □□ □□□□□ □□□□□.
D. □□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
IT □□□□□ □□ □□ □□, □□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□□ □□ □□□ □□□□□□. □□ □ □□ □□□ □□□□ □□ □ □ □□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □ □□□ □□□ □□□ □ □□□□□□.
B. □□□ □□□ □ □□□□ □□ □□ □□□ □□□□□ □□□.

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

NEW QUESTION: 125
□□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□ □□
B. □□□ □□□ □□□ □□□ □□
C. □□ □□□□ □□□□ □□□ □□
D. □□ □□□ □□□□ □□□□□ □□
Answer: (SHOW ANSWER)
Incremental backups are backups that only copy the data that has changed since the last backup, whether it was a full or incremental backup. The main reason to use incremental backups is to minimize the backup time and resources, as they require less storage space and network bandwidth than full backups. Incremental backups can also improve key availability metrics, such as recovery point objective (RPO) and recovery time objective (RTO), but that is not their primary purpose. Reducing costs associated with backups and increasing backup resiliency and redundancy are possible benefits of incremental backups, but they depend on other factors, such as the backup frequency, retention policy, and media type. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION: 126
□□□ □□□□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□□. □ □□□ □□□ □ □□ □□□□ □□ □□□□□ □□□□ □ □ □□ □□□□□?
A. □□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□.
B. □□□□ □□□ □ □□ □□ □□ □□□ □□□□□.
C. □□□□ □□□□ □□□□□ □□ □□ □□ □□□ □□□ □□□□□ □□□.
D. □□□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The most important thing for incident management to focus on when addressing an issue that causes an outage is restoring the system to operational state as quickly as possible. Incident management is the process of detecting, investigating, and resolving incidents that disrupt or degrade a service or system. An incident is an unplanned event that affects the normal functioning or quality of a service or system. An outage is a type of incident that causes a complete loss of service or system availability. The main goal of incident management is to restore the service or system to its operational state as quickly as possible, minimizing the impact on users and business operations.
*The other options are not as important as option B. Analyzing the root cause of the outage to ensure the incident will not re-occur is a valuable activity, but not the most important

thing for incident management to focus on when addressing an issue that causes an outage. Root cause analysis is a process of identifying and eliminating the underlying factors that caused an incident or problem. Root cause analysis can help to prevent or reduce the likelihood of similar incidents or problems in the future. However, root cause analysis is usually performed after the incident has been resolved and the service or system has been restored. Ensuring all resolution steps are fully documented prior to returning the system to service is a good practice, but not the most important thing for incident management to focus on when addressing an issue that causes an outage. Documentation is a process of recording and maintaining information about an incident and its resolution steps. Documentation can help to improve communication, accountability, learning, and improvement within incident management. However, documentation should not delay or interfere with the restoration of the service or system. Rolling back the unsuccessful change to the previous state is a possible solution, but not the most important thing for incident management to focus on when addressing an issue that causes an outage.
Rolling back is a process of reverting a change that has been applied to a service or system that caused an incident or problem. Rolling back can help to restore the service or system to its previous state before the change was made.

NEW QUESTION: 127
□□ □□□ □□ □□□ □□□ □□ □□□ □□ □ □□□□.
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: 128

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

A. Wi-Fi Protected Access 3 (WPA3)

B. □□□ □□□ □□(DES)

C. □□ □□ □□ □□ □□(WEP)

D. □□ □□ □□(SSL)

Answer: A (LEAVE A REPLY)

Wireless security relies onstrong encryptionto prevent unauthorized access and data interception.

Option A (Correct):WPA3is thelatest and most secureWi-Fi encryption standard, offeringstronger protectionagainst brute-force attacks and improvingkey management.

Option B (Incorrect):DES is outdatedand vulnerable tomodern attacks, making it unsuitable for wireless security.

Option C (Incorrect):WEP is highly insecuredue toweak encryptionand can be cracked inminutesusing basic tools.

Option D (Incorrect):SSL secures web traffic, notwireless networks.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coverswireless security, encryption, and network security best practices.

NEW QUESTION: 129

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

A. □□□□ □□□□ □□□□ □□□□ □

B. □□ □□□□□□ □□ □□ □□

C. □□□□□□ □□□(DBA)□ □□□□ □□ □□

D. □□□□□□□□ □□□□ □□□□ □□

Answer: D (LEAVE A REPLY)

Understanding the business process flow is crucial as it provides insights into how different applications and organizational functions use and update the database fields in real-time. This perspective helps the auditor validate that appropriate business approvals are in place for these use cases.

References

ISACA CISA Review Manual 27th Edition, Page 128-129 (Business Process Flow)

NEW QUESTION: 130

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

A. □□ □□ □□□(IPS) □ □□□

B. □□□ □□ □□(DLP) □□

C. □□□ □□

D. □□□ □□ □□□□□ □□

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

NEW QUESTION: 131
□□ □ □□□ □□□□□□ □□□□□ □□□□ □ □□ □□□ □□ □□ □□□ □□ □□□?
A. □□□ □□□ □□□□ □□ □□
B. □□ □□□ □□□ □□ □□ □□
C. □□□□ □□□ □□□ □□ □ □□ □□
D. □□ □□□ □□□ □□□□□□ □□ □□
Answer: (SHOW ANSWER)
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 and ExplanationsDatabase, Question ID 216

NEW QUESTION: 132
□□ □□ □□□□ IS □□□□ □□ □ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□□□. □□□ □□□□ □□□□ □□ □□□ □□ □ □□ □□ □□□□ □□□?
A. □□□□□□(KPI)
B. □□ □□ □□□□(MAD)
C. □□ □□ □□(RPO)
D. □□ □□ □□(MTTR)
Answer: B (LEAVE A REPLY)
The primary factor to determine system criticality within an organization is the maximum allowable downtime (MAD). MAD is the maximum time frame during which recovery must become effective before an outage compromises the ability of an organization to achieve

its business objectives and/or survival. MAD reflects the business impact of a system outage onthe organization's operations, reputation, compliance, and finances. MAD can help to prioritize system recovery efforts, allocate resources, and establish recovery objectives.

NEW QUESTION: 133
□□ □□□ □□ □□□ □□ □□□□ □□□□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□□. □□ □□□□ □□□ □□□ □□□ □□ □□□□□ □□□ □ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □□ □□
B. □□ □□□ □□□ □□ □□
C. □□ □□ □□□ □□ □□□□ □□ □□
D. □□ □□□ □□□□ □□□□ □□ □□
Answer: (SHOW ANSWER)
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 and 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: 134
□□ □ □□ □□□ □□□□ □□ □□□ □□□□□?
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: 135
□□ □ □□□□□ □□□□ □□□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □ □□□□□?
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: 136
□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□. □□ □□□ □□□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □□ □□ □ □□ □□□ □ □□ □□ □□□□□?
A. □□□ □□ □□ □□□□ □□□□ □□ □□ □□ □□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□□□□ □□ □ □□□□□□□ □□□□□ □□□ □□□.
C. □□□ □□ □ □□ □□□ □□□□ □□ □□ □□□ □□□□□ □□□□□.
D. □□□□□□□ □□□ □□□ □□ □□ □□□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide

direct evidence of the system's functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete. References: CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 137
□□ □□□ □□□□ □□□ □□□□ □ □□□ □□□□□□□□ □□□□ □□□□□ □. □□ □ □□□□ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□ □□□□□□□.
B. □□ □□□ □□□□□.
C. □□□ □□□□ □□□□□.
D. □□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed in-Depth Explanation:
Implementing edit checks ensures data validity and integrity by verifying inputs and reducing inconsistencies in the database.
Updating the data dictionary (Option A) does not resolve inconsistency issues. Data modeling (Option C) and training (Option D) are less relevant to addressing data accuracy directly.
ISACA CISA Reference: Domain 4 - Information Systems Operations, Maintenance, and Support

NEW QUESTION: 138
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: 139
□□□□ □□ □ □□ □□□ □□ □□□□□ □□ □□, □□ □□□ □□□□ □□□ □ □□□ □□□□ □□ □□ □□ □□□ □□ □ □□□□□?
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: 140
□ □□ □□□ □□□ □□ □□□ □ □□□ □□ □□ □□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□ □□ □□□□□. □□ □ □□ □□□ □□ □□□□ □ □ □□ □□□□□?
A. □□ □□ □□□□ □□□ □□ □□□□□ □□□ □□□ □ □□□□.
B. □□ □□ □□□ □□ □□□ □□□□ □□□ □ □□□□.
C. □□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□□.
D. □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□ □ □□□□.

Answer: (SHOW ANSWER)

The greatest concern is regulatory noncompliance arising from cross-border data processing and storage.

ISACA guidance on cloud data sovereignty states that when data is stored across multiple jurisdictions, organizations must navigate complex legal and regulatory challenges, including conflicting national laws and cross-border transfer restrictions. This is especially important for financial organizations, which often operate under stricter regulatory obligations regarding customer data, outsourcing, and location of processing.

Option A is correct because the key risk in extending cloud servers into several foreign countries is that the outsourced processing arrangement may violate applicable regulations or create conflicts among data protection, financial-sector, and jurisdictional requirements. ISACA notes that data sovereignty means data is governed by the laws of the country where it is stored, and that organizations must ensure compliance when cloud data spans borders.

Option B is not the greatest concern. Distributed server deployment can introduce integrity challenges, but ISACA's cross-border cloud guidance emphasizes the legal and governance burden far more directly than integrity degradation as the primary risk.

Option C is incorrect because data classification does not become invalid merely because data is stored overseas. Classification remains an internal governance concept, although handling requirements may change depending on jurisdiction. ISACA specifically recommends maintaining strong data classification systems alongside legal and compliance review for cross-border cloud use.

Option D is also not the greatest concern. Data ownership and responsibility should be clarified contractually, but ISACA identifies legal compliance and jurisdictional conflicts as the dominant governance risk in cross- border cloud environments.

Therefore, A is the best answer because regulatory exposure from cross-border outsourced processing is the most significant concern in this scenario.

References (Official ISACA):

* ISACA, Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage.
* ISACA Journal, Data Owners' Responsibilities When Migrating to the Cloud.
* ISACA Journal, Addressing the Challenges of IT Audits by Supreme Audit Institutions.

NEW QUESTION: 141

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

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 ReviewManual (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: 142
□□ □ □□□ □□□ □□□ □ IS □□□□ □□ □□□□ □□□□ □ □□□ □□□□ □?
A. □□□□ □□□□ □□□□ □□□□□.
B. □□□ □□ □□□□□□ □□ □□□□□.
C. □□□ □□□ □□ □□ □□□ □□□□ □□□□.
D. □□□ □□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 143
□□ □□□ □□□□ □□ □□□ □□□□□□□ □□ □□ □□□□ □□□□ □□□□ □ □□□□ □□□□. □□ □ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
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: 144
□□ □ □□ □□□ □□□□ □□ □□□□□?
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: 145
□□ □□ □□□ □□ □□ □□□□ □□ □□ □□□□□ □□□□ □□□ □□, □□ □ □□ □□□□ □□ □ □□ □□□ □□□ □□□□□?
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 - TheAuditor 2
Internal Audit Follow Ups: Are They Really Worth The Effort

NEW QUESTION: 146
□□ □□ □□ IT □□ □□□□□ □□□□ □ □□ □ □□ □□ □□□□ □□□?
A. □□□ □□
B. □□□ □□
C. □□ □□ □□(EVA)
D. □□ □□□□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 147
□□□□ □□ □□□ □□ □□□□ □□□□ □□□□□ □□ □□ □□□□ □□□ □□ □□ □□ □□ □ □□□ □□□□□□. □□ □ □□□ □□□□ □□ □□ □□□ □□□ □□?
A. □□ □□□ □□
B. □□□ □□ □□
C. □□ □□□
D. □□ □□ □ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
□□ □□ □ □□□ □□□ □□ □□□□□ □□□ □□□ □□□□□ □ □, □□ □ □□ □ □□ □□ □□□□ □□□?
A. □□□ □□
B. □□□□ □□ □□□
C. □□ □□
D. □□ □□□□
Answer: (SHOW ANSWER)
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: 149
□□□ □□ □□□□□ □□□ □ □□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□□□
B. □□□ □□□ □□□
C. □□□□ □□ □□ □□

D. □□□ □□ □□ □□

Answer: (SHOW ANSWER)

Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.

To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.

The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.

References:

ISACA, CISA Review Manual, 27th Edition, 2020, page 247

Data Classification: What It Is and Howto Implement It

NEW QUESTION: 150

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

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

B. □□ □□ □□□ □□ □□□□ □□ □□□□□.

C. □□□ □□□□□ □□ □□□□ □□ □□□□□□□.

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

Answer: A (LEAVE A REPLY)

A mature risk management program ensures that risk assessmentsdirectly influence decision-makingto align IT risks with business objectives.

Risk Assessment Results Used for Decision-Making (Correct Answer - A)

Demonstrates that risk management is embedded in business processes.

Enables proactive risk mitigation strategies.

Example:A company identifies a cybersecurity risk and delays the launch of a new cloud service until additional controls are in place.

Risk Owner Evaluating All Risk Attributes (Incorrect - B)

Important, but risk management is a shared responsibility.

Metrics Dashboard Approved by Management (Incorrect - C)

A useful tool, but does not indicate effective risk management.
Regular Updates to the Risk Register (Incorrect - D)
Keeping records updated is necessary but not a strong indicator of maturity.
References:
ISACA CISA Review Manual
COBIT 2019: Risk Governance
ISO 31000 (Risk Management Framework)

NEW QUESTION: 151
□□ □□□ □□□□ □□□ □□ □□, □□□□□ □ □□□□ □□□□□ □□□□□□ □. □□ □ □ □□□ □□ □□□ □□□□□□ □□□□(EA) □□□ □□□□□? (CISA □□□ - □□ □□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□□□□□.)
A. □□ □□□□
B. □□□ □□□□
C. □□ □□ □□□□
D. □□□□□□ □□□□
Answer: (SHOW ANSWER)
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, aswell 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. Apost-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 mayalso introduce some risks such as loss of control, dependency, or security breaches over the system implementation process

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 152
□□ □ IT □□□□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□ □□ □□□□ □□ □□ □□□ □□
B. □□□ □□ □□ □□(SDLC) □□□□ □□
C. □□ □□□□ IT □□□□ □□ □□ □□□□
D. □□ □□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 153
□□ □ □□ □□□□ □□□ □□□□□□□ □□□□ □□□ □ □□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
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: 154
□□ □ □□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□ □□□□□?
A. □□ □□□□ □□ □□ □ □□ □□ □□
B. □ □□□□□ □□□□ □□□□ □□ □□ □□
C. □□ □□□□ □□ □□ □ □□
D. □□ □□□ □□ □□□□ □□
Answer: C (LEAVE A REPLY)
The best source of information for an IS auditor to use as a baseline to assess the adequacy of an organization' s privacy policy is the local privacy standards and regulations. Privacy standards and regulations are legal requirements that specify how personal data should be collected, processed, stored, shared, and disposed of by organizations. By using local privacy standards and regulations as a baseline, the IS auditor can ensure that the organization's privacy policy complies with the applicable laws and protects the rights and interests of data subjects. Historical privacy breaches and related root causes, globally accepted privacy best practices, and benchmark studies of similar organizations are useful sources of information for improving an organization's privacy policy, but they are not as authoritative and relevant as local privacy standards and regulations. References: CISAReview Manual (Digital Version): Chapter 2 - Governance and Management of Information Technology

NEW QUESTION: 155
□□□□□□ □□□ □□ □□(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: 156
□□□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□ □□ □□□(IS) □□□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□ □ □□ □□□□ □□□ □□ □□□□ □. □□ □□□ □□□□ □□ □□ □□□□ □□ □ □□ □□□ □□ □□ □□□□ □□ □?
A. □□□ □□□ □□□ □ □□ □□□ □□□□□.
B. □□ □□□ □□ □□□□□ □□□□□□.
C. □□ □□ □□ □□□□□ □□□ □□□□□□.
D. □□□□□ □ □□ □□□ □□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The best action that audit management should consider first is to reassign the audit to an internal audit subject matter expert. This is because cloud service audits require specialized knowledge and skills to assess the risks and controls associated with the cloud service provider and the cloud service customer. An IS auditor who is unfamiliar with the technologies in use and their associated risks to the business may not be able to perform an effective and efficient audit, and may miss important issues or provide inaccurate recommendations.
Therefore, it is important to ensure that the IS auditor assigned to the cloud service audit has the appropriate competence and experience.
The other options are not as good as reassigning the audit to an internal audit subject matter expert.

Conducting a follow-up audit after a suitable period has elapsed may not address the quality issues of the initial audit, and may also delay the identification and remediation of any problems. Rescheduling the audit assignment for the next financial year may expose the organization to unnecessary risks and may not meet the audit objectives or expectations. Extending the duration of the audit to give the auditor more time may not be feasible or cost-effective, and may not guarantee that the auditor will acquire the necessary knowledge and skills in time.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1391
ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, p. 14

NEW QUESTION: 157
□□ □ □□ □□ □□□□□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□□ IT □□□ □□
B. □□ □□□ □□ □□□□ □□
C. □□□□□ □□ □□□ □□
D. □□ □□□ □□ □□□ □□
Answer: B (LEAVE A REPLY)
The correct answer is B. Management's commitment to information security.
Management's commitment to information security is the most critical factor for the success of an information security program, as it provides the leadership, support, and resources needed to establish and maintain a secure environment.
Management's commitment to information security can be demonstrated by:
Setting the vision, mission, and goals for information security, and aligning them with the organization's strategies and objectives1.
Establishing and enforcing the policies, standards, and procedures for information security, and ensuring compliance with relevant laws and regulations1.
Allocating sufficient budget, staff, and technology for information security, and investing in training and awareness programs2.
Promoting a culture of security within the organization, and engaging with stakeholders and partners to foster trust and collaboration2.

NEW QUESTION: 158
□□□ □□ □□ □□□□□□□ □□□ □□ □ □□ □□□ □□□□ □□□ □□ □□ (DLP) □□ □□□ □□□□□?
A. □□□□□ DLP
B. □□□□ □□ DLP
C. □□□□ □□ DLP
D. □□□□□ □□ DLP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 159
□□ □□□ □□ □□ □□□ □□□□ □, □□□□ □□□□(AI) □□□□□ □□□□ □ □ □□□□ □□□□□□. □□□□ □□□ □□ □□□□ □ □□□ □□□ □□□□□. □□ □ □ □□□ □□□□ □□ □□ □□□ □□□□□?
A. AI□ □□ □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
B. □□ □□□□ AI □□□ □□□□ □□□ □□□□□.
C. □□ AI □□□ □□ □□□ □□□ □□□□□.
D. □□ □□□ AI□ □□ □□□ □□ □□ □□□□□ □□□□□□.
Answer: D (LEAVE A REPLY)
If the audit team lacks the necessary knowledge to audit a system that uses an AI algorithm, engaging external consultants who have audit experience and knowledge of AI would be the best approach12. These consultants can provide the expertise needed to effectively audit the AI system12. This approach ensures that the audit is conducted thoroughly and accurately, without requiring the audit team to acquire new skills or knowledge12.
References:
Auditing Guidelines for Artificial Intelligence - ISACA
An In-Depth Guide To Audit AI Models - Censius

NEW QUESTION: 160
□□ □□□(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: 161
□□□ IT □□ □□□□□ □□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □, IS □ □□□ □□ □ □□ □□□ □□ □□ □□ □□ □□□□ □□□?

A. □□□ □□□ □□ □□ □□□ □□□□□□□.
B. □□ □□□ □ IT □□ □□□□□ □□□ □□ □ □□□ □□□□□.
C. □□ □□ □ □□ □□□□ □□ □□□ □□ □ □□□ □□□□□.
D. □□ IT □□□ □□ □ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The first thing that an IS auditor should recommend when an organization is made aware of a new regulation that is likely to impact IT security requirements is to determine which systems and IT-related processes may be impacted. This is because the impact assessment is a crucial step to understand the scope and magnitude of the changes that the new regulation may entail, as well as the potential risks and gaps that need to be addressed. The impact assessment can help the organization to prioritize and plan the necessary actions and resourcesto comply with the new regulation in a timely and effective manner12.
Updating security policies based on the new regulation is not the first thing to do, because it requires a clear understanding of the impact and implications of the new regulation, which can only be obtained after conducting an impact assessment. Updating security policies without an impact assessment may result in incomplete, inconsistent, or ineffective policies that may not meet the regulatory requirements or the organizational needs12.
Evaluating how security awareness and training content may be impacted is not the first thing to do, because it is a secondary or supporting activity that depends on the results of the impact assessment and the policy updates. Evaluating security awareness and training content without an impact assessment or policy updates may result in inaccurate, outdated, or irrelevant content that may not reflect the regulatory requirements or the organizational expectations34.
Reviewing the design and effectiveness of existing IT controls is not the first thing to do, because it is a monitoring or assurance activity that follows the implementation of the changes based on the impact assessment and the policy updates. Reviewing IT controls without an impact assessment or policy updates may result in misleading, incomplete, or invalidfindings that may not capture the regulatory requirements or the organizational performance

NEW QUESTION: 162
□□ □□□□□ □□ □□□ □□□□ □, □□ □ □□ □□ □□ □ □□ □□□□□?
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: 163
□□ □ □□□ □□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□ □ □□□□□?
A. □□ □□□ □□ □□ □□□□ □□ □ □□□□.
B. □□ □□□ □□□□ □□ □□□ □□□□.
C. □□ □□□ □□□□ □□□□ □□□ □□ □□□□□.
D. □□ □□□ □□□ □ □□ □□□ □□ □□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
The best answer is C. Changes are approved after being moved to production.
ISACA guidance on change management emphasizes reviews, testing, approvals, and segregation of duties before moving changes forward. If changes are moved into production before approval, the organization has effectively bypassed one of the most important preventive controls in the change process. That creates direct risk of unauthorized, untested, or harmful changes reaching production.
Option A is a documentation weakness. Option B reduces efficiency and prioritization discipline. Option D is a concern for emergency changes, but it is still less severe than routinely approving changes only after implementation. In audit terms, post-production approval represents a fundamental control breakdown.
References (Official ISACA):
* ISACA Journal, Speeding Up Software Delivery With Effective Change Management.

NEW QUESTION: 164
□□ □ □□□ □□□□ □□□ □□ □□□□□ □□□□ □□ □□□□□?
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: 165

□□□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□□?

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

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

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

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

Answer: D (LEAVE A REPLY)

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: 166
□□ □ □□□ □□□□ □□ □□□□□ □□□ □ □□ □ □□□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□□□ □□□□□□ □□ □□ □□
B. □□ □□□ □□□□□□ □□ □□ □□
C. □□□□ □□□□ □□□□□□ □□ □□ □□□
D. □□ □□□□ □□□□□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
Write access to production program libraries presents the greatest risk when granted to a new member of the system development staff. Production program libraries contain executable code that runs on live systems and supports critical business functions. Write access allows a user to modify or delete existing programs, or add new programs to the library. If a user were to make unauthorized or erroneous changes to production programs, it could cause serious disruptions, errors, or security breaches in the organization's operations.
Therefore, writeaccess to production program libraries should be restricted to authorized personnel only, and subject to strict change management controls.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 167
□□ □ IS □□□□ □□ □ □□□ □□□□ □□ □□□ □□□□□?

A. □□ □□□□ □□□ □□□□ □□□ □□□□□□ □□□ □□□□ □□
B. □□ □□□□□□ □□□ □□□□ □□
C. □□□□ □□□ □□□□ □□□□□ □□□□□ □□
D. □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The primary reason for an IS auditor to conduct post-implementation reviews is to determine whether project objectives in the business case have been achieved. A post-implementation review is an audit activity that evaluates whether a project has delivered its expected outcomes or benefits in accordance with its objectives, scope, budget, and schedule. A business case is a document that defines and justifies the need, value, and feasibility of a project. A post-implementation review can help assess whether project objectives in the business case have been achieved by comparing actual results with planned expectations and identifying any gaps or deviations. The other options are not primary reasons for conducting post-implementation reviews, as they do not measure whether project objectives in the business case have been achieved. Ensuring key stakeholder sign-off has been obtained is a project closure activity that confirms that all project deliverables have been completed and accepted by key stakeholders, but it does not evaluate whether project objectives in the business case have been achieved. Aligning project objectives with business needs is a project initiation activity that ensures that the project is aligned with the organization's strategy, goals, and priorities, but it does not evaluate whether project objectives in the business case have been achieved. Documenting lessons learned to improve future project delivery is a project learning activity that captures and shares the knowledge, experience, and feedback gained from the project, but it does not evaluate whether project objectives in the business case have been achieved. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

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

NEW QUESTION: 169
□□□ □□□ □□ □□□ □□□ □ □□ □ □□ □□□ □□ □□□□ □□□□ □□□?
A. □□ □□□□
B. □□ □□
C. □□ □□□□ □□

D. □□□ □□ □□□(UAT) □□

Answer: (SHOW ANSWER)

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

NEW QUESTION: 170

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

A. □□ □□

B. □□ □□

C. □□ □□

D. □□ □□

Answer: A (LEAVE A REPLY)

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: 171

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

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 and Explanations Database, question ID 3335

NEW QUESTION: 172
□□ □□ □□ □□□ □□ □□ □□ □□□(IS) □□ □□□□ □□ □□ □□□(CIO)□ □□□□ □□□ □□ □□□□□ □□□□ □ □ □□ □□□ □□□□□ □□□ □□□□ IS □□□ □□□□ □□□□□ □□□□□ □□□ □□ □□□□□. □ □□ □□ □□□ □ □□ □ □□□ □□ □□ □□ □□□?
A. □□ □□□ □□ □□□□ □□ □□ □□□□ □□□□□□.
B. □□□□□□□(COO)□□ □□□ □□ □□□ □□□□ □□ □□□□□□.
C. □□ □□□□ IS □□□ □□□□□.
D. □□ □ IS □□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
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: 173
□□ □ □□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□ □ □□ □ □□□□ □□□ □□ □□□□□ □□ □ □□□□?
A. □□ □□
B. □□□ □□
C. □□□ □□
D. □□□ □□
Answer: A (LEAVE A REPLY)
The best method to reduce the risk associated with the transition to a new system using technologies that are not compatible with the old system is parallel changeover. Parallel

changeover is a method of system conversion that involves running both the old and the new systems simultaneously for a period of time, until the new system is verified to be working correctly and completely. Parallel changeover can help reduce the risk of data loss, errors, or disruptions that may occur due to the incompatibility of the technologies, as well as provide a backup option in case of failure or malfunction of the new system. Parallel changeover can also help users compare and validate the results of both systems, and facilitate their training and adaptation to the new system.
Modular changeover is a method of system conversion that involves replacing one module or component of the old system with a corresponding module or component of the new system at a time, until the entire system is replaced. Modular changeover can help reduce the complexity and scope of the conversion, as well as minimize the impact on the users and operations. However, modular changeover may not be feasible or effective when the technologies of the old and new systems are not compatible, as it may create integration or interoperability issues among the modules.
Phased operation is a method of system conversion that involves implementing the new system in stages or increments, each with a subset of functions or features, until the entire system is operational. Phased operation can help reduce the risk and cost of implementing a large and complex system, as well as allow for testing and feedback at each stage. However, phased operation may not be suitable or efficient when the technologies of the old and new systems are not compatible, as it may require extensive modifications or adaptations to enable partial functionality.
Pilot operation is a method of system conversion that involves implementing the new system in a limited or controlled environment, such as a department or a location, before rolling it out to the entire organization.
Pilot operation can help test and evaluate the performance and usability of the new system, as well as identify and resolve any issues or problems before full-scale implementation. However, pilot operation may not be relevant or reliable when the technologies of the old and new systems are not compatible, as it may not reflect the actual conditions or challenges of operating both systems concurrently.
References:
TRANSITION TO THE NEW SYSTEM - O'Reilly Media 1
10 Challenges To Think About When Upgrading From Legacy Systems - Forbes

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

Low-priority jobs typically involve non-critical processes or tasks that do not immediately impact business operations. The best approach to handling such jobs is to schedule them subject to resource availability. This ensures that high-priority tasks can access resources when needed without being affected by the execution of low-priority tasks.
Avoiding Low-Priority Jobs (Option A)is not feasible because even low-priority tasks may be necessary for maintenance or support activities.
Including Major Functions in Low-Priority Jobs (Option B)contradicts the classification of " low-priority " because major functions are usually critical.
Allocating Optimal Resources to Low-Priority Jobs (Option C)is inefficient as resources should primarily be allocated to high-priority tasks.
Scheduling based on resource availability optimizes the use of resources, avoids unnecessary delays in high- priority activities, and ensures that low-priority tasks are executed without disrupting overall operations. This aligns with best practices in IT resource management and scheduling.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 175
□□ □ □□ □ □□ □□ □□□ □□□ □ □□ □□□□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□ □□ □□□
B. □□ □□ □ □□ □□□□ □□.
C. □□□ □□ □□ □□□ □□
D. □□ □□ □□□ □□ □□ □□□ □□
Answer: C (LEAVE A REPLY)
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but they do not directly address the issue of repeated incidents.
References: ISACA ITAF 3rd Edition Section 3600

NEW QUESTION: 176
□□□□ □□□□□□□ □□□□□□□ □ □ □□ □□ □□□ □□□□□. □□ □□ □□ □□□□ □□ □□□□ □ □ □□□□□ □□ □□ □ □□□ □□ □ □□ □□□□ □ □□□□□?
A. □□ □□ □□ □□ □ □□□□ □□□□
B. □□□□□□ □□ □□□□ □□ □□
C. □□□□□□ □□ □□ □□
D. □□ □□□□ □□ □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 177
□□ □□□(IS) □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□□ □□□□. □□□□ □□ □□□ □□ □ □□ □□□□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□□ □□□□□ □□ □□□ □□□□.
B. □□□□□ □□□□□ □□□□ □□ □□□□.
C. □□□□ □□□ □□ □ □□□□.
D. □□□ □□ □□□ □□□ □□□□□□□□□.
Answer: A (LEAVE A REPLY)
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: 178
□□ □ IT □□ □□□□□ □□□□ □□□ □□ □□□□ □□ □□□□□?
A. □□□□ □□ □□ □□□ □□ □□□ □□
B. □□□ □□ □ □□ □□ □□
C. □□ □□□ □□□□□ □□ □□
D. IT □□ □ □□□□□ □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 179
□□□□ □□□□□□□ □□ □□□ □□□ □□□□□, □□□ □□□□ □□□ □□□ □□ □□□□□ □□□□□□. □□ □ BEST □□□ □□□□□ □□□□□□ □□□□ □□ □□□□□?
A. □□□□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□□.
B. □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□.
C. □□ □□□□□ □□□□□ □□ □□□□ □□□ □□□□ □□□□□□.
D. □□ □□□ □□ □□□□ □□□□ □□□□ □□□□□.

Answer: B (LEAVE A REPLY)
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 theprocess 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 differentformats, standards, or timeliness than the internal data

NEW QUESTION: 180
□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□□ □□ □□□ □□ □□□ □□
B. □□□ □□ □□ □□
C. □□ □□ □□ □□
D. IT □□□ □□□ □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 181
□□ □ IS □□□□ □□ □□□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□ □ □□□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□
B. □ □□ □
C. □□ □□
D. □ □□

Answer: C (LEAVE A REPLY)
Hash totals are a control technique used to ensure data integrity during batch processing. A hash total is a calculated value based on the data in a batch. This value is compared to a pre-calculated hash total to confirm that all data has been processed correctly and without alteration.
References
ISACA CISA Review Manual (27th Edition): Hash totals are discussed within the context of batch processing controls.
Other Auditing Resources: Hash totals are a fundamental control technique discussed in various audit and information security publications.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 182
□□ □ □□ □□□ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
□□□□ □□□ □□□□□?
A. □□□□□ □□□ □□□□ □□□ □□ □□
B. □□ □□□ □□□□□ □□□ □□□ □□□□ □□
C. □□□□ □□□ □□□ □ □□□□ □□ □□
D. □□□ □□ □□□ □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 183
□□□ □□□ □□ □□□ □□□ □□ □□□ □□ □ 24□□ □□□ □□ □□□ □□□ □ □□□. □□ □ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□□ □□ □□ □□□ □□□□□□.
B. □□ □□□ □□□ □□□□ □□ □□ □□ □□(KPI)□ □□□□□.
C. □□ □□ □□□(IDS)□ □□ □□□ □□□□□□.
D. □□ □□ □□ □□ □□□□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The best recommendation to facilitate compliance with the regulation that requires organizations to report significant security incidents to the regulator within 24 hours of identification is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, procedures, and tools for managing security incidents effectively and efficiently.
Including the requirement in the incident management response plan can help ensure that security incidents are identified, classified, reported, and escalated in accordance with the regulation. The other options are not as effective as including the requirement in the incident management response plan, as they do not address all aspects of incident management or compliance. Establishing key performance indicators (KPIs) for timely identification of security incidents is a monitoring technique that can help measure and improve the performance of incident management processes, but it does not ensure compliance with the regulation.
Enhancing the alert functionality of the intrusion detection system (IDS) is a technical control that can help detect and notify security incidents faster, but it does not ensure compliance with the regulation. Engaging an external security incident response expert for incident handling is a contingency measure that can help augment the organization's internal capabilities and resources for managing security incidents, but it does not ensure compliance with the regulation. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2

NEW QUESTION: 184
IS □□□□ □□□ DevSecOps □□ □□□ □□□□ □□□□. □□ □ □□□ □□□ □ □ □□□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. CI/CD(□□□□ □□/□□□□ □□) □□□□ □□ □□ □□ □□□ □□
B. □□□□ □□ □□□ □□□ CI(Continuous Integration/Continuous Delivery)□ □□ /CD) □□□□
C. □□□□□□ □□□ □□ □□ □ □□□ □□
D. □□ □□ □□□□□ □ □□□□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□ □ □□□ □□□ □□□□.
A. □□□□□□ □□□□ □□□□□□□.
B. □□ □□□ □□ □□□ □□□□ □□□□□□.
C. □□□ □□ □□□ □□□□□□□.
D. □□□ □□□□□ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system is whether the user requirements were met. User requirements are the specifications and expectations of the users of the system, such as the features, functions, performance, quality, and security of the system. User requirements are usually defined and documented in the early stages of the system acquisition process, such as in the request for proposal (RFP) or the contract. User requirements are also used as the basis for testing and evaluating the system before and after implementation.
Determining whether the user requirements were met can help the IS auditor assess whether the system is fit for purpose and delivers value and benefits to the users and the organization. Determining whether the user requirements were met can also help the IS auditor identify any gaps, issues, or problems with the system that may affect its functionality, usability, or reliability. Determining whether the user requirements were met can also help the IS auditor provide feedback and recommendations for improvement or enhancement of the system.
Stakeholder expectations were identified is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a prerequisite or input for it.
Stakeholder expectations are the needs and wants of the various parties who have an interest or influence in the system, such as users, managers, customers, suppliers, regulators, or auditors. Stakeholder expectations are usually identified and analyzed in the initial stages of the system acquisition process, such as in the feasibility study or the business case. Stakeholder expectations are also used as inputs for defining and prioritizing the user requirements.
Vendor product offered a viable solution is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather an outcome or result of it. Vendor product is the system that is provided by an external supplier or service provider to meet the user requirements. Vendor product offered a viable solution means that the vendor product satisfied or exceeded the user requirements and delivered value and benefits to the users and organization. Vendor product offered a viable solution can be determined by comparing and evaluating the user requirements and the vendor product performance and quality.

Test scenarios reflected operating activities is not the most important thing for the IS auditor to determine in a post-implementation review of a recently purchased system, but rather a factor or criterion for it. Test scenarios are sets of conditions or situations that are used to test and verify whether the system meets the user requirements. Test scenarios reflected operating activities means that test scenarios simulated or replicated real-world scenarios that occur during normal operations of business processes or functions that use or depend on the system. Test scenarios reflected operating activities can help ensure that test results are valid, reliable, and relevant.
References:
Post Implementation Review: How to conduct and its Benefits 1
Post-implementation reviews - Department of Prime Minister and Cabinet 2 How To Conduct A Post Implementation Audit of Your RecentlyInstalled System 3

NEW QUESTION: 186
□□ □ □□□□ IT □□□□□ □□□ □□ □□□ □□□ □□□□□?
A. IT □□□□□□ □□□□□ □ □□ □□□□ □□□□□ □□□□□.
B. IT □□□□□ □□□□□ □□□□ □□□□□.
C. IT □□□□□□ □□□□ □□ □□□ □□ □□□□□□□.
D. IT □□□□□□ □□ □□ □□□□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 187
□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□□. □□ □ □□ □□□ □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□□ □□ □□□ □□□□ □□□ □ □□□□.
B. □□□□□ □□ □□ □□□□□.
C. □□□ □□ □□ □□ □□ □□□□ □□□□.
D. □□□□ □□□□□ □□ □□□ □□□ □□ □□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
□□□□ □□□□ □□□ □ □□□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□ □?
A. □□□□ □□
B. □□□□□□ □□□□(EA)
C. □□□□ □□□ □□(BCP)
D. □□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 189

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

A. □□□□ □□□ □□□□ □□ □□□ □□□□□.

B. □□ □□□ IS □□ □□□□ □□□□□□.

C. □□□□ □□ □□□□ □□□□□□.

D. □□□□□ □□□ □□□□□□.

Answer: (SHOW ANSWER)

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: 190

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

A. □□□□□ □□□□ □□□ □□□ □ □

B. □ □□□ □□ □□ □□ □□ □□

C. □ □□ □□□□ □□□ □□□ □□

D. □□□ □□ □□□ □□□□ □□ □□ □□

Answer: C (LEAVE A REPLY)

The percent of issues resolved by the first contact, also known as the first contact resolution (FCR) rate, is a metric that measures the effectiveness and efficiency of the IT help desk services. It indicates how many customer support issues are resolved on the first interaction with the IT help desk, without requiring any follow-up calls, emails, chats, or escalations. The FCR rate is calculated by dividing the number of issues resolved on the first contact by the total number of customer support issues, and multiplying by 100%1.
The FCR rate is the best indicator of service quality among the four monthly performance metrics, because it reflects the following aspects of the IT help desk services:
Customer satisfaction: Customers are more likely to be satisfied with the IT help desk services if their issues are resolved quickly and effectively on the first contact, without having to wait for a response or repeat their problem to multiple agents. A high FCR rate can improve customer loyalty, retention, and advocacy2.
Cost efficiency: Resolving issues on the first contact can reduce the operational costs of the IT help desk services, such as labor costs, phone costs, or overhead costs. A high

FCR rate can also increase the productivity and utilization of the IT help desk agents, as they can handle more issues in less time3.
Service level: Resolving issues on the first contact can improve the service level of the IT help desk services, such as reducing the average handle time (AHT), increasing the service level agreement (SLA) compliance, or decreasing the backlog of unresolved issues. A high FCR rate can also enhance the reputation and credibility of the IT help desk services4.
Therefore, an IS auditor should review the FCR rate as a key performance indicator (KPI) of the IT help desk services, and compare it with the industry standards and benchmarks. According to MetricNet's benchmarking database, the FCR industry standard is 74 percent. This number varies widely, however, froma low of about 41 percent to a high of 94 percent5. An IS auditor should also recommend ways to improve the FCR rate, such as: Training and empowering the IT help desk agents to handle a wide range of issues and provide accurate and consistent solutions Implementing a knowledge base or a self-service portal that provides relevant and updated information and guidance for common or simple issues Improving communication and collaboration between different departments or teams that may be involved in resolving complex or escalated issues Using feedback and analytics tools to monitor and measure customer satisfaction and identify areas for improvement

NEW QUESTION: 191
□□ □□□(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: 192
□□ □□□ □□□□ □□ □□□ □□□□□□□ □□ □□ □□□□ □□□□ □□□□ □ □□□□ □□□□. □□ □ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□□□□ □□□ □□□□ □□□□.
B. □□ □□□□□ □□□□□ □□□□□.
C. □□□ □□□ □□□□□□ □□□□.
D. □□□ □□□□ □□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
□□□ □□□(PKI)□□ □□□ □ □□□ □□□□ □□ □□□(IS) □□□□ □□ □□□ □ □□□□□ □□□□ □ □□□ □□ □ □□□□□?
A. □ □□ □□□ □□ □□
B. □□ □□□□□ □□□□□ □□ □□
C. □□ □□ □□ □□ □□
D. PKI □□ □□
Answer: C (LEAVE A REPLY)
The best answer is C. Reviewing key compromise detection activities.
In a PKI, the greatest practical risk in key management is failure to detect and respond when keys are compromised. If compromise is not detected promptly, confidentiality, integrity, authentication, and nonrepudiation can all be undermined. ISACA materials discussing PKI and cryptographic transition stress the importance of certificate revocation, rollout strategies, and careful key management because compromise of keys directly affects trust in the system.
Option D is important, but documentation alone does not prove that compromise can be detected in practice.
Option B may help monitoring, but it is narrower than the broader control objective of detecting compromised keys. Option A is not a core audit concern in comparison. From a CISA perspective, the most important focus is whether the organization can detect, contain, and revoke trust when keys are exposed or misused.
References (Official ISACA):
* ISACA Journal, Building Resilient Security in the Age of Quantum Computing - discusses PKI key management complexity and certificate revocation as critical control considerations.

NEW QUESTION: 194
□□ □□ □□ □□□ □□ □□□ □□□□□□□ □□ □□ □□□ □□ □□ □□□□ □□□□, □□□ □□ □□ □□□ □□□□ □□□ □□□□□. □□□ □□□□ □□ □ □□ □□□ □□□□□ □□□□?
A. □□□
B. □□□
C. □□
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 195
□□ □ □□ □□□ □□□□ IT □□ □□□ □□□ □ □□ □□□□ □□□ □□□□□?
A. □□ □□□□□ □□□ □□□□ □□□□□.
B. □□□ IT □□ □□□ □□□□ □□□□□.
C. □□□ IT □□□ □□ □□ □□□□ □□□□ □□□□□.
D. □□□ □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
The most concerning thing for an IS auditor reviewing an IT strategy document is that the strategic IT goals are derived solely from the latest market trends. An IT strategy document is a blueprint that defines how an organization will use technology to achieve its goals. It should be based on a thorough analysis of the organization's internal and external factors, such as its vision, mission, values, objectives, strengths, weaknesses, opportunities, threats, customers, competitors, regulations, and industry standards. An IT strategy document should also align with the organization's business strategy and reflect its unique needs and capabilities. If an IT strategy document is derived solely from the latest market trends, it may not be relevant or appropriate for the organization's specific situation. It may also lack coherence, consistency, feasibility, or sustainability.
The other options are not as concerning as option C. Target architecture is defined at a technical level is not a concern for an IS auditor reviewing an IT strategy document. Target architecture is the desired state of an organization's IT systems in terms of their structure, functionality, performance, security, interoperability, and integration. Defining target architecture at a technical level can help an IS auditor to understand how the organization plans to achieve its strategic IT goals and what technical requirements and standards it needs to follow. The previous year's IT strategic goals were not achieved is not a concern for an IS auditor reviewing an IT strategy document. The previous year's IT strategic goals are the outcomes that the organization intended to accomplish with its IT initiatives in the past year. Not achieving these goals may indicate some challenges or gaps in the organization's IT performance or execution. However, this does not necessarily affect the quality or validity of the current IT strategy document. An IS auditor should focus on evaluating whether the current IT strategy document is realistic, measurable, achievable, relevant, and time-bound.

Financial estimates of new initiatives are disclosed within the document is not a concern for an IS auditor reviewing an IT strategy document. Financial estimates are projections of the costs and benefits of new initiatives that are part of the IT strategy document. Disclosing financial estimates within the document can help an IS auditor to assess whether the new initiatives are aligned with the organization's budget and resources and whether they provide value for money. References: IT Strategy Template for a Successful Strategic Plan | Gartner, Definitive Guide to Developing anIT Strategy and Roadmap - CioPages, An Example of a Well-Developed IT Strategy Plan - Resolute

NEW QUESTION: 196
□□□□ □□ □□ □□□□ □□□□□□□ □□□ □□□ □□□□□□ □□□ □□ □ □□ □□□□ □□□□□ □□□□□□. □□ □□(Protected Audit)□ □□□□ □□□□ □□ □□ □□□(IS) □□□□ □□ □ □□□ □□ □□ □□□□ □□□?
A. □□□ □□□□□ □□ □□□□ □□□□□.
B. □□ □□□ □□□□ □□□ □□□□ □□□□□.
C. □□□ □□□□ □□□ □□□□ □□□□□□.
D. □□□□ □□□□ □□□□ □□□□□ □□□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Understanding the specific agile methodology that will be followed is the first step that an IS auditor should do to ensure the effectiveness of the project audit. An IS auditor should familiarize themselves with the agile approach, principles, practices, and tools that will be used by the project team, as well as the roles and responsibilities of the project stakeholders. This will help the IS auditor to identify and assess the relevant risks and controls for the project audit. The other options are not the first steps that an IS auditor should do, but rather possible subsequent actions that may depend on the specific agile methodology. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.3.21
CISA Review Questions, Answers and Explanations Database, Question ID 211

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 197
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: 198
□□□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□.
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: 199
□□□ IT □□□□ DevOps□ □□□□ □□ □□□□□ □□□□ □□□ □□□ □□□ □ □□□ □□□□ □□ □□ □□□ □□ □□□ □ □□ □□□□□. □□ □ □□ □□□ □ □□ □□□ □□□□□?
A. □□□ □□□□ □□ □ □□□□ □□ □ □□□ □□□□□□.
B. DevOps □□ □□□ □□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□□ □.
C. □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □ □□□□ □□□□□.
D. IT □□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 200
□□ □ □□ □□ □ □□ □□□ □□□ □□ □□ □□□□ □□□□ □ □□ □□□□ □ □□ □□□□□?
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: 201
□□ □ □□□□ □□□□ □□ □□□□ □□ □ □□□□□□ □□□ □□□ □□ □□ □□ □□□ □□ □□□□ □□□ □ □□ □□□ □□□□□?
A. □□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□□.

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

NEW QUESTION: 202
□□□ □□□□ □□□ □□□□□?
A. □□ □□□ □□□□ □□□□□
B. □□□ □□□□□ □□□□ □□□
C. □□□□□□ □□□□□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 203
□□□ □□□□ □□□□ □□□□ □□ □ □□ □□ □□□ □□ □□ □□□□ □□□ □□?
A. □□□□ □□□ □□ □□ □□□
B. □□□ □□ □□ □□□
C. □□ □□□ □□□□□
D. RAID(□□ □□□□ □□ □□)
Answer: C (LEAVE A REPLY)
A virtual tape library (VTL) is a disk-based backup system that emulates a tape library. It provides faster backup and recovery than traditional tape systems, and it can be integrated with data deduplication and replication technologies to enhance disaster recovery. A VTL can also be replicated to an offsite location for additional protection. A VTL is the best disaster recovery solution for an environment where data virtualization is used, because it can handle large volumes of data, support multiple backup applications, and provide consistent performance.
Onsite disk-based backup systems (A) are not the best disaster recovery solution, because they are vulnerable to the same risks as the primary data center, such as fire, flood, power outage, or sabotage. Tape-based backup systems (B) are not the best disaster recovery solution, because they are slow, prone to errors, and require manual intervention.
Redundant array of independent disks (RAID) (D) is not a backup system, but a storage technology that improves performance and fault tolerance by distributing data across multiple disks. RAID does not protect against data corruption, human error, or malicious attacks.
References:
Virtualization Disaster Recovery Overview: Definitions and Guides
Disaster Recovery Virtualization - VMware
What is Virtual Disaster Recovery? - Definition from Techopedia
How Does Virtualization Help With A Disaster Recovery Plan

NEW QUESTION: 204
□□□ □□ □ □□□ □□ □□□□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □ □ □ □□□□□?
A. □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□.
B. □□ □□ □ □□ □□ □□□ □□□□□ □□□□.
C. □□ □□ □□□ □□ □□□ □ □□ □□□□ □□□ □□□ □□□.
D. □□ □□□ □□ □□ □□□□□□(CMDB)□ □□□□.
Answer: B (LEAVE A REPLY)
The greatest concern to an IS auditor who is assessing an organization's configuration and release management process is that changes and change approvals are not documented. This is because documentation is essential for ensuring the traceability, accountability, and quality of the changes made to the configuration items (CIs) and the releases deployed to the production environment. Without documentation, it would be difficult to verify the authenticity, validity, and authorization of the changes, as well as to identify and resolve any issues or incidents that may arise from the changes. Documentation also helps to maintain compliance with internal and external standards and regulations, as well as to facilitate audits and reviews.
The other options are not as concerning as option B, although they may also indicate some weaknesses in the configuration and release management process. The organization does not use an industry-recognized methodology, but this does not necessarily mean that their process is ineffective or inefficient. The organization may have developed their own methodology that suits their specific needs and context. However, using an industry-recognized methodology could help them adopt best practices and improve their process maturity. All changes require middle and senior management approval, but this may not be a problem if the organization has a clear and streamlined approval process that does not cause delays or bottlenecks in the change implementation. However, requiring too many approvals could also introduce unnecessary complexity and bureaucracy in the process. There is no centralized configuration management database (CMDB), but this does not mean that the organization does not have a way of managing their CIs and their relationships. The organization may use other tools or methods to store and access their configuration data, such as spreadsheets, documents, or repositories. However, having a centralized CMDB could help them improve their visibility, accuracy, and consistency of their configuration data.
References:
1: The Essential Guide to Release Management | Smartsheet
2: 5 steps to a successful release management process - Lucidchart
3: Configuration Management process overview - Micro Focus
4: Release and Deployment Management process overview - Micro Focus

NEW QUESTION: 205

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

A. □□□□ 24□□ □□□□ □□□ □□□□□ □□□.

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

C. □□□□□□ □□ □□□ □□□□□ □□□□ □□□.

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

Answer: C (LEAVE A REPLY)

Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:
CISA Review Manual (Digital Version), Chapter 5, Section 5.51
CISA Review Questions, Answers and Explanations Database, Question ID228

NEW QUESTION: 206

□□□□ PC□ □□ □□□□ □ □□□□□ □□□□□□ □□□ □□□□ □□□□. □ □ □ □□ □ □□□ □□□□□?

A. □□□□ PC□ □□□ □□□□□□□.

B. □□□□□□ □□□ □□□ □□□ □ □□□□.

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

D. □□□ □□□ □ □□□□□ □□□□ □ □□□□.

Answer: (SHOW ANSWER)

The major advantage of moving from many desktop PCs to a thin client architecture is that desktop application software will never have to be upgraded. A thin client architecture is a type of client-server architecture that uses lightweight or minimal devices (thin clients) as clients that connect to a central server that provides most of the processing and storage functions. A thin client architecture can offer several benefits over a traditional desktop PC architecture, such as lower cost, higher security, easier maintenance, etc. One of these benefits is that desktop application software will never have to be upgraded on thin clients, as all the applications are installed and updated on the server, and accessed by thin clients through a network connection. This can save time and money for installing and upgrading software on individual devices, and ensure consistency and compatibility among different devices. The security of the desktop PC is enhanced is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one.

A thin client architecture can enhance the security of desktop PCs by reducing the exposure orvulnerability of data and applications on individual devices, and centralizing the security management and control on the server. However, this advantage may depend on other factors such as network security, server security, user authentication, etc.
Administrative security can be provided for the client is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can provide administrative security for clients by allowing administrators to configure and manage client devices remotely from the server, and enforce policies and restrictions on client access or usage. However, this advantage may depend on other factors such as network reliability, server availability, user compliance, etc.
System administration can be better managed is a possible advantage of moving from many desktop PCs to a thin client architecture, but it is not the major one. A thin client architecture can improve system administration by simplifying and streamlining the tasks and activities involved in maintaining and supporting client devices, such as backup, recovery, troubleshooting, etc., and consolidating them on the server.
However, this advantage may depend on other factors such as network bandwidth, server capacity, user satisfaction

NEW QUESTION: 207
□□□□□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □□ □ □□ □□□ □□□□ □□□□.
A. □□□ □□ □□.
B. □□ □□□ □□ □□□ □□□ □□□□□□.
C. □□ □□ □□□□ □□□□□.
D. □□ □□ □□□□ □□ □□.
Answer: A (LEAVE A REPLY)
The best way to determine whether programmers have permission to alter production data is to review the access rights that have been granted. In audit terms, the question is asking whether the programmers are authorized to perform a specific action in production. The most direct evidence of that authorization is the actual privileges assigned to their accounts or roles. ISACA access-control guidance consistently focuses on granted access, segregation of duties, and restricting direct production or database access.
Option A is correct because granted rights directly show whether programmers can update, modify, or otherwise alter production data. If those privileges are present, the permission exists; if not, it does not. This is more direct than reviewing configuration or implementation history.
Option B is not the best answer because reviewing how recent changes were implemented may indicate whether developers were involved in production changes, but it does not directly confirm whether they currently have permission to alter production data. It is indirect evidence.

Option C is also weaker than A. Access control system configuration may reveal how permissions are structured, but the clearest evidence is still the actual rights granted to the programmers or their roles.
Option D is incorrect because log settings show what may be recorded, not what access is authorized. Logs may help detect misuse, but they do not define whether permission exists.
Therefore, A is the best answer because reviewing granted access rights is the most direct and reliable way to determine whether programmers can alter production data.
References (Official ISACA):
* ISACA Journal, An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - logical access and direct database access are central audit concerns.
* ISACA Journal, Auditing Amazon Web Services - audit focus includes how access is restricted and how administrative activity is segregated.
* ISACA, Selected COBIT 5 Processes for Essential Enterprise Security - access should be justified, authorized, logged, and monitored.

NEW QUESTION: 208
□□ □□□ □□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□□ □□□ □. □ □□□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□?
A. □□
B. □□
C. □□
D. □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 209
□□ □ □□□ □□□ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□ □□
B. □□□□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 211
□□ □ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □□□□□?
A. □□ □□ □□□□ 1(SHA-1)
B. □□□ □□
C. □□□
D. □□□ □□□
Answer: C (LEAVE A REPLY)
Encryption is the process of transforming information into an unreadable form using a secret key, so that only authorized parties can access it. Encryption would protect the confidentiality of information sent in email messages, as it would prevent unauthorized parties from intercepting and reading the messages. Secure Hash Algorithm 1 (SHA-1) is a cryptographic hash function that produces a fixed-length output from an input.
SHA-1 does not encrypt information, but rather verifies its integrity by detecting any changes or modifications. Digital signatures are electronic signatures that use encryption and hash functions to authenticate the identity of the sender and the integrity of the message. Digital signatures do not protect the confidentiality of information, but rather ensure its authenticity and non-repudiation. Digital certificates are electronic documents that contain the public key and identity information of an entity, such as a person, organization or device. Digital certificates are issued by trusted third parties called certificate authorities (CAs). Digital certificates do not protect the confidentiality of information, but rather enable secure communication and encryption by verifying the identity and public key of an entity. References:
[Encryption Definition]
[Secure Hash Algorithm 1 (SHA-1) Definition]
[Digital Signature Definition]
[Digital Certificate Definition]

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 212
□□ □ □□ □□□□□□□ □□□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□ □□□ □□□ □□
B. □□□ □ □□ □□
C. □□□□□ □□ □□
D. □□□ □□ □□

Answer: B (LEAVE A REPLY)
The primary advantage of using virtualization technology for corporate applications is to achieve better utilization of resources, such as hardware, software, network and storage. Virtualization technology allows multiple applications to run on a single physical server or device, which reduces the need for additional hardware and maintenance costs. Virtualization technology also enables dynamic allocation and reallocation of resources according to the demand and priority of the applications, which improves efficiency and flexibility. The other options are not the primary advantage of using virtualization technology, although they may be some of the benefits or challenges depending on the implementation and configuration. References:
ISACA, CISA Review Manual, 27th Edition, chapter 4, section 4.21
ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.23

NEW QUESTION: 213
□□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□.
A. □□ □□ □□.
B. □□ □□ □□ □□.
C. □□ □□ □□□□.
D. □□□□□□ □□□□(EA).
Answer: C (LEAVE A REPLY)

NEW QUESTION: 214
□ □□□ IT □□ □□ □□□ □□□□□□. □□ □□ □□□□ □□□□□□ □□□□□ □□□ □ □□ □□□ □□ □ □□□□□?
A. IT □□□
B. □□□ □□
C. □□ □□
D. □□□□□□ □□
Answer: C (LEAVE A REPLY)
Segregation of duties (SOD) is a core internal control and an essential component of an effective risk management strategy. SOD emphasizes sharing the responsibilities of key business processesby distributing the discrete functions of these processes to multiple people and departments, helping to reduce the risk of possible errors and fraud1.
SOD is especially important in IT security, where granting excessive system access to one person or group can lead to harmful consequences, such as data breaches, identity theft, or bypassing security controls2. SOD breaks IT-related tasks into four separate function categories: authorization, custody, recordkeeping, and reconciliation1. Ideally, no one person or department holds responsibility in multiple categories.
In a role-based environment, where access privileges are granted based on predefined roles, it is important to ensure that the roles are designed and assigned in a way that

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

NEW QUESTION: 215
□□ □ □□ □□ □□□□□ □□ □□□ □□□ □□□□□?
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: 216
IS □□□□ □□ □□ □□□□□ □□ □ □□ □□□□ □□□□ □□□ □□ □□□ □ □ □□□□ □□□□□ □□□ □□□□□. □□ □ □□ □□ □□□ □□□□ □ □□ □ □□ □□□ □□□□□?
A. □□□ □□ □□
B. □□ □□(QA) □□□
C. □□ □□□ □□□□□ □□□ □□
D. IT □□□ □□ □ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 217
□ □□□ □□□□ □□ □ □□ □□ □□□ □□□(VLAN) □□ □□□□ □□□□□□ □□□.
VLAN □□□ □□ □□□ □□ □□□ □□□□□?
A. □□□
B. □□
C. □□
D. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 218
□□ □ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□□□ □□□□□.
B. □□□□□ □□□□ □□ SIEM □□□□ □□□ □□□□□.
C. □□ □□□ □□□ □□ □□ □□□ □□□ □□
D. □□□□□ □□□□ □□□□□□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 219
□□ □ □□□ □□ □□ □ □□□ □□(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: 220
□□ □ □□ □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□□ □ □□ □□ □□ □□□□□ □□ □□□□□.
B. □□□ □□□□□□□ □□ □□□ □□□□ □□ □□□□□□ □□ □□□ □□□□ □□.
C. □□ □□□ □□ □□ □□□ □□□□ □□□ □□□□ □□□□□□.
D. □□□ □□□ □□ □□□□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Maintaining an onboarding and annual security awareness program is the best way to prevent social engineering incidents because it can educate the users about the common techniques and tactics used by social engineers and how to avoid falling victim to them. Ensuring user workstations are running the most recent version of antivirus software, including security responsibilities in job descriptions and requiring signed acknowledgment, and enforcing strict email security gateway controls are all good security practices, but they do not directly address the human factor that is exploited by social engineering.
References:
ISACA, CISA Review Manual, 27th Edition, 2020, p. 3671
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2

NEW QUESTION: 221
□□ □ □□ □□ □□□ □□ □□ □ □□ □□□ □□□ □□□ □□ □ □□□□□?
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 and Explanations Database,Question ID 223

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

NEW QUESTION: 223
□□□ □□ □□□ □□(BCP)□ □□□ □□□ □□□.
A. □□ □□ □□ □□ □□□□□□□□□.
B. □□□ □ □□□□ □□ □□ □□ □ □□□□□□□□.
C. □□□ □□□□□□□ □□□ □□□ □□□□□□.
D. □□ □ □□ □□□ □□ □□□□□□□□□.
Answer: D (LEAVE A REPLY)
A BCP must stay current with organizational changes to ensure its effectiveness during a disruption.
Personnel changes and environmental updates are directly relevant to how the BCP would be executed.
References
ISACA CISA Review Manual (Current Edition) - Chapter on Business Continuity and Disaster Recovery Industry Standards (e.g., ISO 22301, NIST SP 800-34) - Guidelines for maintaining and updating a Business Continuity Plan

NEW QUESTION: 224
□□ □□ □□□ □□□ □ □□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□□□(MTD)
B. □□□□ □□□ □□ □□
C. □□ □□ □□ □□(MTBF)
D. □□ □□ □□(MTTR)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 225
□□ □ □□□□ □□ □□□□□ □□□ □□□ □□ □□□□□?
A. □ □□□□ □□□□ □□□ □□□□ □□□ □□□ □□□□□□□ □□□ □□□□ □.
B. □□□ □ □□□ □□□ □□ □ □□□□ □□□□□ □□□□□□.
C. □□□□ □□□ □□ □□□ □□□□ □ □□□□ □□ □□ □□ □□□□ □□□□ □.
D. □□ □□□ □□ □□□□□ □□ □ □□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)
The system only allows payments to vendors who are included in the system's master vendor list is an example of a preventative control in an accounts payable system. A preventative control is a control that aims to prevent errors or irregularities from occurring in the first place. By restricting payments to vendors who are authorized and verified in the master vendor list, the system prevents unauthorized or fraudulent payments from being made. The other options are examples of other types of controls, such as backup (recovery), reconciliation (detective), and communication (directive) controls. References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION: 226
□□ □ □□ □□ □□□□□ □□□ □□ □□□ □□□ □□□□□?
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's commitment to information security, as they depend on or derive from it. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 227
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: 228
□□□ □□ □□□ □□ □□ □□□ □□□□□□□ □□□□ □, IS □□□□ □□ □ □ □ □□□ □□ □□ □□□□ □□□□ □□□?
A. □□□ □□ □□(SLA)□ □□ □□ □□□ □□ □□□□□.
B. □□ □□□ □□ □□ □□□□ □□□□□□□.
C. □3□ □□ □□ □□□ □□□□□□.
D. □□□ □□□□ □□□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The primary area of focus when an organization decides to outsource technical support for its external customers is to align service level agreements (SLAs) with current needs. SLAs are contracts that define the scope, quality, and expectations of the services provided by the vendor, as well as the remedies or penalties for non-compliance. SLAs are essential for ensuring that the outsourced technical support meets the customer' s requirements and satisfaction, as well as the organization's objectives andstandards. By aligning SLAs with current needs, the organization can specify the key performance indicators (KPIs), metrics, and targets that reflect the desired outcomes and value of the technical support. This can also help to monitor and evaluate the vendor's performance, identify gaps or issues, and implement corrective actions or improvements.

References:
Service Level Agreement (SLA)Examples and Template
What is an SLA? Best practices for service-level agreements

NEW QUESTION: 229
□□ □ □□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□ □?
A. □□□□ □□□ □□□□ □□□ □□□ □□□ □□□.
B. □□□□ □□ □□□ □□□□ □□□.
C. □□□□ □□ □□□□ □□ □□□□□ □□□□□□□.
D. □□□□ □□□□ □□ □□□□ □□□.
Answer: (SHOW ANSWER)
The most effective control over visitor access to highly secured areas is to require visitors to be escorted by authorized personnel. This control ensures that visitors are supervised at all times and do not enter any restricted or sensitive areas without permission. It also allows authorized personnel to verify the identity, purpose, and clearance of the visitors, and to monitor their behavior and activities. Escorting visitors also reduces the risk of tailgating, piggybacking, or unauthorized duplication of access credentials.
Requiring visitors to use biometric authentication, monitoring visitors online by security cameras, and requiring visitors to enter through dead-man doors are all examples of technical controls that can enhance visitor access control, but they are not as effective as escorting visitors. Biometric authentication can provide a high level of identity verification, but it does not prevent visitors from accessing unauthorized areas or compromising security in other ways. Security cameras can provide a record of visitor movements and actions, but they may not deter or detect security breaches in real time. Dead-man doors can prevent unauthorized entry by requiring two-factor authentication, but they do not ensure that visitors are accompanied by authorized personnel.
References:
ISC Best Practices for Facility Access Control1
Visitor Management Best Practices From Top Organizations2
8 Best Practices for Setting Up a Visitor Management System3

NEW QUESTION: 230
□□□ □□ □□ □□□□□□ □□ □□ □ □□ □□□ □□□□ □□□?
A. □□ □□ □□ □ □□
B. □□□□ □□□ □□□□ □□□□□.
C. □□ □□ □□ □ □□□ □□
D. □□ □□ □ □□
Answer: (SHOW ANSWER)
The activities that should be separated are initiating and closing error logs. This is a segregation-of-duties issue. The same person who opens an error record should not also

have sole authority to close it, because that creates an opportunity to suppress incidents, conceal inadequate investigation, or bypass proper resolution and review. ISACA guidance regularly stresses the importance of segregation of duties as a foundational control principle.
Option A is correct because separating initiation from closure helps ensure independent review, proper follow- up, and accountability in the incident process. This aligns with classic CISA logic: one role records or raises the issue, while another role validates resolution and closure.
Option B is less compelling because collecting and analyzing logs are closely related operational security activities and are often performed within the same monitoring function.
Option C is also less appropriate to separate in this context because identifying root causes and recommending workarounds are naturally linked problem-management activities. ISACA guidance on root cause analysis connects these activities to incident and problem handling.
Option D is not the best answer because recording and classifying incidents are typically performed together at intake or triage. Separating them would usually add process friction without the same control benefit as separating initiation from closure.
Therefore, A is the best answer because it best reflects appropriate segregation of duties in incident handling.
References (Official ISACA):
* ISACA Journal, IS Audit Basics: Trust but Verify - highlights the importance of segregation of duties.
* ISACA Journal, Trends, Challenges and Strategies for Effective Audit in a Rapidly Changing Landscape - reinforces segregation of duties as a continuing control requirement.
* ISACA Journal, Resilient GRC: Tackling Contemporary Challenges With a Robust Delivery Model - discusses bias and segregation-of-duties concerns.
* ISACA, Root Cause Analysis / ISACA Glossary - supports the linkage between root cause analysis and incident/problem processes.

NEW QUESTION: 231
□□ □ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□ □□□□□ □□□?
A. □□□ □□ □□□ □□□□ □□□□□.
B. □□□□□□□ □□□□ □□ □□ □□□ □□□□□.
C. □□□ □□□□□□ □□ □□ □□□ □□□□□.
D. □□ □□ □ □□□ □□□ □□ □□.
Answer: B (LEAVE A REPLY)
The correct answer is B. Assessing key controls that support the migration.
ISACA guidance explains that internal audit should be involved in cloud procurement, design, and adoption to identify relevant risks and ensure that appropriate controls are in

place and operating effectively. That is an assurance role, not a management or implementation role.
Option A is incorrect because mitigating risk to an acceptable level is a management responsibility, not an internal audit responsibility. Internal audit evaluates and provides assurance, but should not own risk treatment in a way that impairs independence.
Option C is incorrect because implementing security controls is also a management or operational responsibility, not the auditor's role.
Option D is incorrect because budget and resource impact analysis is primarily a management planning function.
Therefore, the correct answer is B, because internal audit's proper role is to assess whether the key controls supporting the cloud migration are appropriate and effective.
References (Official ISACA):
* ISACA Now Blog, Five Major Auditing Challenges in Cloud Computing and How to Overcome Them
- internal audit should identify cloud risks and ensure appropriate controls are in place and operating effectively.
* ISACA, Now Is the Time for IT Auditors to Perform Advisory Pre-Implementation Reviews
- internal audit provides observations and recommendations to enhance the control environment before deployment.
* ISACA Journal, Digital Trust and the Audit Function - audit acts as assurance for implementation of required practices.

NEW QUESTION: 232
□□ □ □□□□□□ □□□□□ □□□□□(API) □□ □□□ □□□ □□ □□□ □□□ □ □□ □□ □□□ □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□(XML) □□□ □□□□□□.
B. □□ □□ □□(TLS)□ □□□□□.
C. SOAP(Simple Object Access Protocol)□ □□□□□.
D. API □□□□□□ □□□□.
Answer: B (LEAVE A REPLY)
The best recommendation to mitigate the risk of eavesdropping associated with an API integration implementation is to implement Transport Layer Security (TLS). TLS is a cryptographic protocol that provides secure communication over a network by encrypting the data in transit and authenticating the parties involved. TLS can prevent unauthorized parties from intercepting, modifying or tampering with the data exchanged between the API endpoints. Encrypting the XML file, implementing SOAP, and masking the API endpoints are not sufficient to mitigate the risk of eavesdropping, as they do not provide end-to-end encryption or authentication for the API communication. References: IS Auditand Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 233
□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□ □ □□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□□□. □□ □ □□ □□□□ □□ □ □□□ □□□□ □ □□ □□□ □□□□□?
A. □□ □□□ □□□□□□□.
B. □□□□□□□ □□ □□□□ □□□□□□□□.
C. □□□□□□ □□□□ □□□□ □□□ □□□ □□□□□□□.
D. □□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Changing the default configurations of a database system is a critical control for securing it from unauthorized access or exploitation. Default configurations often include weak passwords, unnecessary services, open ports, or known vulnerabilities that can be easily exploited by attackers. The other options are not as important as changing the default configurations, as they do not address the root cause of the security risks. Normalizing tables in the database is a design technique for improving data quality and performance, but it does not affect security. Changing the service port used by the database server is a form of security by obscurity, which can be easily bypassed by port scanning tools. Using the default administration account after changing the account password is still risky, as the account name may be known or guessed by attackers. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.4

NEW QUESTION: 234
□□ □□□□□□ □□ □, □□□ □□□ □□ □ □□□□ □□□□□□ □□ □□□ □ □□□□□□. □□ □ □□ □□□ □□□□ □□□ □ □□ □□□ □□□□□?
A. □□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□□.
B. □□□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□□□□ □□□□□ □□□ □□□□□.
D. IT □□ □□□ □□□□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
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: 235
□□ □ □□□ □□□ □□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□?

A. □□□□□ USB □□
B. □□ □□□ □□□
C. □□ □□ □□(MFA)
D. □□ □□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The greatest risk to laptop computers is data exposure in case of theft or loss. The most effective safeguard is full disk encryption, which ensures that even if the device is stolen, data remains unreadable without the encryption key.
* Disabled USB ports (A): Prevents some forms of data exfiltration but does not protect stored data.
* MFA (C): Protects user authentication but not the data if the disk is removed.
* Passkey phrases (D): Improves authentication strength but is weaker than encryption for data protection.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 5 (Protection of Information Assets), section on endpoint security and encryption controls.

NEW QUESTION: 236
□□ □ □□ □□ □□□□□ □□□□ □□ □ □□□□□ □□ □□□□□?
A. □□ □□ □□□ □□ □□ □□ □□ □□
B. □□ □□ □□□ □□□□ □□ □□□□, □□ □□ □ □□ □□(GRC) □□ □□
C. □□ □□ □□ □□ □□□ □□□□ □□□□□.
D. □□□ □□□□ □□ □□ □□□ □□□□□□□.
Answer: C (LEAVE A REPLY)
Assessing and tracking all compliance audit findings is the best way to support the effectiveness of a compliance program. This allows an organization to identify areas of non-compliance, take corrective action, and monitor improvements over time12. While implementing an awareness plan, using a governance, risk, and compliance (GRC) tool, and monitoring applicable regulations can contribute to a compliance program, they do not provide the same level of continuous improvement and effectiveness as assessing and tracking audit findings.

NEW QUESTION: 237
□□□ □□ □□□□□ □□ □□ □□□□ □□ □□ □ □□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□□□□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)
Impact assessment is an activity that occurs during the issues management process for a system development project. Issues management is a process of identifying, analyzing,

resolving, and monitoring issues that may affect the project scope, schedule, budget, or quality. Impact assessment is a technique of evaluating the severity and priority of an issue, as well as its implications for the project objectives and deliverables. The other options are not activities that occur during the issues management process, but rather related to other processes such as contingency planning, configuration management, or help desk management. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
CISA Review Questions, Answers and Explanations Database, Question ID 217

NEW QUESTION: 238
□□ □ □□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □?
A. □□□□□ USB □□
B. □□ □□□ □□□
C. □□ □□ □□ □□
D. 2□□ □□
Answer: B (LEAVE A REPLY)
The best method to safeguard data on an organization's laptop computers is full disk encryption. Full disk encryption is a technique that encrypts all the data stored on a harddrive, including the operating system, applications, files, and folders. This means that if the laptop is lost, stolen, or accessed by an unauthorized person, they will not be able to read or modify any data without knowing the encryption key or password. Full disk encryption provides a strong level of protection for data at rest, as it prevents data leakage or exposure in case of physical theft or loss of the device.
References:
How to Protect theData on Your Laptop
6 Steps to Practice Strong Laptop Security

NEW QUESTION: 239
□□ □□□□ IT □□□□ IS □□□□ □□□ □□□ □□ □□□ □□□□ □□ □□ □ □□ □□ □□□□□ □□□ □ □□ □□□□□□. □□ □ □□□□ □□ □ □□ □□ □ □□ □□□ □□□□□?
A. □□□□□ □□ □□□ □□□□ □□□ □□□ □□ □□□□□□.
B. □□ □□ □ □□ □□□□ IT □□□□ □□□ □ □□ □□□□□.
C. IT □□□□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□□□ □□□□.
D. □□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 240
□□ □ □□ □□□□(EA) □□□□□ □□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□□□□ □□□ □□□□ □□□□ □□

B. EA□ □□□ □□ □□□□ □□□ □ □□□ □□ □□
C. EA□ □□ □□ □ □□□ □□□□□ □□□□ □□
D. □□□ □□□ □□□ □□ □□□(ROI)□ □□□□□ □□□□ □□
Answer: A (LEAVE A REPLY)
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: 241
□□ □□ □□□ □□ □□□□ □□ □□ □ □□ □□□ □□□□□□□□ □□□ □□ □□ □□□□□□. □□ □□□□ □□ □ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□□ □□□□□.
B. IT □□□□□ □□□□.
C. □□ □□□ □□□□ □□□□□□.
D. □□ □□□ □□ □□□□□ □□□□□□.
Answer: B (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 242

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

A. □□ □□

B. □□□

C. □□ □□□

D. □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 243

□□ □ □□□ □□□□ □□ □□□ □□□□□?

A. □□□□ □□□□ □□ □□□ □□□□ □□

B. □□ □□□ □□□□ □□□□ □□□□ □□□ □□□□ □□

C. □□□ □□ □ □□ □□□ □□□□ □□

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 244

□□ □ □□ □□□□□□□ □□□□□ □□ □□□□□ □□□□ □□□□□□ □□□ □□ □□□□□(API)□ □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □□ □□ □□□□□?

A. API□ □□ □□□ □□□□ □□

B. □□□ □□□□ □□□ □□

C. □□□□□□□ □□ □□ □□□

D. □□□□□ □□□ □□ □□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 245

□□ □ □□□□□ □□ □□□ □□□□□?

A. □□□ □□□ □□□ □□□ □□□□ □□ IP □□□ □□□□□ □□□□□ □□□□ □.

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

C. □□□□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □3□□□ □□□ □□.

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

Answer: A (LEAVE A REPLY)

Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee

into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception. References: [ISACA CISA Review Manual 27th Edition], page 361.

NEW QUESTION: 246
□□□ □□ □□□ □□□ □□□□ AI□ □□ □□□ □□□ □, □□ □□□ □□□□ □ □ □□ □□□ □□□ □□□ □□□.
A. AI □□□□ □□ □□ □□□ □□ □□.
B. AI □□□□ □□ □□ □□ □□.
C. □□ □□□ □□ □□ □□ □□ □ □□□.
D. AI □□□□ □□ □□ □□□ □□□ □□□ □ □□ □□.
Answer: A (LEAVE A REPLY)
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 and CCPA Compliance Guidelines

NEW QUESTION: 247
□□ □□□ □□□, □□ □□□ □□□ □□ □□□ □□□□ □□□□□□ □□□?
A. □□ □□
B. □□□ □□
C. □□ □□

D. □□□ □□

Answer: D (LEAVE A REPLY)

Service accountsare used by applications or systems to perform automated tasks and shouldnot be allowed for interactive login, as they present security risks if compromised.

Service Accounts (Correct Answer - D)

Used for running background tasks (e.g., database services, scheduled jobs).

Should have minimal permissions and be denied interactive logins.

Example:A compromised service account with interactive login could allow attackers to gain system access.

Local Accounts (Incorrect - A)

Local administrator accounts should be restricted but may still be required for some systems.

Administrator Accounts (Incorrect - B)

Should be restricted, but disabling them entirely could lock out system management.

Console Accounts (Incorrect - C)

Console access is sometimes needed for system recovery and troubleshooting.

References:

ISACA CISA Review Manual

NIST 800-63B (Digital Identity Guidelines)

CIS (Center for Internet Security) Best Practices

NEW QUESTION: 248

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

A. □□□□□□ □□□□ □□

B. □□□□□ □□□ □□□ □□

C. □□ □□ □□□□ □□ □□ □□ □□

D. □□□□ □□ □□ □□

Answer: B (LEAVE A REPLY)

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: 249

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

A. □□ □□

B. □□□ □ □□□ □□□ □□□

C. □□□□ □□□ □□(BCP) □□□ □□

D. □□ □□ □ □□

Answer: B (LEAVE A REPLY)

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: 250

□□ □ □□□ □□ □□(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: 251

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

A. □□ □□ □□

B. □□ □□ □□(EVA) □□

C. □□ □□ □□

D. □□□ □□□□

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation:

Earned Value Analysis (EVA) provides a quantitative measure of project progress by comparing planned value, earned value, and actual costs. This gives insight into schedule and budget performance, making it the best tool to assess whether the project is on track.
Critical path (A): Helps in identifying dependencies but not progress.
Work breakdown structure (C): Defines scope but does not measure progress.
Traceability matrix (D): Ensures requirements coverage, not schedule/cost progress.
ISACA Reference: CISA Review Manual 27th Edition, Domain 3 (Information Systems Acquisition, Development, and Implementation), section on project management metrics and monitoring techniques.

NEW QUESTION: 252
□□□□ □□ □□□□ □□□□□□ □□□ □□□□ □□ □□□ □□□ □, □□ □□ □ □□□□ □□□□ □□ □□□ □□□□ □□ □□ □□□□□.
A. □□□□ □□□□ □ □□□□ □□.
B. □□□□□ □□□□ □□□□ □□□□.
C. □□ □□ □□ □□□ □□ □ □□.
D. □□□□ □□ □□□□ □□□ □□□ □□□.
Answer: B (LEAVE A REPLY)
The business process supported by the system is the most important factor for an IS auditor to understand when planning an audit to assess application controls of a cloud-based system. An IS auditor should have a clear understanding of the business objectives, requirements, and risks of the process, as well as the expected outputs and outcomes of the system. This will help the IS auditor to determine the scope, objectives, and criteria of the audit, as well as to identify and evaluate the key application controls that ensure the effectiveness, efficiency, and reliability of the process. The other options are less important factors that may provide additional information or context for the audit, but not its primary focus. References:
CISA Review Manual (Digital Version), Chapter 5,Section 5.31
CISA Review Questions, Answers and Explanations Database, Question ID 212

NEW QUESTION: 253
□□ □ □□□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □ □□□ □ □□□ □□□□□?
A. □□□ □□□□ □□□□ □□ □□□ □□□ □□□□□ □□□□□ □□□□□.
B. □□□ □□□□ □□ □□□ □□ □□ □□□□□ □□□□ □□□□.
C. □□□ □□□ □□ □□□□ □□□□ □□□□ □□□ □ □□ □□□□□.
D. □□□ □□ □□□□ □□□ □□ □□□□□.
Answer: B (LEAVE A REPLY)
The finding that should be of greatest concern to an IS auditor assessing the effectiveness of an organization' s vulnerability scanning program is that results are not reported to individuals with authority to ensure resolution. This indicates a lack of accountability and

communication for vulnerability management, which may result in unresolved or delayed remediation of identified vulnerabilities. This may expose the organization to increased risk of cyberattacks or breaches. The other findings are also concerning, but not as much as this one, because they may affect the completeness, accuracy or timeliness of the vulnerability scanning process, but not necessarily its effectiveness. References:
ISACA, CISA Review Manual, 27th Edition, chapter 4, section 4.41
ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.2

NEW QUESTION: 254
□□ □□□□ □□□□ □ □□ □□ □□ □□□ □□□□□ □□□□□?
A. □ □□ □□
B. □ □□
C. □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)
A mesh configuration provides the greatest fault tolerance. ISACA's glossary explicitly defines mesh topology as "a fault-tolerant topology in which network nodes and endpoints are mostly, if not fully, interconnected." That directly answers the question.
Option D is correct because a mesh topology provides multiple alternate communication paths. If one link or node fails, traffic can often be rerouted through other paths, making the network more resilient than star, ring, or bus topologies.
Option A is less fault tolerant because the central hub or switch can become a single point of failure.
Option B is less fault tolerant because failure in the ring can disrupt communication unless specialized redundancy exists.
Option C is the least fault tolerant among these common topologies because the shared backbone can become a major single point of failure.
Therefore, D is the best answer, and ISACA's glossary directly supports it.
References (Official ISACA):
* ISACA Glossary, Mesh topology - "A fault-tolerant topology..."

NEW QUESTION: 255
□□□□ □□□□□□ □□□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□.
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 and Systems Resources | COBIT, Risk, Governance ... - ISACA, CISACertification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 256
□□ □ □□ □□ □□□ □□ □□□ □□□□ □□□□□□ □□ □□ □□□□ □□□ □ □ □□ □□□□□□?
A. □□ □□□
B. □□ □□
C. □□□□□□
D. □□ □□□□□
Answer: A (LEAVE A REPLY)
Threat modeling is an approach that enables IS auditors to identify, analyze, and mitigate potential security vulnerabilities within an application by understanding the threats, attacks, vulnerabilities, and countermeasures. This proactive technique helps in designing secure applications.
References
ISACA CISA Review Manual 27th Edition, Page 276-277 (Threat Modeling)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 257
□□□ □□□ □□□□□ □□ □□ □□□ □□□□□ □□□□□□ □□□□ □□ □□ □□ □□□ □□□ □□□□.
A. □□ □□ □□(ITF).
B. □□ □□□□□.
C. □□ □□.
D. □□□ □□ □□.
Answer: C (LEAVE A REPLY)
Transaction tagging is a technique by which transactions are marked with unique identifiers or headers and traced through the system using agents or sensors at each

processing point1. Transaction tagging allows for continuous monitoring and analysis of transaction processing in a high-volume, real-time system by providing visibility into the performance, availability, and reliability of each transaction and its components1. Transaction tagging can also help to identify and isolate errors, bottlenecks, anomalies, and security issues in the system1.

NEW QUESTION: 258
IS □□ □□□□ IT □□□ □□□□ □□□ □□ □□□□□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□. □□ □□ □□□ □□□ □□□□□ □□□ □□ □□ □□□ □□□□□□□. □□ □ □□ □ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□
B. □□□ □□□ □□□ □□ □□
C. □□□ □□ □□ □□□ □□□
D. □□□ □□□ □□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 259
IS □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□ □□□ □. □□ □□ □ □□ □□ □□□□ □□□□ □ □□ □□□□□?
A. □□□□ □□ □□□□ □□□□ □□□□.
B. □□□□ □□□ □□□ □□ □□ □□□□ □□□ □□ □□□□□.
C. □□□□ □□□ □□□ □□□□□ □□□□□.
D. □□□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The finding that should be ranked as the highest risk is that network penetration tests are not performed.
Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices.
Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, butnot as risky as the lack of network penetration tests, because they either do not directly affect the networksecurity controls, or they can be addressed by documentation or approval processes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 260

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

A. □□ □□

B. □□□ □□

C. □□□ □□

D. □□□ □□

Answer: D (LEAVE A REPLY)

The most likely application input control that would detect data input errors in the customer account number field during the processing of an accounts receivable transaction is a validity check. A validity check is a type of application control that verifieswhether the data entered in an application matches a predefined set of values or criteria1. For example, a validity check can compare the customer account number entered by the user with a list of existing customer account numbers stored in a database, and reject any input that does not match any of the valid values2.

The other options are not as likely to detect data input errors in the customer account number field, because they do not compare the input with a predefined set of values or criteria. A limit check is a type of application control that verifies whether the data entered in an application falls within a specified range or limit1. For example, a limitcheck can ensure that the amount entered for an invoice does not exceed a certainmaximum value2. A parity check is a type of application control that verifies whether the data entered in an application has an even or odd number of bits1. For example, a parity check can detect transmission errors in binary data by adding an extra bit to the data and checking whether the number of bits is consistent3. A reasonableness check is a type of applicationcontrol that verifies whether the data entered in anapplication is logical or sensible based on other related data or information1. Forexample, a reasonableness check can ensure that the date entered for an order is not in the future or before the date of creation of the customer account2. References:

What are application controls? Definition, examples and best practices1 General Control Vs Application Control: Key Differences and Example ...4 Parity Check - an overview | ScienceDirect Topics

NEW QUESTION: 261

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

A. □□□□□ □□ □□ □□

B. □□ □□□ □□

C. □□□ □□□ □□□□ □□ □□□□.

D. □□□□□□(KPI) □□

Answer: C (LEAVE A REPLY)

An IT service desk is a function that provides technical support and assistance to the users of an organization' s IT systems and services. An IT service desk typically handles issues

such as software installation, hardware troubleshooting, network connectivity, password reset, system configuration,and user training. An IT service desk aims to ensure that the IT systems and services are available, reliable, secure, and efficient for the users.
One of the best indications that there are potential problems within an organization's IT service desk function is an excessive backlog of user requests. A backlog is a list of user requests that have not been resolved or completed by the IT service desk within a specified time frame. An excessive backlog means that the IT service desk is unable to meet the demand or expectations of the users, and that the users are experiencing delays, dissatisfaction, or frustration with the IT service desk.
An excessive backlog of user requests can indicate various problems within the IT service desk function, such as:
Insufficient staff, resources, or capacity to handle the volume or complexity of user requests Ineffective processes, procedures, or tools for managing, prioritizing, or resolving user requests Lack of skills, knowledge, or training among the IT service desk staff to deal with different types of user requests Poor communication, collaboration, or coordination among the IT service desk staff or with other IT functions or stakeholders Low quality, performance, or security of the IT systems or services that cause frequent or recurring user issues Therefore, an excessive backlog of user requests is the best indication that there are potential problems within an organization's IT service desk function.
References:
What is an IT Service Desk? Definition and Functions - Indeed
The Most Common IT Help Desk Issues - SherpaDesk
18 Common IT Help Desk Problems and Solutions - E-Pulse Blog

NEW QUESTION: 262
□□ □□□(IS) □□□□ □□□ □□ □□ □□□□□ □□□□ □□□□. □□ □ □□ IT □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□?
A. □□□ □□
B. □□ □□□(ROI)
C. □□ □□ □□
D. □□ □□ □□ □□□
Answer: A (LEAVE A REPLY)
An organization ' s IT risk appetite should be primarily driven by its strategic objectives. The risk appetite defines the amount and type of risk the organization is willing to pursue or retain to achieve its goals.
Aligning risk appetite with strategic objectives ensures that risk-taking is consistent with the organization ' s mission and vision. While ROI, cost of controls, and the likelihood of risk events are important considerations in risk management, they are factors evaluated within the context of the overarching strategic objectives.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 2: Governance and Management of IT.

NEW QUESTION: 263
□□ □ □□ □□□□ □□□□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□?
A. □□ □□□□ □□(false negative) □□ □□□□□□.
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: 264
□□ □ □□□ □□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□ □□□□□?
A. □□ □□
B. □□ □□□
C. □□ □□□
D. □□ □□□
Answer: (SHOW ANSWER)
The most useful information regarding an organization's risk appetite and tolerance is provided by its risk profile, as this is a document that summarizes the key risks that the organization faces, the potential impacts and likelihoods of those risks, and the acceptable levels of risk exposure for different objectives and activities.
A gap analysis is a tool that compares the current state and the desired state of a process or a system, and identifies the gaps that need to be addressed. Audit reports are documents that present the findings, conclusions, and recommendations of an audit engagement. A risk register is a tool that records and tracks the identified risks, their

causes, their consequences,and their mitigation actions. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.1: IT Governance

NEW QUESTION: 265
□□ □□□□□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□□□□?
A. □□
B. □□
C. □□□□
D. □□□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
Secure code reviews identify security flaws or vulnerabilities in code before deployment. This makes them detective controls, since they help find issues but do not directly prevent or correct them.
Option A: Correct - they detect flaws.
Option B: Corrective controls are applied after issues are detected.
Option C: Monitoring is ongoing observation, not review-based.
Option D: Deterrent controls discourage actions (e.g., policies, warnings), not detect issues.
ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on software development controls and code review practices.

NEW QUESTION: 266
□□ □□□□□□(KPI) □ □□ □□ □□□ □□□□ □□□ □□□ □□ □□□□□□□ □□ □□□ □□□ □□□□ □□ □□□□□?
A. □□ □□ □□□□ □□□ □□□□ □□ □□
B. □□□ □□ □□□ □
C. □□ □□ □□□□ □□ □□□□□ □□
D. □□ □□ □□□□ □□ □
Answer: A (LEAVE A REPLY)
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: 267
□□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□ □?
A. □□□ □□□□□ □□□□□.
B. □□□□ □□□ □□□□□□.
C. □□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 268
□□ □ □□□ □□□□ □□□□ □□□□□□ □□□ □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□ □□ □ □□ □□□ □□ □□ □□□□□?
A. □□ □□ □□□ □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□□□□□.
B. □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □ □□ □□□ □□□□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□□ □□□□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
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: 269
□□ □□□□ □□□□□ USB □□□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□

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

NEW QUESTION: 270
□□□ □□ □□ □ □□ □□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□ □ □□ □□
B. □□ □□ □□□ □□□ □□
C. □□□□ □□ □□
D. □□□ □□□□ □□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
If SoD cannot be fully implemented, an independent review of changes after deployment provides assurance that inappropriate or unauthorized code has not been introduced. Other options either weaken controls or fail to provide adequate oversight.
References (ISACA): COBIT BAI06 (Managed IT Changes).

NEW QUESTION: 271
□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□□.
A. □□□□□□ □□□□(EA)□ □□□□□□.
B. □□□ □□ □□□ □□□□□□□.
C. □□ □□□□ □□□□□ □□□□□□□.
D. □□□ □□ □□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
The primary focus of a post-implementation review is to verify that user requirements have been met. User requirements are specifications that define what users need or expect from a system or service, such as functionality, usability, reliability, etc. User requirements are usually gathered and documented at the beginning of a project, and used as a basis for designing, developing, testing, and implementing a system or service. A post-implementation review is an evaluation that assesses whether a system or service meets its objectives and delivers its expected benefits after it has been implemented. The primary focus of a post- implementation review is to verify that user requirements have been met, as this can indicate whether the system or service satisfies the user needs and expectations, provides value and quality to the users, and supports the user goals and tasks. Enterprise architecture (EA) has been complied with is a possible focus of a post-implementation review, but it is not the primary one. EA is a framework that defines how an organization's business processes, information systems, and technology infrastructure are aligned and integrated to support its vision and strategy. EA has been complied with, as this can indicate whether the system or service fits with the organization's current and future state, and follows the organization's standards and principles. Acceptance testing has been properly executed is a possible focus of a post-implementation review, but it is

not the primary one. Acceptance testing is a process that verifies whether a system or service meets the user requirements and expectations before it is accepted by the users or stakeholders. Acceptance testing has been properly executed, as this can indicate whether the system or service has been tested and validated by the users or stakeholders, and whether any issues or defects have been identified and resolved.
User access controls have been adequately designed is a possible focus of a post-implementation review, but it is not the primary one. User access controls are mechanisms that ensure that only authorized users can access or use a system or service, and prevent unauthorized access or use. User access controls have been adequately designed, as this can indicate whether the system or service has appropriate security and privacy measures in place, and whether any risks or threats have been mitigated.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 272
□□□ □□ □□□ □ □□□□□□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□ □ □□□□□□ □□□□ □□ □□ □ □□ □□□ □□□□□?
A. □□ □□ □□□
B. □□□□ □□ □□
C. □□□□ □3□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
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: 273

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

A. □□□ □□□ □□ □□□ □□□ □ □□□□.

B. □□ □□□□ □□ □□ □□□ □□□□□.

C. □□ □□□ □□ □□ □□□ □□□□□□□.

D. □□ □□□ □□□ □□□□ □□□□ □□ □□□□.

Answer: C (LEAVE A REPLY)

The most important thing for an IS auditor to validate when auditing network device management is that all devices have current security patches assessed. This is because security patches are essential for fixing known vulnerabilities and preventing unauthorized access, data breaches, or denial-of-service attacks on the network devices. If the network devices are not patched regularly, they may expose the network to various cyber threats and compromise the confidentiality, integrity, and availability of the network services and data12.

Devices cannot be accessed through service accounts is not the most important thing to validate because service accounts are typically used for automated tasks or processes that require privileged access to network devices. Service accounts can be secured by using strong passwords, limiting their permissions, and monitoring their activities. However, service accounts alone do not protect the network devices from external or internal attacks that exploit unpatched vulnerabilities3.

Backup policies include device configuration files is not the most important thing to validate because backup policies are mainly used for restoring the network devices in case of failure, disaster, or corruption. Backup policies can help with recovering the network functionality and data, but they do not prevent the network devices from being compromised or attacked in the first place. Backup policies should be complemented by security policies that ensure the network devices are patched and protected4.

All devices are located within a protected network segment is not the most important thing to validate because network segmentation is a technique that divides the network into smaller subnets or zones based on different criteria, such as function, security level, or access control. Network segmentation can help isolate and contain the impact of a potential attack on a network device, but it does not prevent the attack from happening. Network segmentation should be combined with security patching and other security measures to ensure the network devices are secure.

NEW QUESTION: 274

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

A. □□□□□

B. □□□ □□

C. □□ □ □□□(PKI)

D. □□ □□□□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 275

□□ □ IT □□ □□ □□□ □□□□□ □□□□ □□ □□□(IS) □□□□ □□ □□□ □ □ □□□ □□□□□?

A. □□□□□ □□□□□ □□ □□□ □□□□□.

B. □□□□ □□□ □□□ □□ □□ □□□ □□□□□.

C. □□ □□□ □□□ □□□□ □□□ □□□ □□□□.

D. □□□□ □□□ □□□ □□□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 276

□□ □ □□ □□ □□□□ □□ □□□□□ SQL □□□ □□□ □□□ □□ □□□ □ □ □ □□ □ □□□ □□□□□?

A. □□□□ □□□ □□□ □□□□□ □ □□□□.

B. □□□□ □□□ □□□□ □□□ □ □□□□.

C. □□□□ □□□□ □□□ □ □□□□.

D. □□□ □□□□ □□□ □ □□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 277

□□ □ □□□□ □□ □□ □□□□□ □□□□ □□□ □□ □□□ □□□□ □ □□□ □□□ □□□□□□. □□ □□ □□ □□□ □□□ □, □□ □ □□ □□□ □□ □□□ □□□□□?

A. □□□□□ □□□ □□□ □□□ □□ □□□□ □□□□□.

B. □□ □□□□ □□ □□(QA) □□□ □□□ □ □□□ □□□□ □□□□.

C. □□□□ □□ □□□ □□□□□ □□ □□□□.

D. □□ DevSecOps □□□□□ □□□□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

Change control is the process of managing and documenting changes to an information system or its components. Change control aims to ensure that changes are authorized, tested, approved, implemented, and reviewed in a controlled and consistent manner. Change control is an essential part of ensuring the security, reliability, and quality of an information system.

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

NEW QUESTION: 278
□□ □□□(IS) □□□□ □ □□□□□ □□□ □□□□, □□□□ □□□ □□ □□□ □ □ □□□ □□□□ □□□ □□□□□□. □□□□ □□□ □□□ □ □□ □□□ □□ □ □□ □□□□□?
A. □□□ □□□□ □□□□□ □□□ □□ □□□□□ □□□□□□.
B. □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □□□ □□ □□□□ □□□□□□□.
D. □□ □□□ □□□□ □□□□□□□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version.
This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application. An older version of the source code mayalso 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: 279
□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□ □ □□□ □□□□.
A. □□□ □□.
B. □□ □□.

C. □□ □□ □□□.
D. □□ □□ □□□.
Answer: (SHOW ANSWER)
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 and Challenges in IT2 4: Implementing Segregation of Duties: A Practical Experience Based on Best Practices - ISACA1

NEW QUESTION: 280
□□ □ □□□ □□ □ □□□ □□ □□□ □□ □□□□□ □□□□ □□□ □□□□□?
A. □□□ □□ □□(DLP) □□□
B. □□□ □□□□ □□
C. □□□□ □□ □□(NAC)
D. □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 281
□□ □ □□□ □□ □□(QC) □□□□ □□ □□□ □□ □ □□□ □□□□ □□ □□□ □□?
A. □□ □□□ □□
B. □□ □□ □□ □□□ □□
C. □□ □ □□ □□
D. □□ □□ □ □□ □□
Answer: (SHOW ANSWER)
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: 282
□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□□□ □□ □□ □□□ □□□ □ □□□.
A. □□ □□ □□ □□ □□
B. □□□ □□ □□□ □□□□□
C. □□ □□□ □□□ □□□□□ □□□□□.
D. □ □□□□ □□□□□ □□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Ensuring access rules agree with policies is an information systems security officer's primary responsibility for business process applications. An information systems security officer should verifythat the access controls implemented for the business process applications are consistent with the organization's security policy and objectives. The other options are not the primary responsibility of an information systems security officer, but rather the tasks of an application owner, a senior management, or a business analyst.
References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.3.11
CISA Review Questions, Answers and Explanations Database, Question ID 208

NEW QUESTION: 283
□□ □ □□□ □□ □□ □□□□□ □□□□ □□ □ □□□□ □□ □□□□□?
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: 284
□□ □ 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 deskservice, 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 ImportantHelp Desk KPIs to Track and Measure Help Desk Performance

NEW QUESTION: 285

IS □□□□ □□□ □□ □□ □□□□ □3□ □□□□□ □□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□□. □□ □ □□□ □□□ □□□□□ □□□□□ □□□ □□□ □□ □□□□□□ □□ □ □□□□ □□□ □□□□□?

A. □□□ □□ □□(SLA)

B. □□□□ □□ □□ □□

C. □□ □□□ □□□□ □□□□ □□

D. □□ RACI □□

Answer: A (LEAVE A REPLY)

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 and Explanations Database

NEW QUESTION: 286
□□ □□□(IS) □□□□ □□ □□□□ □□ □□□□□□ □□□(DBA)□ □□ □□□ □ □ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□□□□. □□□□ □ □ □ □□□ □□ □□ □□□?
A. □□ DBA□ □□ □□□ □□□ □ □□□ □□□ □□□□□.
B. □□ □□ □□ □□□□ □□□□□
C. □□ □□ □□□ □□□□□ □□□ □□□□□.
D. □□ □□ □□ □□ □□□□□ □□□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
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:
DatabaseAdministrator (DBA) Definition
Segregation of Duties | ISACA
[Compensating Control Definition]

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 287

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

A. □□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
B. □□ □□□ □□ □□□□ □□□□□□.
C. □□ □□ □□□□ □□ □□ □□ □□□□□.
D. □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 288

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

A. □□ □□□ □□□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□ □□ □□□□□.
D. □□□□ □□□□ □□ □□□ □□□□ □□□□□□.

Answer: D (LEAVE A REPLY)

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: 289

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

A. □□□ □□□ □□□ □□ □□□ □□□□□.

□□□ □□ □□□ CISO□□ □□□□□.
B. □□ □□□ □□□ □□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□.
C. □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The completeness of the vulnerability scanning process depends on the accuracy and currency of the organization's systems inventory, which is a list of all the hardware and software assets that are owned or used by the organization. A complete and up-to-date systems inventory can help ensure that all the systems are identified and scanned for vulnerabilities, and that no system is missed or overlooked. Vulnerability scanning results are reported to the CISO is a good practice for ensuring accountability and visibility of the vulnerability management process, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as reporting does not guarantee that all the systems are scanned. The organization is using a cloud-hosted scanning tool for identification of vulnerabilities is a possible option for conducting vulnerability scanning, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as the type of scanning tool does not affect the scope or coverage of the scanning. Access to the vulnerability scanning tool is periodically reviewed is a critical control for ensuring the security and integrity of the vulnerability scanning tool, but it is not the most important thing to verify when determining the completeness of the vulnerability scanning process, as access review does not ensure that all the systems are scanned.

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

NEW QUESTION: 291
□□ □□□ □□ □ □□ □□ □□ □ □□□ □□□□ □□□□□□ □□□□ □ □□ □ □□ □□ □□□□□?
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 detectany 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 customersafter 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 and Examples - Guru99 : What is Integration Testing? Definition, Types, Tools and Examples - Guru99 : What is Acceptance Testing? Definition, Types, Tools and Examples - Guru99

NEW QUESTION: 292
□□ □ □□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□ □□□□ □□ □□ □ □□□ □□□□□?
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: 293
IS □□□□ □□ □□ □ □□□□ □ □□□ □□□ □□□□□ □□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□ □□□□□?
A. □□ □□ □□
B. □□□ □□□
C. □□□ □□□
D. □□□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 294
□□ □□ □□□ □□ IT □□ IT □□□□ □□ □□□□□, □□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□□ □□□□. □□ □ □□ □□□ □□□□ □□ □ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□ IT □□□□ □□□□□□.
B. □□□□ □□□ □□ □□□ □□□□□□.
C. □□ IT □□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□□ □□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
The best course of action for the IS auditor is A. Escalate to IT management for resolution. This is because IT management is responsible for overseeing and coordinating the IT activities and functions within the organization, and ensuring that they comply with the audit findings and recommendations1. IT management can help resolve the issue of finding ownership by:
Clarifying and communicating the roles and responsibilities of each IT team, and how they relate to the finding and its remediation2.
Evaluating and assigning the finding to the most appropriate IT team, based on their expertise, authority, and availability2.

Providing guidance and support to the assigned IT team, and monitoring their progress and performance in remediating the finding2.

NEW QUESTION: 295
□□□ □□□ □□ □ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□ □ □ □□□□?
A. □□ □□□ □□(BCP)
B. □□ □□ □□(RPO)
C. □□ □□ □□(MTTR)
D. □□ □□ □□ □□(MTBF)
Answer: B (LEAVE A REPLY)
A recovery point objective (RPO) is the maximum acceptable amount of data loss after an unplanned data- loss incident, expressed as an amount of time. This is generally thought of as the point in time before the event at which data can be successfully recovered- that is, the time elapsed since the most recent reliable backup1. RPOs are important to consider when reviewing an organization's defined data backup and restoration procedures, because they determine how frequently the organization needs to perform backups, and how much data it can afford to lose in case of a disaster. RPOs are usually defined based on the business impact and criticality of the data, as well as the compliance and regulatory requirements. For example, a financial institution may have a very low RPO (such as a few minutes or seconds) for its transactional data, while a research institute may have a higher RPO (such as a few hours or days) for its experimental data.
The other possible options are:
A). Business continuity plan (BCP): A BCP is a document that outlines how an organization will continue to operate or resume its critical functions and processes in the event of a disruption or disaster. A BCP includes various elements, such as risk assessment, business impact analysis, recovery strategies, roles and responsibilities, communication plan, and testing and maintenance. A BCP is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. A BCP defines the recovery objectives and strategies for the entire organization, while the data backup and restoration procedures are more specific and technical in nature.
C). Mean time to restore (MTTR): MTTR is a metric that measures the average time it takes to restore a system or service after a failure or outage. MTTR is an indicator of the efficiency and effectiveness of an organization's recovery process, as well as the availability and reliability of its systems or services. MTTR is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. MTTR reflects the actual performance of the recovery process, while the data backup and restoration procedures define the expected steps and actions for the recovery process.

D). Mean time between failures (MTBF): MTBF is a metric that measures the average time between failures or outages of a system or service. MTBF is an indicator of the quality and durability of an organization's systems or services, as well as their susceptibility to failures or outages. MTBF is related to an organization's defined data backup and restoration procedures, but it is not the most important factor to consider when reviewing them. MTBF reflects the potential frequency of failures or outages, while the data backup and restoration procedures define the contingency plans for failures or outages.

NEW QUESTION: 296
□□ □ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□
B. □□ □□□□
C. □□ □□□□
D. □□ □□□
Answer: (SHOW ANSWER)
Job scheduling ensures that system resources are allocated efficiently by prioritizing high-priority tasks during peak periods. It prevents resource contention by scheduling less critical jobs at off-peak times or when resources are underutilized. This method is the most direct and effective way to ensure adequate resources for essential activities.
System Virtualization (Option A):While useful for optimizing resource utilization, it does not prioritize activities dynamically.
Zero Trust (Option C):This is a security framework and does not address resource allocation.
Code Optimization (Option D):This improves performance but is not directly related to resource scheduling.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 297
□□ □□ □□ □□ □□ □□□ □□□□ □□□□ □□ □□(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: 298
□□ □ IT □□□□□ □□□ □□□ □□□□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□
B. □□ □□
C. □□□□□ □□ □□ □□
D. □□□□□□ □□□
Answer: B (LEAVE A REPLY)
The best criteria for monitoring an IT vendor's service levels are the performance metrics, as they provide quantifiable and measurable indicators of how well the vendor is delivering the agreed-upon services, such as availability, reliability, quality, timeliness, and customer satisfaction. A service auditor's report is a document that provides an independent opinion on the vendor's controls and processes, but it may not reflect the actual service levels or performance. A surprise visit to the vendor may help to verify the vendor's compliance and operations, but it may not be feasible or effective for monitoring the service levels on a regular basis. An interview with the vendor may help to obtain feedback and insights from the vendor's perspective, but it may not be objective or reliable formonitoring the service levels. References: CISA Review Manual(Digital Version), Chapter 2: Governanceand Management of IT, Section 2.4: IT Service Delivery and Support

NEW QUESTION: 299
□ □□□ □□ □□□□□□□ □ □□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□□□□. □ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□□?
A. □□□□ □□□(IaaS)
B. □□□□ □□□□□(SaaS)
C. □□□□ □□□(PaaS)

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

NEW QUESTION: 300
□□ □□ □ □□ □□□ □□ □□□ □□□□□ □□ □□ □□□ □ □□ □□ □ □□ □□□ □□ □□ □□ □□□□ □□□□□?
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: 301
□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□.
A. □□□ □□ □□□ □□ □□.
B. □□□ □□□□ □□□ □□ □ □□ □□□.
C. □□□ □□□ □□□ □□ □□□
D. □□ □□□ □□ □□.
Answer: B (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 302
□□ □ □□ □□□ □□ □□□ □□□ □□□□ □□ □ □□□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□ □ □□ □□□□□?
A. □□ □□□
B. □□ □□□

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

NEW QUESTION: 303
IT □□ □□ □□□ IT □□□ □□□□ □□ □□ □ □□□ □□ □□ □□ □□□?
A. IT □□□ □□ □□□□ □□□□ □□□□ □□□□□.
B. □ IT □□□ □□ □□□ □□ □□□□□ □□□□□.
C. □□ □□□□ □□□□□ □□□□ □ □□□ IT □□ □□□ □□□□□.
D. □□□ □□□ IT □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Identifying required IT skill sets that support key business processes is the first step to enable the alignment of IT staff development plans with IT strategy. An IT strategy is a plan that defines how IT will support the organization's goals and objectives. Identifying required IT skill sets means determining the knowledge, abilities, and competencies that IT staff need to perform their roles and responsibilities effectively and efficiently. This can help to align IT staff development plans with IT strategy, as well as to identify and address any skill gaps or needs within the IT workforce. The other options are not the first steps to enable alignment, but rather possible subsequent actions that may depend on the required IT skill sets. References:
CISA Review Manual (Digital Version), Chapter 5, Section 5.11
CISA Review Questions, Answers and ExplanationsDatabase, Question ID 229

NEW QUESTION: 304
□□□ IS □□□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□. □□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□ □□□ □□ □□□□ □□□□□.
B. □□ □□□□□ □□□□ □□ □□□ □□ □□□□□□.
C. □□□□ □□□ 10% □□ □□□ □□ □□□□□ □□□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
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: 305
□□ □ □□□ □□□□ □□□□ □□□ □ □□ □□ □□□□□?
A. □□ □□□□□
B. 256□□ □ □□
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: 306
□□□□□□ □□□□, □□□ □□ □□□□ □□□ □□□□ □□ □ □□□ □□ □ □ □□□□?
A. □□ □□ □□(BIA)□ □□□□ □□□□□.
B. □□ □□□□ □□□□ □□□□ □□□□ □□□□□.
C. □□□ □□□□ □□□□ □□□ □□□□.
D. □□□□ □□□□ □□□ □□ □□□(UAT)□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
Resilience is the ability of an organization to continue to operate effectively during or after a disruptive event. A business impact analysis (BIA) is a key process to identify the critical systems and processes that support the organization's objectives and determine the impact of their disruption. Without a BIA, the organization may not be able to prioritize the recovery of the most important systems and processes, which poses the greatest risk to its resilience. The other options are not as significant as a BIA, as they relate to data quality,

system monitoring, and user acceptance testing, which are important but not essential for resilience. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.2 Business Continuity Planning1

NEW QUESTION: 307
□□ □□□□ □□□ □□ □□□ □□□ □□□□ □□□ □□ □ □□□□□?
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: 308
□□ □ □□ □□□ □□□□ □□□ □□ □□ □□(BIA)□ □□□ □ □□ □□□□ □ □ □□ □□□□□?
A. □□□□□□□□(BIA)□ □□□□ □□ □□□□□ □□□□ □□□□□.
B. □□□ □□□ □□□ IT □□□□ □□□□□□.

C. □□ □□□ □□ □□□□ □□□□ □□□ □□□□□□.
D. BIA□ □□□□ □□□ □□ □□□□□.
Answer: (SHOW ANSWER)
The business impact analysis (BIA) is a critical component of an organization ' s business continuity planning (BCP) process. The most concerning issue is when system criticality information is provided only by the IT manager (Option B). This presents a risk of bias or incomplete analysis, as business units must also provide input to ensure a comprehensive assessment.
ISACA CISA Reference: According to ISACA's BCP and DRP guidelines, BIA should involve input from multiple business functions, including finance, operations, and risk management, rather than relying solely on IT.
Risk Implication: Without broader business input, the criticality of systems may be misclassified, leading to incorrect recovery priorities and potential business disruption.
Alternative Choices:
Option A: While a risk assessment is important, a BIA can still be completed without it and later validated.
Option C: The use of questionnaires is a valid method if responses are verified.
Option D: Lack of executive sign-off is concerning but does not directly impact the accuracy of system criticality assessment.

NEW QUESTION: 309
□□ □ □□□□ □□ □□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□?
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: 310
IS □□ □□ □□, □3□ □□□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□ □ □□□□□□□. □□□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□□ □3□ □□□□□□ □□□ □□□□□.
B. □3□ □□□□□ □□ □□ □□ □□□ □□□□□□.
C. □□ □□ □ □□□□ □□ □□□ □□□□□.

D. □3□ □□□□□□ □□□□□□(NDA) □□□ □□□□□.

Answer: (SHOW ANSWER)

The best recommendation to address the situation of inconsistencies in privacy requirements across third- party service provider contracts is to prioritize contract amendments for third-party providers. This is because:

Privacy requirements are essential to ensure the protection of personal information and compliance with relevant laws and regulations, such as the GDPR and the CCPA123.

Inconsistencies in privacy requirements can create risks of data breaches, legal liabilities, reputational damage, and consumer distrust for the organization that outsources its data processing to third-party providers123.

Suspending contracts with third-party providers that handle sensitive data (option A) is not a feasible or effective solution, as it may disrupt the business operations and cause contractual penalties or disputes4.

Reviewing privacy requirements when contracts come up for renewal (option C) is not a proactive or timely approach, as it may leave the organization exposed to privacy risks for a long period of time until the contracts expire4.

Requiring third-party providers to sign nondisclosure agreements (NDAs) (option D) is not a sufficient measure, as NDAs only cover the confidentiality of information, but not other aspects of privacy, such as data minimization, retention, access, deletion, and security4.

Therefore, the best recommendation is to prioritize contract amendments for third-party providers (option B), as this would allow the organization to align the privacy requirements with its own policies and standards, as well as with the applicable laws and regulations. This would also enable the organization to monitor and audit the compliance of third-party providers with the privacy requirements and enforce appropriate remedies or sanctions in case of noncompliance45.

References: 1: Understanding CPRA service provider contract requirements - Transcend 2: What you must know about 'third parties' under GDPR and CCPA 3: Data Privacy Implications for Service Provider and Third-Party Contracts 4: Privacy and outsourcing for businesses - Office of the Privacy Commissioner of Canada 5: Data Security Guidelines for outsourcing and third party compliance - European Union Agency for Network and Information Security

NEW QUESTION: 311

□□ □ □□□ □□□□ □□ □□ □□□(IoT) □□□ □□ □□□□□ □□□□ □□ □ □□□ □□□□ □□ □□□ □□□ □□□ □□ □ □□□ □□□□ □□ □□□□□?

A. □□□ □□□□ □□□ □□ □□ □□

B. □□□ IoT □□ □□ □□

C. □□□□ □□□ □□(NAC) □□ □□

D. IoT □□□ □□□ IT □□ □□

Answer: C (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

The most effective way to prevent unauthorized IoT devices from connecting is through network access control (NAC), which enforces authentication and authorization before allowing a device onto the network.
Vulnerability scans (A): Identify weaknesses but do not actively prevent device connections.
Reviewing IoT configurations (B): Focuses on existing devices, not unauthorized ones.
Policies (D): Provide guidance but do not enforce technical prevention.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on network security and endpoint access control.

NEW QUESTION: 312
IT □□□□□□ □□ □□□ □□ □□□ □□□□□.
A. IT □□□□ □□□□□ □□
B. IT □□□ □□ □□
C. IT □□ □ □□ □□
D. IT □□ □□□□□ □□ □□□□
Answer: (SHOW ANSWER)
An IT balanced scorecard is primarily used for measuring IT strategic performance. An IT balanced scorecard is a framework that translates the IT strategy into measurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth. An IT balanced scorecard helps to monitor and evaluate how well the IT function is delivering value to the organization, achieving its strategic goals, and improving its capabilities and competencies. The otheroptions are not the primary uses of an IT balanced scorecard, because they either focus on specific aspects of IT rather than the overall performance, or they are not directly related to the IT strategy. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.3

NEW QUESTION: 313
□□□ □□ □□□□□□ □□□□ □□ □□□ □□□□ □ □□ □□□ □□□ □□□ □□□.
A. □□ □□.
B. □□□ □□.
C. □□□□□□ □□□.
D. □□□ □□□.
Answer: (SHOW ANSWER)
In the development of a new financial application, the IS auditor's first involvement should be in the feasibility study. A feasibility study is a preliminary analysis that evaluates the technical, operational, economic, and legal aspects of a proposed project or system. A feasibility study helps determine whether the project or system is viable, feasible, and desirable for the organization and its stakeholders.

The IS auditor's role in the feasibility study is to provide an independent and objective assessment of the project or system's risks, benefits, costs, and impacts. The IS auditor should also ensure that the feasibility study follows a structured and systematic approach, considers all relevant factors and alternatives, and complies with the organization's policies and standards. The IS auditor should also verify that the feasibility study is documented and communicated to the appropriate decision-makers.
The IS auditor's involvement in the feasibility study is important because it can help: Identify and mitigate potential risks and issues that could affect the project or system's success Evaluate and justify the project or system's alignment with the organization's strategy, goals, and value proposition Estimate and optimize the project or system's resources, budget, schedule, and quality Assess and enhance the project or system's security, reliability, performance, and usability Ensure that the project or system meets the expectations and requirements of the users and other stakeholders The other three options are not the first involvement of the IS auditor in the development of a new financial application, although they may be part of the subsequent stages of the development process. Control design is the process of defining and implementing controls that ensure the security, integrity, availability, and efficiency of the system. Application design is the process of specifying the functional and technical features of the system. System test is the process of verifying that the system meets the specifications and requirements. Therefore, feasibility study is the best answer.
References:
[Feasibility Study - ISACA]
[IS Auditing Guideline G13 Performing an IS Audit Engagement - ISACA]

NEW QUESTION: 314
□□ □ □□□ □□ □ □□□ □□□ □□□ 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: 315
IS □□□□ □□ □□□ □□□ □□, □□ □□ □□□ □ □□□ □□□□ □□ □□□ □ □□□ □□ □□□ □□□□□□. □□□□ □□□ □□□ □□ □□□?
A. □□ □□□ □□□ □□ □□ IT □□□□ □□□□ □□□□□.
B. □ □□□ □□ □□□□□ □□□□□□.
C. □□□ □□ □□ □□□ □□□□□□.
D. □□ □□ □□□□ □□ □□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The IS auditor should review the organization's patch management policy to determine the expected frequency and scope of patching, as well as the roles and responsibilities of the patch management team. This will help the auditor assess the severity and impact of the non-compliance, and identify the root cause and possible remediation actions12.
References
1: How to Create a Patch Management Policy: Complete Guide 2: Free Patch Management Policy Template (+Examples)

NEW QUESTION: 316
□□ □ □□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□ □□?
A. □□ □□ □□□ □□ □□□ □□□□□.

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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 317
□□ □ □□□□□□ □□□□□ □□□□□(API) □□ □□ □□□ □□ □□□□□ □□ □ □□□ □□□□□?
A. □□ API □□□ □□ □□ □□ □□
B. □□□ □□ □ □□ □□□□ □□
C. □□□□ □□□□ □□□ □□
D. □□ □□ □□ □□
Answer: (SHOW ANSWER)
Limiting the rate of incoming requests, known as rate limiting, helps prevent API overloading by controlling the number of requests a client can make within a specific timeframe. This measure protects the API from being overwhelmed, ensuring better availability and performance. While dedicated servers, continuous integration/deployment, and stress testing contribute to overall system robustness, rate limiting directly addresses the risk of unavailability due to excessive or malicious traffic.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 318
□□ □□□□ □□□□ □□□ □□ □□□□ □□ □ □□□ □□ □ □□□□□?
A. □□ □□ □□□ □□ □□
B. □□ □□ □□ □□
C. □□ □□□□ □□(false negative) □□ □□□□□□.
D. □□ □□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 319
□□ □ □□□□□ □□ □□□ □□□□□?

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: 320
□□ □ □□ □□ □□ □□□□□□□□ □□□□ □□□□ □□□ □□□□ □□□□ □ □□□□□□ □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□ □□□□□?
A. □□□□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
Continuous auditing provides the greatest assurance that a middleware application compiling data from multiple sales transaction databases for forecasting is operating effectively12. Continuous auditing involves the use of automated tools to continuously monitor and audit a system's operations12. This allows for real- time identification and resolution of issues, ensuring that the system is always functioning as expected12. It also provides ongoing assurance about the integrity and reliability of the data being compiled by the middleware application12.
References:
5 Data Integration Methods and Strategies | Talend
What Is Middleware? Definition, Architecture, and Best Practices

NEW QUESTION: 321

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

A. □□ □□

B. □□□ □□

C. □□ □□

D. □□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 322

□□□□ □□ □□ □□(CSA) □□□□□ □□ □□ □ □□ □□□ □□ □□□□□?

A. □□ □□ □□

B. □□ □□□ □□ □□

C. □□ □□ □□ □□

D. □□□□ □□□□ □□

Answer: (SHOW ANSWER)

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: 323

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

A. □□□

B. □□□ □□□ □□
C. □□□ □□
D. □□
Answer: (SHOW ANSWER)
Due professional care is the obligation of an IS auditor to exercise the appropriate level of skill, competence, and diligence in performing an audit. It also requires the IS auditor to comply with the relevant standards, guidelines, and ethical principles of the profession. Completing an engagement by email only may compromise due professional care, as it may limit the IS auditor's ability to obtain sufficient and appropriate evidence, to communicate effectively with the auditee and other stakeholders, and to perform adequate quality assurance and review procedures. The other options are not as relevant as due professional care, as they relate to specific aspects of an audit, such as proficiency (the knowledge and skills of the IS auditor), sufficient evidence (the quantity and quality of the audit evidence), and reporting (the presentation and communication of the audit results). References: CISA Review Manual (Digital Version), Domain 1: The Process of Auditing Information Systems, Section 1.2 ISACA IT Audit and Assurance Standards

NEW QUESTION: 324
□ □□□□ □□ □□ □□□□□□□ □□□□ □□□□ □□□□ □□□□□□□ □□ □□ □□ □□□□ □□□□□. □□ □ □□ □□□ □□ □□□ □□□□ □□□ □□□ □ □□□□ □□ □□□ □□ □□□?
A. □□□ □□□ □□ □□□□ □□□ □ □□□□.
B. □□□□ □□□□ □□□ □□□ □□□ □□□□□.
C. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
D. □□□□ □□ □□ □□□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 325
□□□ □□ □□□□ □□ □ □□□□ □□□ □□□ □□□□□□ □□ □□ □ □□□ □□ □ □□□□□?
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 and - PwC3

NEW QUESTION: 326
□□ □□ □□□□□ □□□ □ □□ □□ □ □□ □□ □□ □□□ □□□ □□□?
A. □□ □□□ □□□ □□ □□
B. □□□□ □□ □□□ □□□
C. □□□□ □□
D. □□ □□ □□□□ □□□ □□ □□
Answer: D (LEAVE A REPLY)
Residual risk from the findings of previous audits should be the primary basis for prioritizing follow-up audits, because it reflects the level of exposure and potential impact that remains after management has implemented corrective actions or accepted the risk. Follow-up audits should focus on verifying whether the residual risk is within acceptable levels and whether the corrective actions are effective and sustainable. Audit cycle defined in the audit plan, complexity of management's action plans, and recommendation from executive managementare not valid criteria for prioritizingfollow-up audits,because they do not consider the residual risk from previous audits. References: CISA Review Manual (Digital Version), Chapter 2, Section
2.4.3

NEW QUESTION: 327
□□ □ □□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □ □ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
B. □□□□□ □□□ □□ □□(SLA)□ □□□□□ □□□□□□.
C. □□□□□ IT □□□□ □□ □□ □□ □□ □□□ □□□ □□□□□.
D. □□□□□ □□ □□ □□(CSA)□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and

conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 328
□□□ □□ □□(DLP) □□□ □□□ □□ □□□□□□ □□ □□□ □□ □□□ □□□ □□.
A. □ □ □□ □□ □□□□□□ □□□□□□□.
B. □□ □□□□□ □□□□ □□ □□□□.
C. □□□ □□□ □□□ □□□ □□□□□□ □□.
D. □□□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□ □□.
Answer: C (LEAVE A REPLY)
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: 329
□□ □ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
The primary basis on which audit objectives are established is the consideration of risks12. This involves identifying and assessing the risks that could prevent the organization from achieving its objectives12. The audit objectives are then designed to address these risks and provide assurance that the organization's controls are effective in managing them12. While audit risk, assessment of prior audits, and business strategy are important factors in

the audit process, they are secondary to the fundamental requirement of considering risks12.
References:
Objectives of Auditing - Primary and Secondary Objectives of Auditing | Auditing Management Notes Audit Objectives | Primary and Subsidiary Audit Objectives - EDUCBA

NEW QUESTION: 330
□□ □ IS □□□□ □□ □□ □□ □ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□ □□□ □□□ □□□□ □□
B. □□ □□ □□□ □□ □□□□□ □□□□ □□
C. □□□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□□.
D. □□ □□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□
Answer: A (LEAVE A REPLY)
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: 331
□ □□□□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □ □□□ □□□ □ □□ □□□□□□. □□□□ □□ □□□ □□ □□□ □□ □ □□□□ □?
A. □□ □□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ □□□□□.
B. □□ □□ □□□□ □□□ □□□ □□□□□ □□□ □□□□□.
C. □□ □□□ 12□□ □□ □□ □□ □□□ □□□□□□.
D. □□ □□□ □□□□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

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

NEW QUESTION: 333
□□ □ □□ □□□ □□□□ □□□ □□□□□□ □ □□□ □□ □□ □□□ □□□□ □□□ □ □□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□ □□(ITF)
B. □□□
C. □□□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
Data analytics is the process of analyzing large and complex data sets to discover patterns, trends, and insights that can support decision making and problem solving. Data analytics can enable an IS auditor to combine and compare access control lists from various applications and devices by using techniques such as data extraction, transformation, loading, cleansing, integration, aggregation, visualization, and reporting. Data analytics can help an IS auditor to identify and assess the risks and controls related to access management, such as unauthorized or excessive access, segregation of duties violations, access policy compliance, access activity monitoring, and access review and remediation.
The other options are not as effective or relevant as data analytics for combining and comparing access control lists from various applications and devices. Integrated test facility (ITF) is a technique for testing the validity and accuracy of application processing by inserting fictitious transactions into the system and verifying the results. ITF does not directly involve the analysis of access control lists. Snapshots are records of selected information at a specific point in time that can be used to monitor system activity or performance.
Snapshots can provide some information about access control lists, but they are not sufficient to combine and compare them across different sources. Audit hooks are software routines embedded in an application that can trigger an alert or a report when certain conditions are met. Audit hooks can help to detect anomalies or exceptions in access control lists, but they do not provide a comprehensive or integrated view of them.

References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 882 Data Analytics for Auditing Access Control3

NEW QUESTION: 334
□□ □□□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□□□□ □□ □□□ □□ □ □□□□□□. □ □□□□ □□ □□ □□□ □□□ □□□□□?
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 and Explanations Database

NEW QUESTION: 335
□□ □ □□ □□□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. □□□□ □□□□ □□□□
B. □□□□ □□□□ □□□ □□
C. □□ □□ □□ □□
D. □□□ □□ □□
Answer: A (LEAVE A REPLY)
The most effective method for detecting the presence of an unauthorized wireless access point on an internal network is A. Continuous network monitoring. This is because continuous network monitoring can capture and analyze all the wireless traffic in the network and identify any rogue or spoofed devices that may be connected to the network without authorization. Continuous network monitoring can also alert the system administrator of any suspicious or anomalous activities on the network and help to locate and remove the unauthorized wireless access point quickly.
Periodic network vulnerability assessments (B) can also help to detect unauthorized wireless access points, but they are not as effective as continuous network monitoring,

because they are performed at fixed intervals and may miss some devices that are added or removed between the assessments. Review of electronic access logs can provide some information about the devices that access the network, but they may not be able to detect devices that use fake or stolen credentials or devices that do not generate any logs. Physical security reviews (D) can help to prevent unauthorized physical access to the network ports or devices, but they may not be able to detect wireless access points that are hidden or disguised as legitimate devices.

NEW QUESTION: 336
□□ □ □□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □ □□ □□□□ □□ □□ □ □□□ □□□□□?
A. □□ □□□ □□
B. □□ □□ □ □□ □□
C. □□ □□ □□
D. □□ □□ □□ □□ □□
Answer: C (LEAVE A REPLY)
The results of the previous audit are an important source of information for an IS auditor to consider when performing the risk assessment prior to an audit engagement, as they can provide insights into the current state and performance of the auditee, identify any issues or gaps that need to be followed up or addressed, and highlight any areas that require special attention or focus. The designof controls is an important factor to evaluate during an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not reflect the actual implementation or effectiveness of the controls. Industry standards and best practices are useful benchmarks or guidelines for an IS auditor to compare or measure against during an audit engagement, but they are not the most important thing to consider when performing the risk assessment prior to an audit engagement, as they may not be applicable or relevant to the specific context or objectives of the auditee. The amount of time since the previous audit is a relevant criterion to determine the frequency or timing of an audit engagement, but it is not the most important thing to consider when performing the risk assessment prior to an audit engagement, as it does not indicate the level or nature of risk associated with the auditee.

NEW QUESTION: 337
□□□□ □□□ □□□□□□□ □□ □□□ □□□□ □□ □□□ □□□ □, □□ □□ □ □□□□ □□ □□□□ □□□□ □ □□□ □□□ □□□□.
A. □□□ □□ □□(SLA) □□□ □□ □□□ □□□.
B. □□□□ □□□ □□□□□ □□□ □□□.
C. □□□□ □□□□□ □□ □□ □□ □□ □□.
D. □□□□ □□□□ □□□□ □□ □□□□ □□□□ □□□.
Answer: C (LEAVE A REPLY)

In cloud environments, responsibility for controls is split between the provider and the customer. The division depends on the service model (IaaS, PaaS, SaaS). Misunderstanding the shared responsibility model can create gaps in control coverage, where critical risks may not be managed by either party. SLA penalties (A) are contractual issues, not audit priorities. Availability reports (B) and business process redesign (D) are relevant but not as fundamental as defining control ownership. ISACA's cloud audit guidelines stress that proper scoping begins with understanding shared responsibilities to avoid assurance gaps.
References (ISACA): ISACA Cloud Computing Audit Program; ISACA Journal - Shared Responsibility in Cloud.

NEW QUESTION: 338
□ □□□ □□□ □, □□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□ □ □□□ □□?
A. □□ □□ □□ □□ □□
B. □□□□ □□ □□ □□ □□
C. □□ □□□ □□ □□ □□ □□ □□□□
D. □□ □□ □□□□
Answer: A (LEAVE A REPLY)
The most important task for an IS auditor to perform after the merger of two organizations is to verify that access privileges have been reviewed. Access privileges are the permissions granted to users, groups, or roles to access, modify, or manage IT resources, such as systems, applications, data, or networks. After a merger, the IS auditor should ensure that the access privileges of both organizations are aligned with the new business objectives, policies, and processes, and that there are no conflicts, overlaps, or gaps in the access rights. The IS auditor should also verify that the access privileges are based on the principle of least privilege, which means that users are granted only the minimum level of access required to perform their tasks.
The other options are not as important as verifying that access privileges have been reviewed:
Investigating access rights for expiration dates is a useful task, but it is not the most important one. Expiration dates are the dates when access rights are automatically revoked or suspended after a certain period of time or after a specific event. The IS auditor should check that the expiration dates are set appropriately and enforced consistently, but this is not as critical as reviewing the access privileges themselves.
Updating the continuity plan for critical resources is a necessary task, but it is not the most urgent one. A continuity plan is a document that outlines the procedures and actions to be taken in the event of a disruption or disaster that affects the availability of IT resources. The IS auditor should update the continuity plan to reflect the changes and dependencies introduced by the merger, but this can be done after verifying that the access privileges are secure and compliant.

Updating the security policy is an essential task, but it is not the most immediate one. A security policy is a document that defines the rules and guidelines for securing IT resources and protecting information assets.
The IS auditor should update the security policy to incorporate the best practices and standards of both organizations, and to address any new risks or threats posed by the merger, but this can be done after verifying that the access privileges are aligned with the policy.

NEW QUESTION: 339
□□ □□ □□□ □□ □□□ □□□□□ □□, □□□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□.
A. □□ □ □□ □□□□.
B. □□ □□.
C. □□ □□□□ □□.
D. □□ □□ □□□□.
Answer: (SHOW ANSWER)
When information processing is outsourced, the contract should explicitly require the service provider to comply with applicable legal and regulatory requirements. ISACA guidance on third-party risk and outsourcing consistently emphasizes that contracts must address legal obligations, compliance responsibilities, and regulatory expectations because the enterprise remains accountable for the data and services even when they are handled by a third party.
Option C is the best answer because legal compliance is broader and more fundamental than operational specifics such as backup procedures or security administration details. ISACA states that enterprises remain responsible for safeguarding sensitive information and complying with legal and regulatory requirements regardless of what the contract says or which third party processes the data. Therefore, an auditor should expect the contract to expressly address compliance with those requirements.
Option A may be included in many outsourcing contracts, especially for critical services, but backup and recovery processes are service-level or operational matters. They are important, yet not as fundamental as requiring compliance with legal obligations. If the contract fails to address legal compliance, the organization faces regulatory, liability, and governance exposure even if backups are adequate.
Option B is incorrect because audit objectives are normally defined by the auditor or audit plan, not by the outsourcing contract. The contract may include audit rights, access rights, reporting rights, or the right to inspect controls, but it would not typically define the auditor's objectives. ISACA outsourcing guidance highlights right-to-audit clauses rather than audit objectives as contract content.
Option D may also appear in the contract through security requirements, roles, and responsibilities, but it is narrower than legal compliance. Security administration processes

matter, yet they are subordinate to the overarching requirement that outsourced processing comply with applicable law, regulation, and contractual obligations.
So, the strongest answer is C because an outsourced processing contract must specify compliance with legal requirements, which is a core expectation in ISACA's third-party governance and risk guidance.
References (Official ISACA):
* ISACA Journal, A Risk-Based Management Approach to Third-Party Data Security Risk and Compliance - enterprises remain responsible for complying with legal and regulatory requirements even when using third parties.
* ISACA Journal, Critical Information Systems Processes - contracts should include legal obligations and responsibilities.
* ISACA Journal, Ensuring Vendor Compliance and Third-Party Risk Mitigation - contracts should include pertinent clauses for compliance requirements.
* ISACA, Cloud Computing Evolution and Regulation in the Financial Services Industry - outsourcing arrangements should include audit and access rights in line with regulatory requirements.

NEW QUESTION: 340
□□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□ □□ □□□□?
A. □□ □□
B. □□ □□
C. □□□ □□□□ □□□
D. □□□ □□ □□ □□
Answer: D (LEAVE A REPLY)
Recovery facilities providing a redundant combination of Internet connections to the local communications loop is an example of last-mile circuit protection. Last-mile circuit protection is a type of telecommunications continuity that ensures the availability and redundancy of the final segment of the network that connects the end-user to the service provider. The local communications loop, also known as the local loop or subscriber line, is the physical link between the customer premises and the nearest central office or point of presence of the service provider. Byhavingmultiple Internet connections from different providers or technologies, such as cable, DSL, fiber, wireless, or satellite, the recoveryfacilities can avoid losing connectivity in case one of the connections fails or is disrupted by a disaster5.
References:
9: Last Mile Redundancy - How to Ensure Business Continuity - Multapplied Networks

NEW QUESTION: 341
□□ □ □□□□ □□□□□□ □□□□ □□□ □□ □□□ □□ □□□ □□□□ □ □ □ □□□ □□□ □□□□□?

A. □□ □□□ □□ □□ □□□(SSO)□ □□□□□.
B. □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□□.
D. □□□ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential informationfrom the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy.
References:
CISA Review Manual, 27th Edition, page 2301
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2

NEW QUESTION: 342
□□□ □□ □□□ □□□□ □□□□ □, □□□□□ □□□ □□□ □□□□ □□□ □ □□ □□□□□ □□ □ □□□ □ □□ □□□ □□□□□?
A. □□ □□ □□ □□ □□
B. □□ □□ □ □□ □□
C. □□ □□□□□□ □□ □□ □□□□ □□□□□□.
D. □□□□□ □□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
Reviewing a sample of system-generated backup logs is the best step to verify that regularly scheduled backups are timely and run to completion. Backup logs are records that document the details and results of backup operations, such as the date, time, duration, status, errors, and exceptions. By reviewing a sample of backup logs, the IS auditor can check whether the backups are performed according to the schedule and whether they are completed successfully or not. The other steps do not provide as much evidence or assurance as reviewing backup logs, as they do not show the actual outcome or performance of backup operations. References: CISA Review Manual, 27th Edition, page 247

NEW QUESTION: 343
□□ □□□(IS) □□ □□□□ □□ □ IT □□□□□ □□□□ □□ □□□ □□ □□□ □ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□□□(KPI)□ □□□□□.

B. □□ □3□ □□□ □□□□□.
C. □□ □□ □□□ □□□□ □□ □□□ □□□□□□□.
D. □□□□□ IT □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives. KPIs can help the organization tomonitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.
The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization's stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

NEW QUESTION: 344
□□ □ □□ □□□ □□ □□ □□□ □ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□□□ □□ □□□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□□ □□□□ □□□□□.
C. □□ □□□□□ □□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
A data analytics tool is the most effective way to detect as many abnormalities as possible during an IS audit, as it can process large volumes of data, perform complex calculations, and generate visualizations that reveal patterns, outliers, anomalies, or deviations from expected results. A data analytics tool can also help the auditor to test the entire population of data, rather than a sample, and to perform continuous auditing and monitoring.
References
ISACA CISA Review Manual, 27th Edition, page 256
What is Problem Solving? Steps, Process and Techniques | ASQ
Data Analytics for Auditors - IIA

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

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

NEW QUESTION: 346
□□ □□ □□□ □□ □□ □□□ □□□□□□ □□□□ □□□ □□□□□□. □□ □ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□ □□□□□.
B. □□□ □□□ □□□ □□□□□.
C. □□□□□ □□□ □□□ □□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□□ □□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The auditor's primary course of action is to evaluate the impact of the partial compliance. When a control is only partially operating as designed, the auditor must first assess significance: what risk remains, what objectives are affected, and whether the deviation is material enough to become a reportable finding. ISACA audit and follow-up guidance emphasizes capturing and following up on significant issues and deficiencies, which implies the need for impact evaluation before deciding on reporting or recommendations.
Option B is correct because evaluating impact is what determines the seriousness of the deficiency and the appropriate audit response. Without understanding the effect of the deviation, the auditor cannot appropriately decide whether to escalate it, report it, or recommend redesign.
Option C is important and usually happens during audit communication, but discussion with control owners is not the primary analytical step. The auditor must first understand the risk and significance of the partial compliance.
Option D is incorrect because not every partial deviation should automatically become a final-report finding.
The auditor should first evaluate whether the issue is significant and reportable. ISACA follow-up guidance specifically refers to significant issues/findings.
Option A is also incorrect because recommending redesign may be appropriate later, but only after the auditor understands the impact and whether the problem is design-related, operating-related, or user-adoption-related.
Therefore, B is the best answer because impact evaluation comes before escalation, formal reporting, or redesign recommendations.
References (Official ISACA):
* ISACA Journal, Enhancing the Audit Follow-up Process Using COBIT 5 - significant issues/findings should be captured and followed up.
* ISACA Journal, An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - supports a risk-based evaluation approach focused on control process areas.
* ISACA, How Effective Is Your Cybersecurity Audit - effectiveness depends on evaluating gaps and their implications.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 347
□□ □□□ □□□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□. □□ □ □ □ □□ □□□□□ □□□□□ □□□?
A. IT □□□ □□ □□ □ □□ □□□ □□ □□□□□.
B. □□□□ □□ □□□ NAT(□□□□ □□ □□)□ □□□ □ □□□□.
C. □□ □□□ □□ □□□□ □□□□□.
D. □□ □□□ □□ □□□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 348
□□ □□□□ □□ □□ □□ □ □□□□ □□ □□ □□ □□□□□?
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: 349
□□□ □□ □□(DLP) □□ □□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□. □□ □□□ □□□□ □□ □ □□ □□ □□ □□□□ □□□□ □□□?
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 oraccess sensitive data withoutproper protection, such asencryption 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: 350
□□ □ □3□ □□□ □□□□□ □□ □□ □□□ □□□□□□ □□ IS □□□□□ □□ □ □□□□ □□□ □□□□□?
A. □□□ □□□□□ □□ □□ □□□ □□ □□
B. □□□ □□□□□ □□ □ □□ □□
C. □□ □□□□ □□□ □□□□ □□ □□□
D. □□□ □□□□ □□ □□□□□ □□□
Answer: (SHOW ANSWER)
Toverify the effectivenessof a third-party provider'ssecurity controls, anindependent external audit reportis thestrongestevidence.
Option A (Incorrect):Security configuration documentsare helpful butdo not confirm effectivenesswithout validation.
Option B (Incorrect):Policies and procedures outlineintent, but anaudit confirms actual implementation.
Option C (Correct):External audit reports (e.g., SOC 2, ISO 27001)provideindependent assurancethat security controls are effective.
Option D (Incorrect):Management interviews providequalitativeinsights but arenot objective evidenceof control effectiveness.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversthird-party risk assessments and audit assurance.

NEW QUESTION: 351
□ □□ □□□ □□ □□ 3□□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□(AI) □□□ □□□□ □□ □□ □□□□ □□□□□□. □□ □ □□ □□□ □□□□ □□□ □ □□□ □ □□ □□□□ □□□ □□□□□?

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

NEW QUESTION: 352
□□ □ □□ □□ □□□ □□ □□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□ □□□?
A. □□□□ □□□□ □□
B. □□ □□
C. □□□□ □□
D. □□ □□□
E. □□ □□ □□ □□ □□□□□ □□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
The best recommendation to prevent fraudulent electronic funds transfers by accounts payable employees is dual control. Dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity. Dual control can prevent fraudulent electronic funds transfers by requiring independent verification and approval of payment requests, amounts, and recipients by different accounts payable employees. The other options are not as effective as dual control in preventing fraudulent electronic funds transfers, as they do not involve independent checks or approvals. Periodic vendor reviews are detective controls that can help identify any irregularities or anomalies in vendor payments, but they do not prevent fraudulent electronic funds transfers from occurring. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent fraudulent electronic funds transfers from occurring. Re-keying of monetary amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent fraudulentelectronic funds transfers from occurring.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 353
□□ □ □□□□□□ □□□□□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□ □□□ □□□□□?
A. □□ □□□
B. □□ □□□
C. □□□ □□□
D. □□□ □□ □□□(UAT)
Answer: C (LEAVE A REPLY)
The best testing approach to facilitate rapid identification of application interface errors is automated testing.

Automated testing is the use of software tools or scripts to execute predefined test cases, compare expected and actual outcomes, and report any discrepancies. Automated testing can help to speed up the testing process, increase test coverage, reduce human errors, and improve test accuracy and consistency. Automated testing can also help to detect interface errors that may occur due to incompatible data formats, communication protocols, or system configurations. References:
CISA Review Manual (Digital Version), Chapter 3, Section 3.3.11
CISA OnlineReview Course, Domain 2, Module 2, Lesson 1

NEW QUESTION: 354
□□ □□□ □□□ □□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□ □□ □ □□ □□□?
A. □□□ □□ □□ □ □□
B. □□ □□ □□□ □□ □□
C. □□ □□□ □□ □□ □□□
D. □□ □□ □ □□□□ □□ □□
Answer: A (LEAVE A REPLY)
The best source of information to determine the required level of data protection on a file server is the data classification policy and procedures, which define the criteria and methods for classifying data according to its sensitivity, value, and criticality, and specify the appropriate security measures and controls for each data category. Data classification policy and procedures help to ensure that data is protected in proportion to its importance and risk exposure. Access rights of similar file servers, previous data breach incident reports,and acceptable use policy and privacy statements are not sufficient or reliable sources of information to determine the required level of data protection on a file server, as they do not provide clear and consistent guidance on how to classify and protectdata. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Information Asset Security Framework

NEW QUESTION: 355
□□□□ □□ □□□□□□ □□□□□ □□□□□ □□□□□ □□ □□□□ □□□ □ □□□ □□□?
A. □□□□ □□□□□(DMZ)□ □□□□ □□□.
B. □□ □□ □□□ □□□□ □□ □□□□□ □□□.
C. □□ □□□ □□ □□□ □□□□ □□□.
D. □□□□ □□ □□□□ □□□□ □□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 356
□□ □ □ □□□ □□ □□□□ □□□□ □□ □□□ □□ □ □□□ □□□□□?
A. □□□ □□□

B. □□□ □□□
C. □□□ □□□
D. □□□ □□
Answer: B (LEAVE A REPLY)
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: 357
□□ □ □□□□ □□□ □□ □□□□□ □□ □ □□□ □□□□□?
A. □□□□ □□ □□□ □□□□ □□□□□□□.
B. □□□ □□ □□□ □□□□ □□□□ □□□□.
C. □□□□ □□□□ □□ □□□□□.
D. □□□ □□□□ □□□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 358

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

A. □□ □□ □□

B. □□ □□ □□ □□

C. □□□□ □□ □□□ □□

D. □□ □□ □□

Answer: B (LEAVE A REPLY)

The best compensating control is performing a bank reconciliation. Duplicate payments are a financial processing error that results in overpayment or duplicate disbursement. ISACA materials explicitly cite duplicate payments as an example of information errors that create cost risk. A bank reconciliation is the best compensating detective control among the choices because it helps identify duplicate disbursements by comparing recorded payments with actual bank activity.

Option B is correct because reconciliation is the control most likely to detect that a payment was processed twice. Once identified, management can investigate and recover the erroneous payment.

Option A is not the best answer because hash totals are generally used to verify data integrity of fields, not to compensate for duplicate payment processing.

Option D is also not the best answer because control totals can help identify completeness or reasonableness during batch processing, but they are less directly effective at detecting duplicate disbursements already posted through an online payment process.

Option C is weak because manual receipting of payments does not directly address duplication of outbound payments.

Therefore, B is the best answer because bank reconciliation is the most effective compensating control among the options for detecting duplicate payment errors. The exact match to this exam-style question is based on standard CISA control reasoning, with ISACA support that duplicate payments are a recognized cost-risk example.

References (Official ISACA):

* ISACA Journal, A Framework for Estimating ROI of Automated Internal Controls - cites duplicate payments and overpayments as examples of cost risk caused by information errors.
* ISACA training and audit fundamentals resources - support the use of detective and compensating controls in audit practice.

NEW QUESTION: 359

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

A. □□ □□□□□□ □□□□ □□□.

B. □□□ □□ □□□□□.

C. □□□ □□□ □□□ □□□□ □□ □□□□.

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

NEW QUESTION: 360
□□ □□□□ □□□ □ □□ □ □□□ □□ □□ □□ □□□?
A. □□□□□□(NDA)□ □□□□□.
B. □□□□ □□ □□ □□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against theorganization'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: 361
IS □□□□ □□□ □□□ □□ □□□ □□□□ □ □□□□ □□□□□□ □□ □□□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□□□□□. □□□□ □ □ □□ □□□□ □□ □□ □ □□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□
B. □□ □□□□□□ □□
C. □□ □□ □□□
D. □□□ □□
Answer: D (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 362
□□ □ □□ □□□□ □□□ □□ □□ □ □□□ □□□□ □□ □□□(IS) □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□ □□□ □□ □□□ □□□□□.
B. □□ □□ □□□□□ □□ □□ □□□(VPN) □□□ □□□□□ □□ □□□□.
C. □□ □□ □□□ □□□ □□ □□(MDM)□ □□□□ □□ □□ □□□□.
D. □□ □□ □ □□ □□□ □□□ □□□ □□□□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)
A lack ofMobile Device Management (MDM) enrollmentis the biggest concern, asunmanaged devicespose 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: 363
□□ □□ □ □□ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□□
B. □□□ □□□
C. □□□□ □□□
D. □□□-□□ □□□□□
Answer: C (LEAVE A REPLY)
The best document for an IS auditor to use in detecting a weakness in segregation of duties is a process flowchart. A process flowchart is a diagram that illustrates the sequence of steps, activities, tasks, or decisions involved in a business process. A process flowchart can help detect a weakness in segregation of duties by showing who performs what actions or roles in a process, and whether there is any overlap or conflict of interest among them. The other options are not as useful as a process flowchart in detecting a weakness in segregation of duties, as they do not show who performs what actions or roles in a process. A system flowchart is a diagram that illustrates the components,

functions, interactions, or logic of an information system. A data flow diagram is a diagram that illustrates how data flows from sources to destinations through processes, stores, or external entities. An entity-relationship diagram is a diagram that illustrates how entities (such as tables) are related to each other through attributes (such as keys) in a database. References: CISA ReviewManual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 364
□□ □ □□□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □ □□ □□□ □ □□□□ □□ IT □□□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
Problem management is an IT service management activity that is most likely to help with identifying the root cause of repeated instances of network latency. Problem management involves analyzing incidents that affect IT services and finding solutions to prevent them from recurring or minimize their impact. Change management is an IT service management activity that involves controlling and documenting any modifications to IT services or infrastructure. Incident management is an IT service management activity that involves restoring normal service operation as quickly as possible after an incident has occurred.
Configuration management is an IT service management activity that involves identifying and maintaining records of IT assets and their relationships. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 334

NEW QUESTION: 365
□□ □ □□□□ □□□ □□(BCP)□ □□ □□□ □□□□□ □□□□ □□□ □□ □ □ □□□ □□□ □□□□□?
A. □□□□ □□□ □□
B. □□ □□□ □□
C. □□□□□ □□□ □□
D. □□ □□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 366
□□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□□□ □ □□ □□ □□ □□□ □ □□□□?
A. □□ □□□ □□ □ 2□ □□ □□□□□.
B. □□ □□ □□□ □□ □□□□□ □□□□.
C. □□ □□□ □□□□ □ □□□□ □□□□□□ □□□□.

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

NEW QUESTION: 367
□□ □□□(IS) □□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □□□□□□ □□□ □□□□ □□□□. □□ □ □□□□ □□ □□□□□ □□□□ □ □□□ □□□ □□?
A. □□□□ □□□□ □□ □□
B. □□□□□ □□□ □□ □□
C. □□ □□ □□
D. □□□ □□□ □□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed in-Depth Explanation:
The primary focus when reviewing operational database management in a cloud environment should be the security settings configuration. Cloud environments often have complex and customizable security configurations, and any misconfiguration can lead to data breaches or unauthorized access. Ensuring proper security settings helps maintain data confidentiality, integrity, and availability.
Cloud vendor security certifications (Option A) are important but do not directly address how security is configured. Auto-scaling of provisioning costs (Option B) relates to resource management rather than security. Large-scale data transfers (Option D) may be relevant, but security settings directly impact data protection.
ISACA CISA Reference: Domain 5 - Protection of Information Assets

NEW QUESTION: 368
□□ □ □□□(PKI) □□□□ □□ □□□ □□□ □□□□□?
A. □□□□(CA)□□ □□□ □□□□ □□□□
B. □□□ □□□□ □□ □□ □□□□ □□□□□□
C. □□□□ □□□ □□□□ □□□□□ □□ □□ □□ □□□□ □□
D. □□ □ □□ □□□□ □□□□
Answer: (SHOW ANSWER)

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

NEW QUESTION: 370
□□ □□□□ □□□□□□ □□□□ □□□ □□ □□(ERP) □□□□ □□□□□□□ □ □□ □□□□□ □□□□ □□□, □ □□□ □□□ □□ □□□□□□ □□□ □□□□ □. □ □□□□□ □ □□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□□□ □ □ □□ □□ □ □□□□□?
A. □□ □□□
B. □□□□ □□
C. □□□ □□ □□□(UAT)
D. □□ □□□
Answer: D (LEAVE A REPLY)
The primary focus of the IS auditor reviewing the first year of the project should be regression testing.
Regression testing is a type of testing that ensures that the existing functionality of the system is not affected by the changes or upgrades made to the system. Since the project involves upgrading the ERP system hosting the general ledger, which is a critical and complex component of the finance department, it is important to verify that the upgrade does not introduce any errors or defects that could compromise the accuracy, completeness, and reliability of the financial data and reports. Regression testing can help identify and resolve any issues before they affect the users and the business processes.
Unit testing, network performance, and user acceptance testing (UAT) are also important aspects of the project, but they are not the primary focus of the IS auditor in the first year. Unit testing is a type of testing that verifies that each individual module or component of the system works as expected. Network performance is a measure of how well the system can communicate and exchange data with other systems and devices over a network. User acceptance testing (UAT) is a type of testing that validates that the system meets the user requirements and expectations. These aspects are more relevant in later stages of the project, when the system is more developed and ready for deployment.
References:
ERP Upgrade: The Path to Modernization | SAP
ERP System Validation: Your Guide To Successfully Validating ERP Systems The role of internal auditors in ERP#based organizations What is Regression Testing? Definition, Tools and Examples What is Unit Testing? Definition, Tools and Examples What is Network Performance? Definition, Metrics and Examples What is User Acceptance Testing (UAT)? Definition, Process and Examples

NEW QUESTION: 371
□□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□□?
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: 372
□□ □□□□ □□□□ □□ □□□□□□□□ □□□ □□□□□. □□ □□□□□ □□ □ □□□□, □□□□□□ □□ □□ □□□□ □□ □□ □□□ □□□□□□. □□ □□ □ □□□ □□□□□?
A. □□ □□□ □□□□ □□□□□ □□□.
B. □□□□□□□ □□ □□□ □□ □□ ID□ □□□□ □□□ □□□□□.
C. □□□□□□□ □□ □□□ □□ □□ □□ □□□ □□□ □□□□□.
D. □□ □ □□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
The best course of action for a security administrator who is called in the middle of the night by the on-call programmer who needs access to the live system is to give the programmer an emergency ID for temporary access and review the activity. This is because:
Requiring that a change request be completed and approved may delay the resolution of the problem and cause further damage or disruption to the system or business operations. A change request is a formal document that describes the proposed change, its rationale, impact, benefits, risks, costs, and approval process. A change request is usually required for planned or scheduled changes, not for emergency or urgent changes.
Giving the programmer read-only access to investigate the problem may not be sufficient or effective, as the programmer may need to perform actions or tests that require write or execute permissions. Read-only access means that the user can only view or copy data or files, but cannot modify or delete them.
Reviewing activity logs the following day and investigating any suspicious activity may not prevent or detect any unauthorized or malicious actions by the programmer in real time. Activity logs are records of events and actions that occur within a system or network. Activity logs can provide evidence and accountability for system activities, but they are not proactive or preventive controls.
Therefore, giving the programmer an emergency ID for temporary access and reviewing the activity is the best course of action, as it allows the programmer to access the live system and resolve the problem quickly, while also ensuring that the security administrator can monitor and verify the programmer's activity and revoke the access when it is no

longer needed. An emergency ID is a temporary account that grants a user elevated privileges or access to a system or resource for a specific purpose and duration. An emergency ID should be:
Created and authorized by a security administrator or manager
Assigned to a specific user and purpose
Limited in scope and time
Logged and audited
Revoked and deleted after use
Some of the best practices for emergency access to live systems are12:
Establish clear policies and procedures for requesting, approving, granting, monitoring, reviewing, and revoking emergency access Define criteria and scenarios for emergency access, such as severity, impact, urgency, and risk Implement controls to prevent unauthorized or unnecessary use of emergency access, such as multifactor authentication, approval workflows, alerts, notifications, and time restrictions Implement controls to track and audit emergency access activities, such as logging, reporting, analysis, and investigation Implement controls to ensure accountability and responsibility for emergency access users, such as attestation, justification, documentation, and feedback

NEW QUESTION: 373
□□ □□□□□ □□□ □□ □ □□□ □□□□ □□ □□□ □□□□ □□□□ □□, □ □, □□ □□□ □□□□□. □□□ □□□ □□□□ □ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□ □□ □□□□□□. □□ □ □□ □□□□ □□ □□ □□□ □□□□□?
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 interlockingdoors 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: 374
□□□□ □□ □ IS □□□□ □□□□ □□□□□ □□□□ □□ □□□□ □□□ □□ □□□□□□. □ □□□□ □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□□ □□
B. □□□□ □□□

C. □□□□ □□

D. □□□□□ □□□□□□

Answer: D (LEAVE A REPLY)

The answer D is correct because the greatest concern for an IS auditor with the situation of business owners being removed from the project initiation phase is that the requirements may be incomplete. The project initiation phase is the first step in starting a new project, where the project's purpose, scope, objectives, and deliverables are defined and documented. The project initiation phase also involves identifying and engaging the key stakeholders who have an interest or influence in the project, such as sponsors, customers, users, or business owners.

Business owners are the individuals or entities who have the authority and responsibility to define the business needs and expectations for the project. They are also the primary beneficiaries of the project outcomes and benefits. Business owners play a crucial role in the project initiation phase, as they provide valuable input and feedback on the requirements and specifications of the project. Requirements are the statements that describe what the project should accomplish or deliver to meet the business needs and expectations. Requirements are essential for guiding the project planning, execution, monitoring, and closure phases.

If business owners are removed from the project initiation phase, it can result in incomplete or inaccurate requirements, which can have negative impacts on the project's quality, scope, time, cost, and risk. Some of the possible consequences of incomplete requirements are:

Misalignment: The project may not align with the business strategy, vision, or goals, which can reduce its value or relevance.

Confusion: The project team may not have a clear understanding of what the project should achieve or deliver, which can affect their performance or productivity.

Rework: The project may need to undergo frequent changes or revisions to accommodate new or modified requirements, which can increase the time and cost of the project.

Dissatisfaction: The project may not meet the expectations or satisfaction of the business owners or other stakeholders, which can affect their acceptance or support of the project.

Failure: The project may not deliver the expected outcomes or benefits, which can affect its success or viability.

Therefore, an IS auditor should be concerned about the involvement and participation of business owners in the project initiation phase, as it affects the completeness and quality of requirements. An IS auditor should review the policies and procedures for stakeholder identification and engagement, verify that the business owners have adequate knowledge and skills to define their requirements, and test that the requirements are well-defined, documented, approved, and communicated.

References:

Project Initiation: The First Step to Project Management [2023] * Asana Everything you need to know about the project initiation phase Project Initiation Phase - The Business Professor Project Initiation: A Guide to Starting a Project Right Way - Kissflow

NEW QUESTION: 375
□□□□ □□□□ □□ □□ □□□ □□□ □, □□ □□□ □□□□ □□□□ □ □□ □ □□ □□□ □□ □□□□□?
A. □□ □□□□ □□
B. ISP □□□ □□ □□
C. □□□□ □□□ □□ □□□
D. □□□□ □□□□ □□□□□
Answer: D (LEAVE A REPLY)
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: 376
IS □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□. □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□□□ □□ □□
B. □□ □□ □□□ □□□ □□
C. □□ □□□ □□□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 377
□□ □□□(IS) □□□□ □□ □□□ □□□ □□ □□□(IoT) □□□ □□□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□□□ □□□ □□ □ □□ □□□ □□□□□?
A. □□ □□□ □□ Io I □□ □□□ □□□ □□□ □□□□
B. IoT □□ □ □□ □□ □□□□□ □□ □□ □□
C. □□ □□□□□□ □□ IoT □□ □□□ □□ □□ □□ □□
D. □□ □□□□ □□□ □□□□ □□ IoT □□
Answer: B (LEAVE A REPLY)
The use of open-source software components in IoT devices presents the greatest security risk due to potential vulnerabilities that may exist within the software. These vulnerabilities can be exploited if patches are not applied promptly, and the organization might not have direct control over the software ' s maintenance and security updates. This risk is amplified in critical manufacturing environments where compromised IoT devices can lead to operational disruptions.
Physical Security (Option A):While important, theft of IoT devices generally poses less risk compared to a system-wide compromise due to software vulnerabilities.
Firmware Storage Constraints (Option C):While a limitation, this is a secondary concern compared to exploitable software.
Devices Not Using Wireless Connectivity (Option D):Wired devices are generally more secure, reducing this as a significant concern.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 378
□□□ □□ □□□□ □□□ □□□ □, □□ □□□ □□□□ □□ □□□ □□ □ □□□ □□□ □□□.
A. □□ □□□□ □□ □□□ □□□.
B. □□□□ □□□ □□ □□ □□□ □□□□□.
C. □□□□ □□□□□ □□ □□□ □□□.
D. □□ □□ □□□ □□□□ □ □□□□ □□.
Answer: (SHOW ANSWER)

NEW QUESTION: 379

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

A. □□ □□ □□□□□ □□□ □□□□ □□□ □□□□□□.

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

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

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

Answer: (SHOW ANSWER)

The best answer is D. The dataset for training the model was obtained from an unreliable source.

ISACA's AI and ML guidance places strong emphasis on the quality, reliability, and validation of input and training data. ISACA notes that controls must validate each data source and that corrupted or poor-quality training data can lead to poor-quality outcomes. If the training dataset comes from an unreliable source, the model's predictions may be fundamentally flawed, biased, manipulated, or unauditable from the start.

Option A. Open source programming language is not inherently a concern. The language itself does not determine whether the model is reliable or controlled.

Option B. Tested with data from the same population as the training data is a common validation step and not inherently problematic by itself.

Option C. Accuracy decreased with a different population can be a concern about generalizability, but in this question it is less fundamental than unreliable training data. If the source data itself is untrustworthy, all downstream results are suspect.

Therefore, D is the correct answer because unreliable training data creates the most serious foundational risk to the model's validity and trustworthiness.

References (Official ISACA):

* ISACA Journal, Developing Trustworthy AI: Understanding the Inputs.
* ISACA Journal, Artificial Intelligence's Impact on Auditing-Emerging Technologies.
* ISACA press release, New ISACA Publications Highlight Machine Learning Technology and Compliance Risk for Auditors.
* ISACA, AI Algorithm Audits: Key Control Considerations.

NEW QUESTION: 380

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

A. □□□ □□ □ □□□.

B. □□□□ □□□ □□ □□ □□□ □□□□□.

C. □□ □ □□□.

D. □□□ □□□□ □□ □□.

Answer: C (LEAVE A REPLY)

The correct answer is C. Remediation and retesting.

ISACA guidance explains that penetration testing identifies exploitable weaknesses and provides guidance to address them. Once findings are identified, the next logical and control-appropriate step is to remediate the weaknesses and then retest to confirm they have been effectively resolved.
Option A is not the best next step because vulnerability scanning may supplement testing, but after a completed penetration test with findings, the priority is to fix what was found and verify closure.
Option B may be part of root cause work, but it is not the primary next step.
Option D is important from an information-handling perspective, but it does not address the control weaknesses identified by the test.
Therefore, the correct answer is C, because findings from a penetration test should drive remediation followed by retesting to validate that the identified weaknesses have been corrected.
References (Official ISACA):
* ISACA, The Future of Cybersecurity Assessments Is Here - VAPT identifies weaknesses and provides guidance to address them.
* ISACA, Taking a Risk-Based Approach to Pen Testing - findings should be evaluated and acted on according to business impact.
* ISACA, Smarter Testing Equals Safer Digital Experiences - findings should be assessed for exploitability and impact, supporting focused remediation.

NEW QUESTION: 381
□□□□□□ □□ □□ □ □□ □□□ □□□□ □□□□□□ □□□(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: 382

□ □□□ □□ □□□□□ □□ □□ □□□ □□□□ □□ □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: 383
□□ □ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□□□?
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: 384
□□ □ IT □□□□ □□□□□□ □□□□ □□ □□□ □□ □ □□□ □□□ □□ □□ □□□?
A. □□ □□ □□(KRIS)□ □□□ □□
B. IT □□□ □□□□ □□□ □□□□ □□
C. □□□□ □□ □□ □□(BIA) □□ □ □□
D. □□□□□□(KPI)□ □□□□ □□
Answer: B (LEAVE A REPLY)

The most significant impact to an organization that does not use an IT governance framework is inadequate alignment of IT plans and business objectives. IT governance is a framework for the governance and management of enterprise information and technology (I and T) that supports enterprise goal achievement1.
IT governance helps to ensure that IT investments and activities are aligned with the business strategy, vision, and values of the organization. IT governance also helps to optimize the value of IT, manage IT-related risks, and measure and monitor IT performance1.
Without an IT governance framework, an organization may face challenges such as:
Lack of clarity and direction for IT decision making
Inconsistent or conflicting IT priorities and demands
Inefficient or ineffective use of IT resources and capabilities
Poor quality or delivery of IT services and products
Increased exposure to IT-related threats and vulnerabilities
Reduced customer satisfaction and trust in IT
Missed opportunities for innovation and competitive advantage
Therefore, an organization that does not use an IT governance framework may fail to achieve its business objectives and may lose its competitive edge in the market.
References:
COBIT 2019 Framework Introduction and Methodology, Section 1.1: What Is Governance of Enterprise I and T?
IT Governance: Definitions, Frameworks and Planning, Section 1: What Is IT Governance?

NEW QUESTION: 385
□□ □ □□□□□□ □□□□ □□□ □□□ □□□ □□□ □□□□□?
A. □□ □□□□□
B. □□□ □□ □□
C. □□ □□□
D. □□ □□
Answer: D (LEAVE A REPLY)
Application containers are a form of operating system virtualization that share the same kernel as the host operating system. This means that any vulnerability or compromise in the kernel can affect all the containers running on the same host, as well as the host itself. Additionally, containers may have privileged access to the kernel resources and functions, which can pose a risk of unauthorized or malicious actions by the container processes. Therefore, securing the kernel is a critical aspect of application container security.
Shared registries (option A) are not an inherent risk in the application container infrastructure, but they are a potential risk that depends on how they are configured and managed. Shared registries are repositories that store and distribute container images. They can be public or private, and they can have different levels of security and access controls. Shared registries can pose a risk of exposing sensitive data, distributing malicious

or vulnerable images, or allowing unauthorized access to images. However, these risks can be mitigated by using secure connections, authentication and authorization mechanisms, image signing and scanning, and encryption.
Host operating system (option B) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is configured and maintained. Host operating system is the underlying platform that runs the application containers and provides them with the necessary resources and services.
Host operating system can pose a risk of exposing vulnerabilities, misconfigurations, or malware that can affect the containers or the host itself. However, these risks can be mitigated by using minimal and hardened operating systems, applying patches and updates, enforcing security policies and controls, and isolating and monitoring the host.
Shared data (option C) is not an inherent risk in the application container infrastructure, but it is a potential risk that depends on how it is stored and accessed. Shared data is the information that is used or generated by the application containers and that may be shared among them or with external entities. Shared data can pose a risk of leaking confidential or sensitive data, corrupting or losing data integrity, or violating data privacy or compliance requirements. However, these risks can be mitigated by using secure storage solutions, encryption and decryption mechanisms, access control and auditing policies, and backup and recovery procedures.
Therefore, option D is the correct answer.
References:
Application Container Security Guide | NIST
CSA for a Secure Application Container Architecture
Application Container Security: Risks and Countermeasures

NEW QUESTION: 386
□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □ □□ □□ □ □□□□□?
A. □□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□ □□
B. □□ □□□ □□□ □□ □□□ □□□ □□□□□ □□□□□ □□
C. □□ □□□ □□□ □□ □□ □□ □□ □□□ □□□□□□ □□
D. □□ □□□□ □□□ □□□ □□□□□ □□ □□□□□ □□
Answer: D (LEAVE A REPLY)
The answer D is correct because the most important thing to determine when conducting an audit of an organization's data privacy practices is whether the systems inventory containing personal data is maintained.
A systems inventory is a list of all the systems, applications, databases, and devices that store, process, or transmit personal data within the organization. Maintaining a systems inventory is essential for data privacy because it helps the organization to identify, classify, and protect the personal data it holds, as well as to comply with the relevant privacy laws and regulations. A systems inventory also enables the organization to perform data

protection impact assessments (DPIAs), data breach notifications, data subject access requests, and data retention and disposal policies.
The other options are not as important as option D. Whether a disciplinary process is established for data privacy violations (option A) is a policy issue that may deter or sanction the employees who violate the data privacy rules, but it does not directly affect the data privacy practices of the organization. Whether strong encryption algorithms are deployed for personal data protection (option B) is a technical issue that may enhance the security and confidentiality of the personal data, but it does not address the other aspects of data privacy, such as accuracy, consent, and purpose limitation.Whether privacy technologies are implemented for personal data protection (option C) is also a technical issue that may support the data privacy practices of the organization, but it does not guarantee that the organization follows the best practices or complies with the applicable laws and regulations.
References:
IS Audit Basics: Auditing Data Privacy
Best Practices for Privacy Audits
ISACA Produces New Audit and Assurance Programs for Data Privacy and Mobile Computing

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

NEW QUESTION: 388
IT □□ □□□ □□□ □ □□ □ □□ □□□ □□□ □□□□.
A. IT □□ □□□□ □□□□ □□□□□.
B. □□ □□□ □□ □□ □□□ □□□□ □□□□.
C. □□□□□□(KPI)□ □□□□.
D. □□ □□□ □□□□ □□ □□□ □□ □□□□□.
Answer: B (LEAVE A REPLY)
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: 389
□□ □ □□□ □□□□□□ □□□□□ □□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□(DoS) □□□ □□□ □□□ □□□□□.
B. □□ □□□□□ □□ □□□□□ □□□□ □ □□ □□□□ □ □□□□.
C. □□ □□□□ □□□□ □□□ □ □□□□ □□□□.
D. □□□ □□ □□□ □ □□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
The primary advantage of a decentralized database architecture over a centralized one is that it reduces the concentration of risk in a single location or single service point. Because data and processing are distributed, the effect of a single outage or denial of service event is generally reduced compared with a centralized architecture, where one core point of failure can disrupt the whole environment.
Option A is therefore the best answer. Decentralization improves resilience by avoiding total dependency on one central database or service node. In audit and risk terms, this lowers the impact of certain availability attacks or failures by distributing exposure.
Option B is incorrect because real-time synchronization over public networks is usually more difficult, not easier, in decentralized environments. Distributed synchronization introduces latency, consistency, and network management challenges.
Option C is incorrect because transaction consistency is generally harder to maintain in decentralized systems.
Distributed databases often trade some degree of simplicity or immediacy of consistency for resilience, scalability, or local autonomy.
Option D is incorrect because uniform security policy enforcement is usually easier in centralized architectures, where governance and administration can be applied from a single control point.
So the correct answer is A, because the main architectural benefit of decentralization in this context is reduced single-point failure risk and reduced impact from centralized service disruption.
References (Official ISACA):
* ISACA Glossary - control and architecture terminology reference.
* ISACA COBIT resources - governance and resilience principles support reducing concentration risk through architectural design choices.

NEW QUESTION: 390
□□□□ □□□ □□ □□ □□ □□ □, □□ □□□(IS) □□□□ □□ □□ □□ □□□ □□□□ □□□□ □□□□□(SaaS) □□□ □□□□ □□□□□□. □□□□ □□□ □ □□ □□ □□□?
A. IT □□□□ □□□ □□□□ □□□□□□□ □□□□□.
B. □□□ □□□ □□□□□ □□□□□.
C. □3□ □□ □□□ □□□□□ □□□□□.
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: 391
□□ □□□□ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□□□ □□□
C. □□ □□□
D. □□□□ □□
Answer: A (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 392
□□ □□□ □□□□ □□□ □ □□ □□□□ □□ □□□ □□□ □□□□.
A. □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□
B. □□ □□ □□□□ □□
C. □□ □□□ □□ □□ □□ □□
D. □□ □□□□ □□ □□ □□ □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 393
□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □, □□ □□□ □□□□ □□□ □□ □□ □□ □□□?
A. □□□ □□□ □□□ □□□□ □□□□□.
B. □□□□□□ □□□□ □□□□□□.
C. □□ □□□ □□□ □□□□□ □□□□□□.
D. □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
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 causeof 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 internalaudit resources and time

NEW QUESTION: 394
□□□□□□ □□ □□ □□□(IS) □□ □ □□□□□□□ □□ □□ □□□□□ □□ □ □ □□ □□□ □□□ □ □□□ □□□□ □□□ □□□ □□□□□□□. □□ □ IS □□ □□ □□□□ □ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □ □□□□ □□□□ □□ □□ □□□ ID □□ □□□ □□□□ □□□.
B. □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□□□□ □ □ □□ □□□ □□□ □□□.
C. □□□□□□ □□□□□□ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□ □ □□□ □□□□□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 395
□□ □ □□□ □□□□ □□ □□□ □□□□ □ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□ □□□□
B. 2□□ □□
C. □□□□ □□
D. □□ □□ □□□
Answer: A (LEAVE A REPLY)
The answer A is correct because user activity monitoring is the most effective control to mitigate against the risk of inappropriate activity by employees. User activity monitoring (UAM) is the process of tracking and recording the actions and behaviors of users on devices, networks, or applications that belong to an organization. UAM can help to prevent, detect, and respond to insider threats, such as data theft, fraud, sabotage, or misuse of resources. UAM can also help to enforce policies, ensure compliance, and improve productivity and performance.
Some of the benefits of UAM are:
Prevention: UAM can deter employees from engaging in inappropriate activity by making them aware that their actions are monitored and recorded. UAM can also prevent unauthorized access or use of sensitive data or resources by implementing access controls, encryption, or alerts.
Detection: UAM can detect any anomalies, deviations, or violations in user activity by analyzing the data collected from various sources, such as logs, keystrokes, screenshots,

or video recordings. UAM can also use artificial intelligence or machine learning to identify patterns, trends, or risks in user behavior.
Response: UAM can respond to any incidents or issues related to user activity by notifying the relevant stakeholders, such as managers, security teams, or auditors. UAM can also provide evidence or proof of user activity for investigation or remediation purposes.
Some examples of UAM tools are:
Teramind: Teramind is a cloud-based UAM platform that offers features such as user behavior analytics, risk scoring, policy enforcement, data loss prevention, and productivity optimization.
Digital Guardian: Digital Guardian is a data protection platform that offers UAM capabilities such as endpoint detection and response, data classification and tagging, and threat hunting and incident response.
XPLG: XPLG is a log management and analysis platform that offers UAM features such as log aggregation and correlation, user behavior profiling and anomaly detection, and real-time alerts and dashboards.
The other options are not as effective as option A. Two-factor authentication (option B) is a security mechanism that requires users to provide two pieces of evidence to verify their identity before accessing a system or resource. Two-factor authentication can enhance the security and privacy of user accounts, but it does not monitor or record the user activity after the authentication. Network segmentation (option C) is a technique that divides a network into smaller subnetworks based on criteria such as function, location, or security level. Network segmentation can improve the performance, security, and manageability of a network by reducing congestion, isolating threats, and enforcing policies. However, network segmentation does not track or record the user activity within each segment of the network. Access recertification (option D) is a process that verifies and validates the access rights of users to systems or resources periodically or on- demand. Access recertification can ensure that users have the appropriate level of access based on their roles and responsibilities, but it does not monitor or record the user activity with the access rights.
References:
[User Activity Monitoring: Examples and Best Practices | SEON]
Top 10 user activity monitoring tools: software features and tracking price - Dashly blog
Whatis User Activity Monitoring? How It Works, Benefits, Best Practices and More - Digital Guardian What Is User Activity Monitoring? Learn the What, Why, and How - XPLG

NEW QUESTION: 396
□□□ □□□ □□□ □□ □□□□ □ □□□ □□□□ □, □□ □□□ □□ □□□□ □ □□□ □□ □□□ □□□□ □□□□ □□ □□□□□□. □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □□□□□?
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: 397
□□ □□□□ □□ □ □□□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□ □□ □□□ □□□□ □□□ □□□□□?
A. □□□
B. □□□
C. □□ □□
D. □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 398

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

A. IS □□ □□□□□ □□ □□ □□ □□□ □□□□□□□.

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

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

D. □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 399

SQL □□□ □□□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□?

A. □□□□ □□

B. SSL(Secure Sockets Layer) □□□

C. □□ □□□ □□

D. □□□ □□

Answer: C (LEAVE A REPLY)

Input validation is the best control to address SQL injection vulnerabilities, because it can prevent malicious users from entering SQL commands or statements into input fields that are intended for data entry, such as usernames or passwords. SQL injection is a technique that exploits a security vulnerability in an application's software by inserting SQL code into a query string that can execute commands on a database server. Unicode translation, SSL encryption, and digital signatures are not effectivecontrols against SQL injection, because they do not prevent or detect SQL code injection into input fields. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

NEW QUESTION: 400

□□ □ □□□□(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 and Responsibilities
What are the Best Practices in Quality Management?
User Acceptance Testing (UAT): A Complete Guide
Employee Onboarding Process: Definition and Best Practices
What Is A Steering Committee? - The Basics

NEW QUESTION: 401
□□□□□ □□ □□ □ □□ □□□ □□□ □□ □□□□□ □□□.
A. □□ □□□.
B. □□□□□□ □□□(DBA).
C. □□□□ □□□.
D. □□□.
Answer: D (LEAVE A REPLY)
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: 402
IT □□□ □□□□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
A. IT □□□ □□ □□□□ □□□ □□□□□.
B. IT □□□ □□□□□□.
C. □□ □□ □□□ □□ □□ □□□ □□□□□.
D. IT□ □□□□ □□□□□□□.
Answer: B (LEAVE A REPLY)
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: 403
□□ □□□(IS) □□□□ □□ □□□ □□ □□ □□(SDLC) □□□□□ □□□ □□□ □ □□□ □□□□ □□ □□□□□. □□□□ □□ □ □□ □□□ □□ □□□ □□ □□□ □ □□□?
A. □□ □□
B. □□□ □□ □□
C. □□ □□(QA) □□
D. □□ □□
Answer: (SHOW ANSWER)
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: 404
□□ □ □□ □□□ □□□□ □□□□ □□□□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□□ □□□ □□ □□□ □□□□□.
B. □□ □□□□ □□ □□ □□ □□ □□ □ □□ □□□ □□□ □□□□ □□□□□.
C. □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□□.
D. □□ □□ □□□□ IT □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 405
□□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□□ □□□ □, □□ □□□ □ □□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□□□ □□□□ □□ □□□ □□ □□□□□.
B. □□ □□□ □□□□□ □□□□ □□□□□.
C. □□□□ □□□ □□ □□□ □□□□ □□□□□.
D. □□□ □□ □□ □□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.
The other options are less concerning for the IS auditor:
Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not

know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

NEW QUESTION: 406
□□ □ □□□□ □□ □□□□□ □□□ □□□ □□□□ □ □□ □□ □□□□ □□□ □□□. □□ □ □ □□□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□□□ □□□□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
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 that allows 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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 407
IS □□□□ □□ □□ □□ □□□□□ □□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
Audit findings should be communicated as early as possible to avoid misunderstandings, provide an opportunity for corrective action, and ensure transparency.
Option A (Incorrect):The planning phase involves defining audit scope, objectives, and methodology, but findings are not yet available to discuss with management.
Option B (Incorrect):The reporting phase formalizes audit results, but discussing issuesonlyat this stage may lead to delays in corrective action.
Option C (Incorrect):The follow-up phase ensures that management has implemented corrective actions, but this occursafterthe initial discussion of findings.
Option D (Correct):The fieldwork phase is when auditors activelygather evidence, analyze data, and identify issues. Discussing observationsduringthis phase allows for immediate clarification, validation, and resolution of misunderstandings before the final report.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Discusses audit engagement, reporting, and communication best practices.

NEW QUESTION: 408
□□□□□ □□□□□ □□□ □□ □□□ □□□ □□□ □ □□□□□ □□ □□□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□□
B. □□□ □□□
C. □□ □□ □□ □□□
D. □□ □□□
Answer: (SHOW ANSWER)
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: 409

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

A. □□

B. □□□

C. □□

D. □□

Answer: B (LEAVE A REPLY)

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 downtimeand disruption.

Option B (Correct):Aphased approachgradually implements the system in stages, allowing users toadaptand 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: 410

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

A. □□□

B. □□ □□□

C. □□ □□

D. □□ □□

Answer: B (LEAVE A REPLY)

Monitoringcapacity utilizationsupportsavailabilityby ensuring thatresources remain functional and do not exceed operational limits.

Option A (Incorrect):Integrityensures that data isaccurate and unaltered, but monitoring capacity thresholds primarily relates tosystem availability.

Option B (Correct):Availabilityensures that systems remainaccessible and functional, and monitoring capacity utilization helpsprevent downtimeandservice disruptions.

Option C (Incorrect):Confidentialityensures that data isprotected from unauthorized access, which is unrelated to capacity monitoring.
Option D (Incorrect):Nonrepudiationensures that actions can betraced to specific individuals, but it does not relate tocapacity monitoring.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Coverscapacity planning and monitoring for system availability.

NEW QUESTION: 411
□□ □ □□□□ □□□□□□□□ □□ □□ □□□□□ □□□□ □□□□ □□□ □ □ □ □□□□ □□□ □□□□□?
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: 412
□□ □ □□ □□□ □□□(EUC) □□□□□□□ □□ □□□ □□ □□ □ □□□ □□□ □ □□ □□□□□?

A. □□□□ □□□□ □□□□ □□□ □ □□
B. □□□□ □□□ □□
C. □□ □□□□ □□ □□ □□
D. □□□□□□□ □□ □□
Answer: D (LEAVE A REPLY)
Spreadsheets, often used in EUC, are prone to manual input errors and formula mistakes. These errors can significantly compromise the accuracy and integrity of financial reporting.
References
ISACA CISA Review Manual (Current Edition) - Chapter on End-User Computing (EUC) risks Industry Research on Spreadsheet Errors: Multiple studies highlight the prevalence of errors in spreadsheets, especially those used for financial purposes.

NEW QUESTION: 413
□ □□□ □□□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□ □□□□. □□ □ □□ □□□ □□□□ □□□ □□□□ □□ □□□ □ □□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□ □□ □□
B. □□ □□ □□
C. □□□ □□□
D. □□□□ □□□ □□
Answer: (SHOW ANSWER)
A computer-assisted technique is the most helpful method for an IS auditor to determine whether duplicate vendor payments exist on a complex system with a high volume of transactions. A computer-assisted technique is a tool or procedure that can be used to perform audit tests or procedures on data stored in electronic form. Examples of computer-assisted techniques include data analysis software, query tools, scripting languages, and specialized audit software. A computer-assisted techniquecan help an IS auditor to identify and extract duplicate payments from a large data set, perform calculations and comparisons, and generate reports and summaries. A computer-assisted technique can also provide more accuracy, efficiency, and coverage than manual methods.
Stratified sampling, statistical sampling, and process walk-through are not as helpful as a computer-assisted technique for this purpose. Stratified sampling is a sampling method that divides the population into subgroups based on certain characteristics and selects samples from each subgroup. Statistical sampling is a sampling method that uses probability theory to determine the sample size and selection criteria. Process walk-through is a review technique that involves following a transaction or process from start to finish and observing the inputs, outputs, controls, and documentation. These methods may be useful for other audit objectives, but they are not as effective as a computer-assisted technique for detecting duplicate payments in a complex and high-volume system.
References: ISACA Frameworks: Blueprints for Success, [ISACA Glossary of Terms]

NEW QUESTION: 414
□□ □ □□□ □□ □□ □□ □□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□ □□?
A. □□ □□
B. □□ □□
C. □ □□
D. □□□ □□
Answer: (SHOW ANSWER)
Water sensors are devices that can detect the presence of water or moisture in a given area. They are often deployed below the floor tiles of a data center to monitor for any water leaks that may damage the equipment or cause electrical hazards. Water sensors can alert the data center staff or trigger an automatic response to prevent or mitigate the water leakage.
The other options are not likely to be deployed below the floor tiles of a data center. Temperature sensors and humidity sensors are usually deployed above the floor tiles to measure the ambient conditions of the data center and ensure optimal cooling and ventilation. Air pressure sensors are typically deployed at the air vents or ducts to monitor the airflow and pressure distribution in the data center.
References:
Data Center Environmental Monitoring
Water Detection in Data Centers

NEW QUESTION: 415
□□ □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□ □□□ □, □□ □□ □ □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□ □□□□ □□ □□ □□
B. □□□ □□
C. □□□□□ □□ □□ □□□ □□□□□ □□□□□□□.
D. □□ □□ □□
Answer: C (LEAVE A REPLY)
The best answer is C. Insufficient due diligence performed on the vendor.
ISACA guidance on third-party and cloud risk repeatedly emphasizes the need for thorough vendor due diligence before entering or expanding a business relationship. When confidential backups are being migrated to a cloud solution, insufficient due diligence is the greatest concern because it can expose the organization to security, privacy, resilience, and compliance failures across the whole service arrangement.
Option A is relevant for retired media handling, but it is narrower than the overall third-party risk. Option B affects performance and growth, not necessarily confidentiality. Option D is a business issue, but not the greatest audit concern when confidential data is involved. Vendor due diligence is the most important control at this stage.
References (Official ISACA):

* ISACA, The Top 5 Cybersecurity Threats and How to Defend Against Them.
* ISACA Journal, The Encrypted Truth Is Already Out There.

NEW QUESTION: 416
□□ □□□ □□□□ 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: 417
□□ □ □□ □□□ □□□□□□ □□□ □□ □ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□?
A. IS □□□□ □□□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□□.
B. IS □□□□ □□□□□□ □□□ □□□□ □□ □□□□ □□□□□ □□ □□□ □□ □□□.
C. IS □□□□ □□□□□□ □□□ □□□ □□ □□□ □□□ □□ □□□ □□□□□ □.
D. IS □□□□ □□□□□□ □□□ □□ □□ □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
The IS auditor's independence would be most likely impaired if they implemented a specific control during the development of an application system. This is because the IS auditor would be auditing their own work, which creates a self-review threat that could compromise their objectivity and impartiality. The IS auditor should avoid participating in any operational or management activities that could affect their ability to perform an unbiased audit. The other options do not pose a significant threat to the IS auditor's independence, as long as they follow the ethical standards and guidelines of the profession.

NEW QUESTION: 418
□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□□. □ □ □ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□ □ □□□□ □□□ □□□ □□?
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 and 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 yourapps and data4 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

NEW QUESTION: 419
IS □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□ □ □□□□□ □□ □□□□ □□ □□□□□□□ □□□□ □□□ □ □□□ □□□ □□□□□□. □□ □□□ □□□ □ □□ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□(IDS)□ □□□□□□.
B. □□ □□ □ □□□ □□□□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
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, CISAReview Questions, Answers and ExplanationsDatabase - 12 Month Subscription2 What Is Cloud Security? | Google Cloud3
5 Cloud Application Security Best Practices | Snyk4

NEW QUESTION: 420
□□ □□□ □□ □□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□□
D. □□ □□
Answer: A (LEAVE A REPLY)
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 informationabout 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: 421
□□□ □□ □□□ □□□(EUC)□ □□□ □ □□ □ □□ □□□ □□ □ □□ □□□ □ □□?
A. IT □□□ □□ □□
B. □□ □□□□ □□□ □□□ □□
C. EUC □□ □□ □ □□□ □□□□□ □ □□
D. □□□ □□□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 422
□□ □ □□ □□ □□□□□ □□□ □□□ □□□□□□ □□□ □□ □□□ □□□ □ □□□ □□ □□□□ □□□ □ □ □□□□?
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: 423
□□□ □□ □□□□□ □□□□ □□ □□□□ □□ □□□□ □□□□. □□ □ □□ □ □□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□□?
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: 424
□ □□□ □□ □□□□ □□ □□□ □□ □□□□ □ □□□ □□ □□□ □□□□□ □ □□□□□□. □□ □□□□ □□□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□ □□□□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□?
A. □□ □□ □□□
B. □□□□ □□□
C. □□ □□ □□□
D. □□□□ □□□
Answer: (SHOW ANSWER)
The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying, analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible foroverseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not for managing project risks. The information security officer is responsible for ensuring that the project complies with the organization's information security policies and standards, but not for managing project risks. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 425
□□ □ □□□ □□□ □□□ □ □□□ □□□□□□ □□□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□?
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 dataon 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: 426
□□ □ □□□ □□ □□□ □□ □ □□ □□ □□□ □□□□ □ □□ □□□□ □□□ □ □□□□?
A. □□□□ □□□ □□□□□□ □□□□□.
B. □□□□□ □□ □□□ □□□□□.
C. □□□ □□ □ □□ □□ □□□
D. □□□ □ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The most effective control to protect information assets in a data center from theft by a vendor is to monitor and restrict vendor activities. A vendor may have legitimate access to the data center for maintenance or support purposes, but they may also have malicious intentions or be compromised by an attacker. By monitoring and restricting vendor activities, the organization can ensure that the vendor only performs authorized tasks and does not access or tamper with sensitive data or equipment. Issuing an access card to the vendor, concealing data devices and information labels, and restricting use of portable and wireless devices are also useful controls, but they are not as effective as monitoring and restricting vendor activities in preventing theft by a vendor. References:

CISA Review Manual, 27th Edition, page 3381
CISA Review Questions,Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 427
□□ □□□ □□ □□□□ □□ □□□□ □□ □□ □□□□ □□ □□□□ □□□ □□ □□ □□ □□□ □□□□□□.
□□ □ □□ □□□ □□□□ □□□ □ □□ □□□ □□□□□?
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 and Explanations Database3, Question ID: QAE_CISA_710.

NEW QUESTION: 428
□3□ □□□□□ □□ □□□ □□□ □□□□ □□□□. □□ □ □□ □□□ □□□□ □ □ □ □□□□ □ □□□ □□□□□?
A. □□□ □□□□□□□ □□ □□□ □□□□ □□□□.
B. □□□ □□ □□ □□□ □□ □□□□ □□□□.
C. □□□ □□□□ □□ □□□ □□□□□.
D. □□□□ □3□ □□□□□ □□□□□□.
Answer: (SHOW ANSWER)
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 and Implementation, Section 3.4: System Implementation.

NEW QUESTION: 429
□□ □□ □ □□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □ □□ □□□ □ □□□ □□□□□?
A. □□ □□□□ □□□ □□□□ □□ □□□□□□ □□
B. □□ □□□□□ □□□ □□
C. □□□ □□□ □□ □□ □□□□ □□□□□.
D. □□ □□□ □□□ □□ □□ □□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
To detect unauthorized disclosure of confidential documents sent over corporate email, monitoring all emails based on pre-defined criteria is the best approach. This involves setting up automated monitoring systems that analyze email content, attachments, and metadata to identify any potential unauthorized disclosures. By defining specific criteria (such as keywords related to confidential information), organizations can proactively detect and prevent leaks. Requiring encryption before sending documents (option A) is important but does not address monitoring for unauthorized disclosures. Firewalls (option B) protect the network but do not specifically focus on email content. Reporting outgoing emails marked as confidential (option C) relies onuser self-reporting and may not catch all incidents12. References: 1(https://www.isaca.org/resources/isaca-journal

/past-issues/2010/data-governance-for-privacy-confidentiality-and-compliance-a-holistic-approach) 2 (https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-6/best-practices-for- privacy-audits)

NEW QUESTION: 430
□□ □ □□□(PKI)□ □□□□ □□ □□□ □□□□□ □□ □ □□ □□□ □□ □□□ □□ □□□□□?
A. □□□ □□□ □ □ □□ □□ □□ □ □□□□ □□ □□
B. □□□ □□□ □□ □□ □□□ □□
C. □□□ □□□□ □□□□ □□□(IaaS)□ □□ □□
D. □□ □□□□ □□ □□□ □□ □ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 431
□□□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□□. □□ □ □□ □ □□□ □□□□ □ □□□ □□ □ □□□ □□□□□?
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 functionalityand 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: 432
□□ □ IT □□□ □□ □□□□□□□ □□□ □ IS □□□□ □□ □□ □□□□ □ □□ □ □□□□□?
A. □□□□□□□ □□ □□□□ □□□ □ □□□□.

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

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

NEW QUESTION: 434
□□ □ □□□ □□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□ □□ □□ □ □□ □□□□□?
A. □□□□ □□ □□□□□ □□ □□ □□□ □□□□□ □□□□□□.
B. □□□□ □□ □□□□□ □□ □□□□ □□□□ □□□ □□□□□.
C. □□ □ □ □□ □□□ □□ □□ □□□□□ □□□□ □□ □□□□□ □□□□□.
D. □□□□ □□ □□ □□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Data analytics is the process of collecting, transforming, analyzing, and visualizing data to gain insights and support decision making1. Data analytics can be used to facilitate the testing of a new account creation process by applying various techniques and methods to evaluate the quality, functionality, performance, and security of the process. One of the approaches that would utilize data analytics to test the new account creation process is to review new account applications submitted in the past month for invalid dates of birth.
This approach would involve the following steps:
Extract the data of new account applications from the source system, such as a database or a web service, using appropriate tools and methods.
Transform and clean the data to ensure its accuracy, completeness, consistency, and validity, using techniques such as data profiling, data cleansing, data mapping, and data validation2.
Analyze the data to identify any anomalies, errors, or outliers in the date of birth field, using methods such as descriptive statistics, exploratory data analysis, hypothesis testing, or anomaly detection3.
Visualize the data to present the findings and insights in a clear and understandable way, using tools and techniques such as charts, graphs, dashboards, or reports.
By reviewing new account applications submitted in the past month for invalid dates of birth, the tester can use data analytics to:

Verify if the new account creation process is working as expected and meets the business requirements and specifications for the date of birth field.
Detect any defects or issues in the new account creation process that may cause invalid dates of birth to be accepted or rejected incorrectly.
Measure and monitor the performance and reliability of the new account creation process in terms of data quality, accuracy, and completeness.
Evaluate and improve the test coverage and effectiveness of the new account creation process by identifying any gaps or risks in the test cases or scenarios.
Therefore, option C is the correct answer.
Option A is not correct because attempting to submit new account applications with invalid dates of birth is not a data analytics approach, but a functional testing approach that involves executing test cases or scenarios manually or automatically to validate the behavior and functionality of the new account creation process.
Option B is not correct because reviewing the business requirements document for date of birth field requirements is not a data analytics approach, but a requirements analysis approach that involves examining and understanding the needs and expectations of the stakeholders for the new account creation process.
Option D is not correct because evaluating configuration settings for date of birth field requirements is not a data analytics approach, but a configuration testing approach that involves verifying if the settings and parameters of the new account creation process are correct and consistent with the requirements.
References:
What is Data Analytics? Definition and Examples1
Data Transformation: Definition and Examples2
Data Analysis: Definition and Examples3
Data Visualization: Definition and Examples
Functional Testing: Definition and Examples
Requirements Analysis: Definition and Examples
Configuration Testing: Definition and Examples

NEW QUESTION: 435
□□□, □□ □ □□ □□□(IoT) □□□ □□ □□ □□□□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□□□ □□□□□ □□□□□ □□□□□.
B. □□□□ □□ □□□ □□□ □□□□ □□ □□ □□ □ □□□□ □□□ □□□□□.
C. □□ □□ □□□ □□ □□□ □□ □ □□ □□□ □□
D. □□ □ □ □□□ □□□□ □□ □□□ □□□ □□□□ □□
Answer: B (LEAVE A REPLY)
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: 436
□□ □□ □□□ □□□□ □, □□ □□□(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.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 437
□□ □□□(IS) □□□□ □ □□□ □□□□ □□□ □□ □□□(CASB) □□□□ □□□ □ □□□□. □□□□ □□□□ □ □□ □□□ □□□ □□ □ □□□□□?
A. □□□□ □□□□ □□□□□.
B. □□□□ □□□□ □□□□□.

C. □□□□ □□□□□ □□□□ □□□□□.
D. □□□□ □□□□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)
Periodic recertification of users ensures that only authorized individuals retain access to cloud services and helps identify and revoke access for users who no longer require it. This is a critical control for maintaining security and compliance in a cloud environment.
Classifying Cloud Services (Option A):This is foundational but does not verify ongoing user access.
Centrally Managing Users (Option B):While useful for consistency, it does not assess whether access rights are still valid.
Ensuring Cloud Process Resilience (Option C):This focuses on operational continuity rather than access control.
Periodic recertification aligns with governance practices to ensure access rights remain appropriate over time.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 438
□□ □ □3□ □□□ □□□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□ □□ □□□?
A. □□□ □□□□□ □□ □□□□ □□□ □□ □□ □□□
B. □□□ □□□□□ □□ □□ □□□ □□ □□
C. □□□ □□□□□ □□ □□ □□□□□ □□□
D. □□□ □□□□□ □□ □ □□ □□
Answer: (SHOW ANSWER)
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 inaccurate.
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 and Explanations Database - 12 Month Subscription

NEW QUESTION: 439
□□ □ IT □□ □□ □□□□ □□ □ □□□□ □□□ □□□□□?
A. IT □□ □□□ □□□
B. □□ □□□ IT □□□ □□□
C. IT □□ □□□ □□
D. □□□ □□□ □□ □□
Answer: B (LEAVE A REPLY)
The best evidence of an IT strategy correction's effectiveness is the synchronization of IT activities with corporate objectives. The IT strategy correction is a process of reviewing and adjusting the IT strategy to ensure that it aligns with and supports the corporate strategy and objectives. The synchronization of IT activities with corporate objectives means that the IT activities are consistent with and contribute to the achievement of the corporate goals and vision. The IS auditor can measure and evaluate the IT strategy correction's effectiveness by comparing the IT activities with the corporate objectives, and assessing whether they are aligned, integrated, and coordinated. The other options are not as good evidence of an IT strategy correction's effectiveness, because they either do not reflect the alignment of IT and business, or they are inputs or outputs of the IT strategycorrection process rather than outcomes or results. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

NEW QUESTION: 440
□ □□□ □□ □□ □□□ □□□□ □□□□. □□ □□□□ IT □□□□□ □□ □□ □ □□ □ □□□□ □□ □□□□ □ □□ □□□□ □□□□ □□□□. □□ □□□ □□ □ □□ □□□□ □□□□?
A. □□□

B. □□
C. □□□
D. □□
Answer: (SHOW ANSWER)
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: 441
□□ □ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □ □□ □□□□ □ □□□ □ □□□ □□□□□?
A. □□□ □□ □□□ □□ □□ □□
B. □□□ □□□ □□□ □□□□ □□□□.
C. □□□□ □□ □□ □□□□
D. □□□□ □□□ □□ □□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 442
IS □□□□ □□ □□□□ □□□□ IT □□□ □□ □□□□□ □□□ □□□□□ □□□ □ □□□□ □□ □□ □□ □□□ □□□□ □□□ □□□□□□. □□ □ □□□□ □□ □ □□□□ □□□□ □□□□ □ □□□ □□□ □□ □□□ □□□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□ □□
B. □□ □□ □□
C. IT □□□□ □□□□□
D. □□□□□ □□
Answer: D (LEAVE A REPLY)
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and

services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:
CISA Review Manual, 27th Edition, page 721
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 443
□□ □ □□ □□□ □□□□ □□□□□ IT □□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□□?
A. IT □□ □□ □□□ □□ □□□ □□□ □□□□□ □□
B. □□ □□□□ IT □□ □□ □□ □□□□ □□□□ □□ □□
C. □□□□ IT □□ □□□ □□□□ □□□□ □□
D. IT □□ □□ □□□ □□□ □□□ □□□□□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 444
□□ □□ □□ □□□ □□ □□ □, □□ □□ □□□ □□□□ □□□□ □□□ □□□ □ □ □□□ □□□□ □□ □□□ □□□□□□. □□□□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□.
□□□□ □□ □ □□ □□□ □□□ □□□□□?
A. □□□□□□ □□ □□ □□□□ □□ □□□ □□□□□□.
B. □□ □□□ □□ □□□□□ □□□□.
C. □□□□ □□□□ □□□ □□ □□□ □□□□□.
D. □□ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
When an auditor finds that the process owner is accepting residual risk beyond the organization's defined risk appetite, it is not appropriate to accept the action plan or wait until the next committee report.
Escalating to audit management (D) is the correct step. Audit management can then determine whether to escalate further to executive management or the audit committee.
Including in the next report (A) delays timely risk response.
Informing executive management directly (B) by passes the audit reporting hierarchy.
Accepting the plan (C) would be inappropriate as it ignores risk governance.
ISACA Reference: CISA Review Manual 27th Edition, Domain 1 (Governance and Risk Management), section on Risk appetite, residual risk, and auditor's role in escalation.

NEW QUESTION: 445

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

A. □□ □□ □□□ □□□□□.

B. □□ □□□ □□□ □□□□ □□□ □□□□□.

C. □□□□ □□ □□□ □□□ □ □□□ □□□□□.

D. □□□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

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: 446

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

A. □□□ □□□□□ □□ □□□ □□ □□

B. □□□ □□□□□ □□□□ □□ □□□ □□ □□ □□

C. □□ □□□□ □□ □□□ □□

D. □□ □□□ □□□□ □□□ □□□□

Answer: A (LEAVE A REPLY)

Thebiggest riskin cloud migration isdata security, especially unauthorized access by the cloud provider.

Option A (Correct):The cloud providermanages and stores organizational data, meaning that abreach, insider threat, or improper accessposes amajor risk. Properencryption and access controlsare critical.

Option B (Incorrect):Whilemulti-tenancy risks exist, cloud providers typically implement strongisolation mechanismsbetween clients.

Option C (Incorrect):Increased dependency on the provider is aconcern, but the impact depends onservice agreements and redundancy measures.

Option D (Incorrect):Limiting the right to audit is acompliance issue, butdata security risksare more critical.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Covers cloud computing risks and security considerations.

NEW QUESTION: 447

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

A. □□ □□□□ □□ □□ □□□□□□.

B. □□□□□ □□ □□□ □□□□□□□.

C. □□□□ □□□ □□ □□ □□□□□ □□□□ □□□□.

D. □□ □□□ □□ □□ □□□□□.

Answer: B (LEAVE A REPLY)

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

Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate1.

Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency1.

Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program1.

NEW QUESTION: 448

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

A. □□□□

B. □□ □□ □ □□

C. □□ □□□ □□(BCP) □□□ □□

D. □□□ □ □□□ □□□ □□□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 449

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

A. EUC □□□□

B. EUC □□□ □□

C. EUC □□ □□ □□

D. □□ □□□□ □□ EUC □□□

Answer: A (LEAVE A REPLY)

The best way to improve the visibility of end-user computing (EUC) applications that support regulatory reporting is to maintain an EUC inventory, as this provides a comprehensive and up-to-date list of all EUC applications, their owners, their locations, their purposes, and their dependencies. An EUC inventory can help identify and manage the risks associated with EUC applications, such as data quality, security, compliance, and continuity. EUC availability controls, EUC access control matrix, and EUC tests of

operational effectiveness are important forensuring the reliability and security of EUC applications, but they do not improve the visibility of EUC applications as much as an EUC inventory. References: CISA Review Manual (DigitalVersion), Chapter 3: Information Systems Acquisition, Development and Implementation, Section
3.4: End-user Computing

NEW QUESTION: 450
□□ □ □□□ □□□ □□ □ □□□ □□□□ □□ □□□□□?
A. □□□ □□ □□□ □□ □□ □□□ □□□ □ □□□□.
B. □□□□□□□ □□ □□ □□□ □ □ □□□□.
C. □□□ □□□□□ □□□ □ □□□□.
D. □□ □□□□ □□ □□ □□□□□ □□□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 451
□□ □□ □□□ □□□□ □□□□ IT □□□□ □□ □□ □□ □□(RPO)□ □□□ □□ □□□□□ □□□□□□. □□ □ □□□ □ □□□ □□□□ □ □□ □□□ □□□ □□ □□□ □□□□□?
A. □□□
B. □□□
C. □□□ □□
D. □□□ □□
Answer: B (LEAVE A REPLY)
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.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 452
□ □□□ □□ □□□□ □□□ □□ □□□ □□□□□ □□□□ □□ □□□(IS) □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□□□. □□□□ □□□□ □ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□ □□ □□□□ □□□ □□□□□.
B. □□□□ □□ □□□□ □□ □□ □□□ □□□□.
C. □□□□ □□ □□□□ □□□ □□□□□.
D. □□□ □□ □ □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
A risk and control framework is a set of principles, processes, and tools that guide an organization in identifying, assessing, managing, and monitoring the risks and controls that affect its objectives and performance. A risk and control framework helps an organization to align its risk appetite and tolerance with its strategy, culture, and values, and to ensure that its security controls are appropriate, effective, and efficient1.
Re-evaluating the organization's risk and control framework is the best recommendation to management because it can help them to:
Review the current risk environment and the sources, causes, and impacts of potential threats and vulnerabilities.
Update the risk assessment and analysis methods and criteria, such as likelihood, impact, severity, and priority.
Reconsider the risk response and treatment options, such as avoidance, reduction, transfer, or acceptance.
Realign the security controls with the risk profile and the business needs and expectations.
Evaluate the performance and effectiveness of the security controls using key indicators and metrics.
Identify the gaps, weaknesses, or inefficiencies in the security controls and implement corrective or improvement actions.
Communicate and report the risk and control status and results to relevant stakeholders.
Re-evaluating the organization's risk and control framework can help management to determine whether the current security controls are excessive or not, and to make informed and rational decisions on how to adjust them accordingly.

NEW QUESTION: 453
□□ □ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□□□□ □□□□ □ □□ □□?
A. □□ □□ □□ □□□
B. □□□□□
C. □□ □□□ □□

D. □□□□ □□ □□□

Answer: (SHOW ANSWER)

Capability maturity models (CMMs) are frameworks that help organizations assess and improve their processes in various domains, such as software development, project management, service delivery, and cybersecurity1. CMMs define different levels of process maturity, from initial to optimized, and describe the characteristics and best practices of each level. By using CMMs, organizations can benchmark their current processes against a common standard, identify gaps and weaknesses, and implement improvement actions to achieve higher levels of process maturity2. CMMs can also help organizations align their processes with their strategic goals, measure their performance, and increase their efficiency, quality, and customer satisfaction3.

Therefore, the use of CMMs would best enhance a process improvement program, as they provide a systematic and structured approach to evaluate and improve processes based on proven principles and practices. Option C is the correct answer.

Option A is not correct because model-based design notations are graphical or textual languages that help designers specify, visualize, and document the structure and behavior of systems4. While they can be useful for designing and communicating complex systems, they do not directly address the process improvement aspect of a program.

Option B is not correct because balanced scorecard is a strategic management tool that helps organizations translate their vision and mission into measurable objectives and indicators. While it can be useful for monitoring and evaluating the performance of a program, it does not provide specific guidance on how to improve processes.

Option D is not correct because project management methodologies are sets of principles and practices that help organizations plan, execute, and control projects. While they can be useful for managing the scope, schedule, cost, quality, and risk of a program, they do not focus on the process improvement aspect of a program.

References:

Guide to Process Maturity Models2

What is CMMI? A model for optimizing development processes1

Capability Maturity Model (CMM): A Definitive Guide3

Model-Based Design Notations4

Balanced Scorecard

Project Management Methodologies

NEW QUESTION: 454

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

A. □□□ □□ □□□(UAT)

B. □□□□ □□□

C. □□□ □□ □□□

D. □□ □□□

Answer: C (LEAVE A REPLY)
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: 455
□□□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□, □□ □□□□ □□ □□□ □□□□ □□□?
A. □□ □□ □□ □ □□ □□□ □□ □□ □□
B. □□ PIN □□ □□
C. □□□□ □□ □□ □□□□ □□ □□□□ □□
D. □□□□ □□□□(CCTV) □□
Answer: (SHOW ANSWER)
Periodic review of access profiles by management is an additional control that is required when using swipe cards to limit employee access to restricted areas. Swipe cards are a type of physical access control that use magnetic stripes or radio frequency identification (RFID) to store and transmit information about the cardholder's identity and access rights. Swipe cards can help to prevent unauthorized entry, protect sensitive assets and data, and monitor access activity. However, swipe cards alone are not enough to ensure effective access control. They need to be complemented by other controls, such as:
Periodic review of access profiles by management: This is a type of logical access control that involves verifying that the access rights assigned to each cardholder are appropriate, necessary, and consistent with the organization's policies and procedures. Periodic review of access profiles can help to detect and correct any errors, inconsistencies, or violations in the access control system, such as outdated, excessive, or redundant access rights, segregation of duties conflicts, or unauthorized changes. Periodic review of access profiles can also help to ensure compliance with internal and external audit requirements and regulations.
Implementation of additional PIN pads: This is a type of multi-factor authentication (MFA) that requires the cardholder to enter a personal identification number (PIN) in addition to swiping their card. MFA can enhance the security of the access control system by adding

another layer of verificationand 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: 456
□□□□ □□□ □□□ □□ □□□□□ □□□ □□□□ □□□ □□ □□□ □□ □□□ □□. □□ □□□□□ □□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□ □ □□ □□□?
A. □□ □□□□ □□□□ □□□ □□□ □□ □□□□□□.
B. □□ □□□□□ □□□ □□□□ □□□□□.
C. □□ □□□□□ □□□□ □□ □□□ □□□□□.
D. □□ □□□(VPN)□ □□ □□ □□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 457
□□ □□□ □□ □□□□ □□ □□□□ □□□ □□ □□□ □□ □□ □□□□ □□□ □□□□□□.
□ □□□ □□□□ □□□ □□□ □□ □□□□□ □□□ □□ □□ □□□□□.
□□ □ □ □□□ □□□□ □□ □□□ □□□ □□□□□?
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: 458
□□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□ □ □□ □□□ □□ □□ □ □□ □ □□□□□?
A. IS □□ □□□ □□□
B. □□□ □□□ □□ □□ □□□ □□□
C. □□□□ □□□ □□ □□□ □□
D. □□□□ □□□ □□□□ □□□□□ □□□
Answer: (SHOW ANSWER)
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: 459
IS □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□. □□ □ □□ □□□ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□ □□ □□□ □□□□□□□.

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

NEW QUESTION: 460
□□ □ □□ □□□(IS) □□□□ □□□ □□□□□□ □□□□(EA) □□□□□ □□□ □ □□ □□□□ □ □□□ □□□□□?
A. IT □□□□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□.
B. □□□□ □□ □□□□ CIO□ □□□ □□□□.
C. □□ □□ □□ □□□ EA □□□□□□ □□□□□.
D. EA □□□□□ IT □□□ □□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)
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: 461
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: 462
IS □□□□ □□□ □□ □ □□□□ □□ □□ □□□□□ □□□□ □□ □□ □□□□ □□. □□□ □□□□ □□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□ □□□ □ □□ □□
B. □□□ □□□ □□ □□ □□ □□
C. □□ □□ □□□□ □□□ □□ □□ □□
D. □□□□ □□□□ □□□ □□ □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 463
□□ □ □□ □□ □□□ □□ □□□ □□□ □□□□□?
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: 464
□□ □ □□□□□ □□□ □□ □□□ □□□□ □ □□□□ □□ □□□□□?
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: 465
□□ □ □□ □□ □□□□□□(CMDB)□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□□□ □□ □□□ □□ □□□□□ □□□□ □□
B. □□ □□□ □□ □□□ □□□□ □□□□□ □□□□□.
C. □□ □□□ □□□ □□□ □□□□ □□
D. □□ □□ □□ □□□ □□□□□ □□
Answer: D (LEAVE A REPLY)
The best answer is D. To document relationships between configuration items.
ISACA's configuration management guidance identifies the value of a CMDB in maintaining information about configuration items and their relationships. That relationship view is what supports effective impact analysis, change management, incident response, and dependency understanding across the environment.
Option A is too narrow. Option B describes monitoring rather than configuration management. Option C may be one data element in some environments, but the defining value of a CMDB is not physical location tracking. The central purpose is documenting configuration items and how they relate to one another.
References (Official ISACA):
* ISACA Glossary / configuration management references.

NEW QUESTION: 466
□□ □□ □□□ □□ □ □□□ □□ □□□□□.
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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 467
□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□ □□□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
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: 468
□ □□□ □□ □□□□ □□□□□ □□□□□□. □□ □ □□ □□□ □□□□ □□ □ □ □ □ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
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: 469
□□□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□.
A. □□□ □□.
B. □□ □□.
C. □□□□.
D. □□□ □□.
Answer: A (LEAVE A REPLY)
The best answer is A. Release management.
In continuous delivery, code moves frequently from development toward production, but the key control point that connects development output to live production deployment is release management. ISACA explains that continuous delivery takes integration output that has met release criteria and updates the application in production. That means the practical bridge between development and production is the release process that governs packaging, approval, timing, and movement into production.

Option C. DevOps is closely related, but it is broader than the specific connector. ISACA describes DevOps as focusing on automation and integration of processes before and after software release into production. That makes DevOps the broader operating model, while release management is the specific connector between development and production in the delivery pipeline.
Option B. Log management is important for monitoring and troubleshooting, but it does not connect development to production.
Option D. Data management is also important, but it is not the delivery bridge in this context.
Therefore, the correct answer is A, because release management is the function that controls and enables the movement of approved changes from development into production.
References (Official ISACA):
* ISACA Journal, Speeding Up Software Delivery With Effective Change Management - continuous delivery updates production with integration output meeting release criteria.
* ISACA Journal, Three Strategies for a Successful DevSecOps Implementation - DevOps is broader automation/integration around release into production.

NEW QUESTION: 470
□□ □ □□□ □□□□□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□□ □□(DES)
B. □□ □□□ □□(AES)
C. □□ □ □□□(PKI)
D. □□ □□□(VPN)
Answer: (SHOW ANSWER)
For online payment security, bothconfidentiality(protection of data) andnonrepudiation(ensuring the sender cannot deny a transaction) are essential.
Option A (Incorrect):DES is outdatedandinsecurefor modern encryption needs. It has been replaced by stronger algorithms.
Option B (Incorrect):AES provides strong encryption(confidentiality) but does not handlenonrepudiationon its own.
Option C (Correct):PKI (Public Key Infrastructure)is the best solution because it providesencryption for confidentialityanddigital signatures for nonrepudiation, ensuring bothsecuretransactions andauthenticationof parties involved.
Option D (Incorrect):AVPN secures network traffic, but it does not address nonrepudiation, which is critical in online payments.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets- Covers encryption, PKI, and secure payment processing.

NEW QUESTION: 471

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

NEW QUESTION: 472
□□ □□ □□□ IT□ □□ □□□□□ □□□□ IT □□ □□□□ □□ □□□ □□□□ □.
A. □□□ □□ □□□ □□□ □□□ □□□□ □.
B. □□□□ □□□□ □ □□□□ □□ □□□.
C. □□□□□□ □□□□(EA)□ □□.
D. IT □□□ □□□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
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 needsagainst 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: 473

IT □□□□□ □□ □□ □ □□ □□□□ □□□□ □ □□□ □□ □ □□□□□?
A. □ □□□□□ □□ □□□ IT □ □□□□□ □□
B. □□ □□ □ □□□□ □□□□ □□□ □□
C. IT □□□□□□ □□□ □□□□□ □□□ □□□□□ □□ □□
D. □□□□□□ IT □□□□□□ □□□□ □□ □□
Answer: C (LEAVE A REPLY)
Controls to minimize risk and maximize value for the IT portfolio should be the most important consideration when conducting a review of IT portfolio management, because they ensure that the IT portfolio aligns with the business strategy, objectives, and priorities, and that the IT investments deliver optimal benefits and outcomes. Assignment of responsibility for each project to an IT team member, adherence to best practice and industry approved methodologies, and frequency of meetings where the business discusses the IT portfolio are also relevant aspects of IT portfolio management, but they are not asimportant as controls to minimize risk and maximize value. References: CISA Review Manual (Digital Version),Chapter 1, Section 1.2.3

NEW QUESTION: 474
□□□□□□□ □□□□ □□ □□□□ □□□□ □ □□□□□. □ □□ □□□ □□□ □□ □□ □□ □□□□ □□□□□. □□□□ □□□□ □□□□ □□□□□ □□□□ □ □ □ □□□□ □□ □□□ □□□□□?
A. □□□□□ □□ □□
B. □□ □□□ □□□ □□□□ □□□ □□
C. □ □□ □□□ □□ □□□ □□
D. □□ □ □□□□ □□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected. Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete.
Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human errors, but it cannot guarantee that the data is accurate or consistent with the source. References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

NEW QUESTION: 475
□□ □ □□□□ □□□□□ □□ □□ □□□□□ □□□□□□ □□ □□ □ □□□□ □□□ □□□□□?
A. □□□□□□ □□ □□ □□ □□□ □□□
B. □□□□ CEO □ CIO□ □□ □□
C. □□□□□ □□□ □3□ □□ □□
D. □□□□□ □□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
The results of a third-party review provided by the vendor would provide the best evidence that a cloud provider's change management process is effective, because it would be an independent and objective assessment of the vendor's compliance with best practices and standards for managing changes in the cloud environment. A third-party review would also include testing of the vendor's change management controls and procedures, and provide recommendations for improvement if needed.
Minutes from regular change management meetings with the vendor would not provide sufficient evidence, because they would only reflect the vendor's self-reported information and may not capture all the changes that occurred or their impact on the cloud services.
Written assurances from the vendor's CEO and CIO would also not provide sufficient evidence, because they would be based on the vendor's own opinion and may not be verified by external sources. A copy of change management policies provided by the vendor would not provide sufficient evidence, because it would only show the vendor's intended approach to change management, but not how it is implemented or monitored in practice.
References:
ISACA Cloud Computing Audit Program, Section 4.5: Change Management
Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, Section 4.3:
Change Management

NEW QUESTION: 476
□□ □ □□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□□ □□
B. □□□ □□□
C. 2□□ □□ □□
D. □□□□□ □□□□ □□ □□
Answer: D (LEAVE A REPLY)
The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System- enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and

recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system.
Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (DigitalVersion), Chapter 3, Section 3.2

NEW QUESTION: 477
□□ □□□ □□□□ □□ □□□ □□ □□□□ □□ □□ □□ □□□ □□□□□ □□ □□□□□.
□□ □□ □□□ □□ □□□ □□□ □□□□□ □□ □□□ □□ □□□ □□ □ □□□ □□?
A. □□ □□
B. □□□□□
C. □□□□ □□
D. □□ □□□
Answer: B (LEAVE A REPLY)
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: 478
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: 479
□□ □ □□ □□ □□ □□□□□ □□□□ □□ □ □□□□ □□ □□□□□?
A. □3□ □□□□ □□□ □□
B. □□□ □□ □□ □□□
C. □□□ □□□□ □□ □□ □□□□□□.
D. □□□ □□ □□ □□
Answer: (SHOW ANSWER)
The effectiveness of a security awareness training program is best indicated by a reduction in unintentional violations. When employees are well-trained and aware of security practices, they are less likely to inadvertently violate security policies or make mistakes that could lead to breaches. While other factors (such as third-party social engineering tests, employee satisfaction, and completion rates) provide valuable insights, the ultimate goal of security awareness training is to minimize unintentional errors and improve overall security posture12. References: 1(https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2
/considerations-for-developing-cybersecurity-awareness-training)
2(https://www.isaca.org/resources/news- and-trends/isaca-now-blog/2023/security-awareness-training-a-critical-success-factor-for-organizations)

NEW QUESTION: 480
□□ □ □□ □□□ □□□□ □□□□ □□□□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□□□□ □□□□ □□□□□□.
B. □□□□ □□ □ □□□ □□□□□.
C. □□□□□□ □□ □□□ □□□□□.
D. □□□ □□ □□□□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 481
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.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 482
□□□ □□ □□□□ □□ □ □□□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□ □ □□□□□ □□□□□□. □□ □ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□.
B. □□ □□□ □□ □□ □ □□□ □□□□□.
C. □□ □□□ □□□ □□□□ □□ □□□ □□□□□.

D. □ □□ □□□ □□ □□□ □□□ □□□ □□□□.

Answer: C (LEAVE A REPLY)

The most important factor for the organization to ensure when reducing the retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for defining the retention and disposal requirements for the data under their custody, based on business, legal, regulatory, and contractual obligations. The policy should reflect the data owner's decisions and obtain their approval. The policy should also include a risk-based approach, but this is not as important as complying with data owner responsibilities. The retention period should allow for review during the year-end audit, but this may not be necessary for low-value transactions that have minimal impact on financial reporting. The total transaction amount may have some impact on financial reporting, but this is not a direct consequence of reducing the retention period. References:
CISA Review Manual, 27th Edition, pages 414-4151
CISA Review Questions, Answers and ExplanationsDatabase, Question ID: 255

NEW QUESTION: 483

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

A. □□ □□ □□(CSA)

B. □□ □□ □□

C. □□□□□ □□□

D. □□ □□

Answer: (SHOW ANSWER)

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: 484

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

A. □□□ □□□ □□ □□ □□□ □□□□□.

B. □□□ □□□ □□□ □□ □□□□□ □□□□□.

C. □□ □□□ □□ □□□ □□□□□ □□

D. □□ □ □□ □□□ □□ □□ □□ □□

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 485

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

A. □□ □□

B. □□ □□

C. □□ □□□

D. IT □□□ □□□□

Answer: C (LEAVE A REPLY)

File checksums are values that are calculated from the contents of a file and can detect any changes or corruption in the file. They are used to verify that the files that are transferred or processed through system interfaces are not altered in any way. File checksums are more effective than periodic audits, file counts, or IT operator monitoring, which are other types of controls that can help ensure the integrity of system interfaces, but they are not as reliable or timely as file checksums.

NEW QUESTION: 486

□□ □□ □ □□□(PKI) □□ □ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□ □ □□□ □□ □□□□□?

A. □□ □□ □□□

B. □□□ □□

C. PKI □□ □□□

D. □□□ □□ □□

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation:
A Certification Practice Statement (CPS) is a detailed document that describes the practices a Certificate Authority (CA) uses when issuing and managing digital certificates. It includes procedures for handling compromised private keys, revocation, renewal, and security controls.
Certificate policy (B): High-level rules governing certificate usage, but not operational details.
PKI disclosure statement (C): Provides users with general PKI-related information.

Certificate revocation list (D): A technical mechanism listing revoked certificates, but not the procedures for managing compromise.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on PKI components and certificate lifecycle management.

NEW QUESTION: 487
□□□□ □□□□□□ □□ □ □□□ □□ □□ □□□ □□□ □□□□ □□□□ □□□ □ □□□□ □□□□ □ □□ □□□ □□□ □□ □□□ □□ □ □□□□□?
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: 488
□□ □ □□□ □□□□ □□□□□□ □□ □□□□ □□□ □□□□ □□ □□□□□?
A. □□□□□(DMZ)
B. □□□□ □□ □□ □□□(IDS)
C. □□□□ □□ □□□□□□ □□□ □□□□
D. □□□□ □□ □□ □□ □□□(IDS)
Answer: B (LEAVE A REPLY)
A heuristic intrusion detection system (IDS) provides the most protection against emerging threats, as it uses behavioral analysis and anomaly detection to identify unknown or zero-day attacks. A heuristic IDS can adapt to changing patterns and learn from previous incidents, making it more effective than a signature-based IDS, which relies on predefined rules and signatures to detect known attacks. A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, and it can provide some protection against external threats, but not against internal or emerging threats.

Real-time updating of antivirus software is important to protect against malware, but it may not be sufficient to prevent new or sophisticated attacks that exploit unknown vulnerabilities. References: CISA Review Manual (Digital Version) 1, page 452-453.

NEW QUESTION: 489
□□□ □□□ □□ □□□□□ □□□ □□ □□□ □□□ □□□□ □□□□. □□ □ □ □ □□□ □□□ □□□□□?
A. □□□ □□ □□ □□
B. □□ □ □□□ □□□□□.
C. □□□ □□ □□□(UAT)□ □□□□□.
D. □□□ □□□□□□ □□□□□□
Answer: A (LEAVE A REPLY)
Performing user acceptance testing (UAT) is the most important activity before implementing a new system, as it ensures that the system meets the user requirements and expectations, and that it is free of major defects. Documenting last-minute enhancements, performing a pre-implementation audit, and ensuring that code has been reviewed are also important activities, but they arenot as critical as UAT. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2

NEW QUESTION: 490
□□ □ □□□ □□ □□□□ □□□ □□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□ □□□□□?
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: 491
□□□ □□ IT □□□ □□□□ □□□□□(SaaS) □□□□□□□ □□□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□.
A. IT □□ □□□.
B. IT □□ □□□.
C. □□□□□□□(CFO).
D. □□ □□ □□ □□□(CRO).
Answer: B (LEAVE A REPLY)

NEW QUESTION: 492
□□□□ □□ □ □ □□ □□□ □□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□ □ □□□□□□. □ □□, □□□ □□ □□□ □ □□ □□□ □□ □□ □□□ □□□□□ □□□□□□. □□ □□ □□□ □□□ □□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
The approach adopted by management in this scenario is risk avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:
CISA Review Manual, 27th Edition, page 641
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 493
□□□□□ □□ □□ □□□□ □□□□ □□□□. □□ □□ □□ □□□ □□□□□ □ □ □□□□ □□□ □□□□ □□□□□.
A. □□□ □□ □□ □□(UPS) □□□ □□ □□□ □□□□
B. □□ □□□□ □□ □□□ □□□□
C. □□□ □□□ □□□
D. □□ □□ □□□ □□□□ □□
Answer: D (LEAVE A REPLY)
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: 494
□□ □ IT □□ □□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□□□□□□ □□ □□ □□□□ □□□□□ □□□□ □□□□□.
B. □□ □□□□ □□□□□□□ □□ □□ □□□ □□ □ □□ □□□□ □□□□ □□ □□□.
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 and Explanations Database, Question ID 202

NEW QUESTION: 495
□□ □ IT □□ □□ □□□□□ □□□□ □□ □□□ □□□ □□□□□?

A. □□□□ □□ □□ □□ □□□ □□□□□ □□
B. □□□ □□□□□ □□□□□□□ □□ □□ □□
C. □□□ □□ □□ □□□ □□□ □□□.
D. IT □□□ □□ □□ □ □□ □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The primary purpose of IT capacity management is to ensure that IT infrastructure can meet current and future performance requirements in a cost-effective manner.
* Option A is correct because it directly relates to capacity management goals.
* Option B (rapid deployment) relates more to change management.
* Option C (security concerns) is outside the scope of capacity management.
* Option D (reducing cost/time) may be a secondary benefit but not the primary objective.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on capacity management and IT service performance.

NEW QUESTION: 496
IS □□□□ □□□□□□ □□□ □□ □□ □□□ □□□□ □, □□ □□□ □□□□ □ □ □□□□□ □□ □□□ □□ □ □□□□□□. □ □□□□ □□ □□□ □□□ □□□ □□?
A. □□□□□□ □□ □□
B. □□□ □□□ □□
C. □□□ □□□ □□
D. □□□ □□□ 10 □□□□
Answer: B (LEAVE A REPLY)
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 thefunctionality, 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 and Explanations Database - 12 Month Subscription

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop

CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 497
□□ □ □□ □□□ □□□□ □□□ □□ □□□ □□(BCP)□ □□□ □ □□ □□□□ □ □□□ □□□□□?
A. BCP□ □□□ □□□ □□□□□□ □□□.
B. BCP□ □□ □□□ □□ □□□□.
C. BCP□ □□ □□□□ □□□ □□ □□□□□.
D. BCP□ □□ □□□ □□□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources,procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
A). The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
B). The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.
C). The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue that can be resolved.

Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization.
Approval by senior management helps to ensure that the BCP is aligned with the organization's strategy, objectives, and priorities, and that it has sufficient resources and authority to be implemented. Approval by senior management also helps to increase the awareness and commitment of the organization's stakeholders to the BCP. While having no approval by senior management may affect the credibilityand acceptance of the BCP, it does not affect the overall validity or effectiveness of the BCP. References: Working Toward a Managed, Mature Business Continuity Plan - ISACA, ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Disaster Recovery and Business Continuity Preparedness for Cloud-based ...

NEW QUESTION: 498
□□□ □□ □□□ □□□□ □□□□ □□□□□?
A. IT □□ □□□
B. □□□ □□□
C. □□□□□□ □□□(DBA)
D. □□ □□ □□□
Answer: (SHOW ANSWER)
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: 499

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

NEW QUESTION: 500
□□ □□□ □□ □□□□ □ □□□□□□□ □□ □□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□ □□ □□□□□□. □□ □□ □□ □□ □□□ □□ □ □□ □□□ □□ □□□ □□□□ □□□□.
A. □□□□ □□ □□(SQL) □□□
B. □□ □□□□.
C. □□□ □□(DoS).
D. □□.
Answer: A (LEAVE A REPLY)
Validation controls are used to check the input data from the user before processing it on the server. If the validation controls are moved from the server side to the browser, it means that the user can modify or bypass them using tools such as browser developer tools, JavaScript console, or proxy tools. This would increase the risk of a successful attack by structured query language (SQL) injection, which is a technique that exploits a security vulnerability in an application's software layer that allows an attacker to execute arbitrary SQL commands on the underlying database. SQL injection can result in data theft, data corruption, or unauthorized access to the system.
Buffer overflow, denial of service (DoS), and phishing are not directly related to the validation controls in a web application. Buffer overflow is a type of attack that exploits a memory management flaw in an application or system that allows an attacker to write data beyond the allocated buffer size and overwrite adjacent memory locations. DoS is a type of attack that prevents legitimate users from accessing a service or resource by overwhelming it with requests or traffic. Phishing is a type of attack that uses fraudulent emails or websites to trick users into revealing sensitive information or installing malware.
References:
Client-side form validation - Learn web development | MDN
JavaScript: client-side vs. server-side validation - Stack Overflow
SQL Injection - OWASP

NEW QUESTION: 501
IS □□□□ □□□ □□ □□□ □□□ □□□□□ □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 maynot be able to resume its critical business operations within the expected time frame, which may result insignificant 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 ofthe backup process

NEW QUESTION: 502
□□ □ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □ □□ □□□□□?
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: 503
□□ □ □□ □□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□ □□□□□?
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: 504
□ □□□ □□□□□□ □□□□(EA) □□□□ □□ □□□□ □□□ □□□□□ □□ □ □□ □□□□□ □□□□□□. □ □□□ □□□ □ □□ □□□ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
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: 505
□□ □□ □ □□□□ □□□□ □□ □□□ □□□ □□□□□ □□□□ □□□□ □ □ □ □□□ □□□ □□□□□?
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 and Explanations Database, Question ID: 2642

NEW QUESTION: 506
□□ □ □□ □□□ □□□□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□□ □ □□ □□□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□ □ □□□□ □□ □□□□ □□□□□□□.
B. □□ □□□ □□□ □ □□□□ □□ □□□ □□□□□.
C. □□ □□ □□□ □ □□□ □□□ □□□□□.

D. □□ □□□ □□□ □□ □□□ □□□□□ □□□□□□.

Answer: A (LEAVE A REPLY)

The most effective control for protecting the confidentiality and integrity of data stored unencrypted on virtual machines is to monitor access to stored images and snapshots of virtual machines. Images and snapshots are copies of virtual machines that can be used for backup, restoration, or cloning purposes. If data stored on virtual machines are unencrypted, they may be exposed or compromised if unauthorized or malicious users access or copy the images or snapshots. Therefore, monitoring access to stored images and snapshots can help detect and prevent any unauthorized or suspicious activities, and provide audit trails for accountability and investigation.

Restricting access to images and snapshots of virtual machines, limiting creation of virtual machine images and snapshots, and reviewing logical access controls on virtual machines regularly are not the most effective controls for protecting the confidentiality and integrity of data stored unencrypted on virtual machines. These controls may help reduce the risk or impact of data exposure or compromise, but they do not provide sufficient visibility or assurance of data protection. Restricting access to images and snapshots may not prevent authorized users from abusing their privileges or credentials. Limiting creation of virtual machine images and snapshots may not address the existing copies that may contain sensitive data. Reviewing logical access controls on virtual machines regularly may not reflect the actual access activities on images and snapshots.

NEW QUESTION: 507

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

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: 508

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

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

NEW QUESTION: 509
IS □□ □□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □, □□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□(IDS)□ □□□□ □ □□□.
A. □□□ □ □□.
B. □□□□□(DMZ).
C. □□□ □□□□.
D. □□□
Answer: D (LEAVE A REPLY)
The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize.
The other options are not as effective as placing an IDS between the firewall and the Internet:
Placing an IDS between the firewall and the organization's web server would not protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network.
Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by twofirewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall.
Placing an IDS between the firewall and the organization's network would not protect the organization's network from external attacks that bypass the firewall. The organization's network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.

NEW QUESTION: 510
□□ □ □□□□□ □□ □□□□ □□ □□□ □□□ □ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□?
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 and Implementation, CISA ReviewManual (Digital Version)

NEW QUESTION: 511
□□ □ □□ □□ □□□ □□ □□□□ □□□(RPA)□ □□□ □□ □□□ □□□ □ □ □□ □□□?
A. □□ □□□ □□□□
B. □□ RPA □□□ □□□□□
C. □□□□ □□ □□(BIA)□ □□ □□
D. □□□□ □□
Answer: D (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 512

IS □□□□ □□ □□□ □□ □□□ □□ □□□□ □□□□ □□□□. □□□□ 5□□ □ □ □□ □ 1□□ □□□□ □□□ □□□□ □□□□□. □ □□ □□□ □□ □□□□ □ □□□ □□ □□ □□□ □□□□□?

A. □□□ □□□□ □□ □ □□□□.

B. □□□ □□□ □□□ □□□□ □□ □□ □ □□□□.

C. □□ □□□ □□ □□□ □□□□ □□ □ □□□□.

D. □□□ □□□□ □□□ □ □□□□.

Answer: D (LEAVE A REPLY)

Evidence of a control's performance must be verifiable. A missing signature or date means there is no confirmation that the review was actually performed. This undermines the completeness and reliability of the control. Accuracy (A) and content (B) relate to quality but do not address the missing attestation. Industry standards (C) may be relevant, but the auditor's main concern is that the absence of sign-off creates doubt about whether the control occurred at all. ISACA audit guidance highlights that sufficient and appropriate evidence is required to support the conclusion that a control is operating as designed. References (ISACA): ISACA Standards - Evidence Collection; ISACA ITAF Guidelines.

NEW QUESTION: 513

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

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 and Exercises - Homeland Security
What is Penetration Testing? | Types and Stages | Imperva

NEW QUESTION: 514
□□ □□ □ □□ □□□□□ □□□□ □□□ □ □□□ □□□ □□□□ □ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□ □□□□ □□ □□□ □□
B. □□ □□□□ □□ □□ □□
C. □□ □□□□□□□ □□ □□□□ □□□□□ □□□□□.
D. □□ □□□□ □□□ □□□
Answer: C (LEAVE A REPLY)
The best answer is C. Periodically restoring backup media for key databases.
ISACA guidance is very clear that backup restoration should be tested periodically. A backup is only useful if it can actually be restored successfully within business needs. Organizations sometimes assume that because backups exist, recovery is assured, but ISACA specifically warns that recovery procedures and restoration capability must be tested.
Option A is important for resilience, but offsite storage does not prove the backup is recoverable. Option B helps administration and tracking, but inventory alone does not validate restorability. Option D protects confidentiality of backup data, but it does not ensure successful recovery. The strongest control for recoverability is periodic test restoration.
References (Official ISACA):
* ISACA, Ensuring Data Security: The Importance of Cloud Backups and Drill Testing
* ISACA Journal, Governance of Key Aspects of System Patch Management - recommends periodic testing of backup restoration.
* ISACA Journal, IS Audit Basics: Backup and Recovery

NEW QUESTION: 515
□□□□ 3□ □□□ □□□□□□ □□ □□□□□ □□□ □ □□ □□□ □□ □ □□□ □□?
A. □□□□ □□ □□
B. □□ □□ □□
C. □□□□ □□ □□
D. □□□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 516
□□ □□□ □□□ □□ □□ □□□, □□□ □□□, □□□ □□□□ □□ □□□□ □□ □□□□□. □□ □□□ □□ □□ □□□□□□ □□ □□□□□.
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: 517
□□ □□□□□□ □ □□ □□ □□□ □□□ □□ □□ □□ □□ □□ □ □□□□□ □ □ □□□ □□□?
A. □□□□ □□□ □□□ □□□□□□
B. □□□□ □□ □□□□ □□□□□□
C. □□□□ □□ □□□□□□
D. □□ □□ □□□□□□
Answer: (SHOW ANSWER)
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: 518
□□ □ □□ □□ □□□□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□□□

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

NEW QUESTION: 519
□□□ □□□□ □□□□ □□□ □□□ □□□ □ □□□ □ □□ □□□ □□□ □ □□ □□□□ □□ □□□ □□ □ □□□□□?
A. □□□□ □□ □□ □□□ □□ □□□.
B. □□□□ □□ □□□□ □□□□ □□□.
C. □□□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□ □□□.
D. □□□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 520
□□ □ □□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □□.
B. □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□□□.
C. □□ □□□□□□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□□□.
D. □ □□□□□ □□ □□□ □□ □□□ □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition] , page 281.

NEW QUESTION: 521
IS □□□□ □□□ □□□ □□□□□ □□□□□□ □□□ □□□□ □□ □□ □□□ □ □□□ □□□□. □□ □□ □□□□ □□ □□ □□□□□ □□ □□□ □□□□ □□ □ □□□□□?

A. □□ □□□ □□ □□□ □ □□ □□□□ □□□□□□□□□□.
B. □□□□ □□ □□□ □□□ □ □□ □□□□ □□□□□□□□□□.
C. □□ □□ □□□ □□ □ □□ □□□□ □□□□□□□□□□.
D. □□□□ □□□ □□□ □□□□□ □□□□□ □□□ □□ □□□
Answer: (SHOW ANSWER)
The most appropriate population to sample from when testing for remediation of findings identified in an organization's user provisioning process is all users provisioned after the final audit report was issued. This is because the final audit report is the official document that communicates the audit findings, recommendations, and action plans to the management and other stakeholders. It also establishes a baseline for measuring the progress and effectiveness of the remediation efforts. Therefore, sampling from the users provisioned after the final audit report was issued would provide the most relevant and reliable evidence of whether the audit issues have been resolved or not.
The other options are not as appropriate as option C, as they may not reflect the actual status of the remediation efforts. All users provisioned after the finding was originally identified may include users who were provisioned before the final audit report was issued, which may not capture the full impact of the remediation actions. All users provisioned after management resolved the audit issue may not be accurate, as management's resolution may not be verified or validated by an independent party. All users who have followed user provisioning processes provided by management may not be representative, as there may be exceptions or deviations from the processes that could affect the remediation results.
References:
6: What Is User Provisioning? Definition, Process and Best Practices - Spiceworks
7: What Is User Provisioning? All You Need to Know in One Place - G2
8: What is User Account Provisioning? - Tools4ever
9: What Is Provisioning and Deprovisioning? | Okta

NEW QUESTION: 522
□ □□□ □□ □□□ □□ □□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□. □□ □ □ □□ □□□ □□ □ □□□□ □□□ □□□□□?
A. □□□ □□□ □□ □□□ □□.
B. □□ □□ □□□ □□□ □□ □□ □□ □.
C. □□ □□□□ □□□ □□ □□ □□.
D. □□ □□ □□ □ □□□ □□□ □□
Answer: (SHOW ANSWER)
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: 523
□□ □□□ □□□□ □□ IT □□ □□□ □□ □□ □□□ □□□□ □□□□?
A. □□ □□
B. □□ □□
C. IT □□□
D. □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 524
□□□ □□□ □□ □□□ □□□ □□ □□□ □□ □ 24□□ □□□ □□ □□□ □□□ □ □□□. □□ □ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□ □□ □□ □□ □□(KPI)□ □□□□□.
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: 525
□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. □□ □□ □□□ □□ □□ □□□(CAE)□ □□□ □□ □□□□□.
B. □□ □□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□□□.
C. □□ □□ □□□ □□ □□□□ □□□□.
D. □□ □□ □□□ □□ □□□□ □□□ □□ □□□□□.
Answer: (SHOW ANSWER)
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: 526
□□□ □□ □□□□ □□□ □ □□□□ □ □□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□□.
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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 527
□□ □ □□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□ □□ □ □□□□ □□ □□□□□?
A. □□□□□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□ ID□ □□□□□.
B. □□ □□ □□□ □□ □□□□□.
C. □□ □□ □□□ □□□□ □□□□□□ □□ □□□□□.
D. □□□□□□ □□ □□□□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□□ □ □ □□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 528
□□ □□□ □□□□ □ □□□ IT □□ □ □□□ □□□□ □□□□. □□ □ □□ □□□ □ □□□ □□□□□?
A. □□□□ □□□ IT □□ □□□ □□□□.
B. □□ □□ □□□□ □□□□ □□□□.
C. IT □□□ □□ □□ □□□ □□□□ □□□□.
D. IT □□ □□□ □□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern for an IS auditor when evaluating an organization's IT strategy and plans is that IT is not engaged in business strategic planning, as this indicates a lack of alignment between IT and business objectives, which could result in inefficient and ineffective use of IT resources and capabilities. The absence of a defined IT security policy, the nondistribution of business strategy meeting minutes, and the inadequate documentation of IT strategic planning are also issues that should be addressed by an IS auditor, but they are not as significant as IT's noninvolvement in business strategic planning. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.1

NEW QUESTION: 529
□□□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□□. □□ □ □□ □ □□□ □□□□ □ □□□ □□ □ □□□ □□□□□?
A. □□□□□□ □□□ □□□ □□□□ □□□□□ □□□□□.
B. □□□ □□□□□ □□□□□ □□□□□.
C. □□ □□□ □□□ □□ □□ □□ □□□□□.
D. □□□□□□ □□ □□□□□ □□□ □ □□□□.
Answer: D (LEAVE A REPLY)
The programmer having access to the production programs is the most likely control weakness that would have contributed to the unauthorized changes to the payroll system report. This is because the programmer could modify the production code without proper authorization, documentation, or testing, and bypass the change management process. This could result in errors, fraud, or data integrity issues in the payroll system.
The programmer should only have access to the development or test environment, and the production programs should be under the control of a librarian or a change manager.
References
ISACA CISA Review Manual, 27th Edition, page 254
4 Types of Internal Control Weaknesses
ACCT 4631 - Internal Auditing: CIA Quiz Topic 6 Flashcards

NEW QUESTION: 530
□□□ □ □□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □ □□ □□□ □□ □ □□ □□ □ □□□ □□□?

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

NEW QUESTION: 531
IS □□□□ □□ □□□ □□□□ □ □ □□ □□□ □□□□ □□□□ □□□□ □□□ □□□. □□□□ □□ □ □□ □□□ □□□ □□□ □□□□.
A. □□□ □□□□ □□ □□□ □□□ □□□□□.
B. □□□□ □□□ □□□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□ □□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 532
□□ □ □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□□ □□ □ □□□□ □□. □□ □ □□ □□□□ □□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□ □ □□□□□?
A. □□□ □ □□ □□□ □□□□ □□ □□□□ □□□□□□.
B. □□ □ □□ □□ □□□□ □□□□ □□□ □□□ □□□□ □□□□□.
C. □□□ □□□□ □□□□ □□□ □□□ □□ □□□ □□□□ □□□□□□ □□□□ □.
D. □□□ □□□ □□□□ □□□□ □□□□□□.
Answer: B (LEAVE A REPLY)
Reviewing input and output control reports to verify the accuracy of the system decisions is the most important procedure for the IS auditor to perform during the post-implementation review of intelligent-agent software for granting loans to customers, because it can help identify any errors or anomalies in the system logic or data that may affect the quality and reliability of the system outcomes. Reviewing systemand error logs, signed approvals, and systemdocumentation 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: 533
□□ □□□ □□□ □□ □□ □□ □□ □□□ □□□□□ □□□ □□□ □□□□□□ □. □□ □ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□ □ □□□□□ □□ □□ □ □□□ □□□□□?
A. □□ □□ □□ □□
B. □□ □□□ □□ □□ □ □□
C. □□ □□□ □□□
D. □□□ □□□ □□ □□ □□□□ □□
Answer: (SHOW ANSWER)
A compliance gap analysis is a detailed review of an organization's current state of compliance against a specific regulation or standard. It helps identify the areas and controls that are not meeting the requirements, assess their risk levels, and determine the corrective actions that can be taken to achieve compliance12. A compliance gap analysis is the most useful tool for an IS auditor to review when auditing against a new regulation, as it provides a clear and comprehensive picture of the compliance status, gaps, and remediation plan of the organization.
References
1: Information Security Architecture: Gap Assessment and Prioritization - ISACA
2: How to perform Compliance Gap Analysis? - Sprinto

NEW QUESTION: 534
□□ □ □□ □□ □□(DRP)□ □□ □□□ □□□□□ □□□?
A. □□ □□ □□□
B. □□ □□□□□□□ □□ □□
C. □□ □□□□ □□□□ □□
D. □□ IT □□ □□□
Answer: A (LEAVE A REPLY)
The primary objective of a disaster recovery plan is recovery of interrupted IT-related activities in a way that minimizes the impact of the disruption. Official ISACA definitions describe disaster recovery as activities and programs designed to return the enterprise to an acceptable condition and restore critical business functions through a DRP. ISACA's glossary defines a disaster recovery plan (DRP) as a set of human, physical, technical, and procedural resources to recover an interrupted activity within a defined time and cost. Among the answer choices, A. Minimizing loss of information is the best match. ISACA guidance states that a DRP contains procedures for restoring systems and data, minimizing loss of information and downtime, and ensuring business continuity. This makes option A the strongest answer because it captures a direct purpose of the DRP itself.
Option B ("Assessing the risk of key applications") is an important planning activity, but it is not the primary objective of the DRP. Risk assessment is part of developing continuity

capability, not the ultimate aim of the plan. ISACA continuity guidance treats assessing risks and impacts as a step in the DRP process, not the main end goal.
Option C ("Identifying key business processes") is also an important prerequisite, typically associated more with business impact analysis and business continuity planning. It helps define what must be protected and restored, but it is not itself the primary objective of the DRP. ISACA distinguishes business continuity activities from disaster recovery, with DR focusing more specifically on restoring IT systems, infrastructure, and data after disruption.
Option D ("Documenting all IT assets") may support recovery preparedness, but this is clearly not the primary objective of a DRP. Asset documentation is administrative and supportive; the goal of the plan is restoration and recovery with minimal disruption and data loss.
Therefore, A is the correct answer because official ISACA material directly states that the DRP is intended to restore systems and data while minimizing loss of information and downtime.
References (Official ISACA):
* ISACA Glossary, Disaster Recovery (DR) and Disaster Recovery Plan (DRP) definitions.
* ISACA Now Blog, Disaster Recovery and Business Continuity Preparedness for Cloud-Based Start- Ups - states that a DRP includes restoring systems and data, minimizing loss of information and downtime, and ensuring business continuity.
* ISACA Journal, Working Toward a Managed, Mature Business Continuity Plan - distinguishes DR as focusing on rebuilding/recovering site, infrastructure, and data.
* ISACA Journal, Information System Contingency Planning Guidance - supports that planning activities such as risk awareness are part of planning, not the primary objective itself.

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

NEW QUESTION: 536
□□ □□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□□□ □□ □□ □□□□□ □□□□ □□
B. □□□□ □□□ □□□□□
C. □□ □□□ □□ □□□ □□□ □□□□ □□
D. □□ □□ □□□ □□□□ □□□□ □□
Answer: A (LEAVE A REPLY)

The primary purpose of obtaining a baseline image during an operating system audit is to identify atypical running processes. A baseline image is a snapshot of the normal state and configuration of an operating system, including the processes that are expected to run on it. By comparing the current state of the operating system with the baseline image, an IS auditor can detect any deviations or anomalies that may indicate unauthorized or malicious activity, such as malware infection, privilege escalation, or data exfiltration. A baseline image can also help an IS auditor to assess the performance and efficiency of the operating system, as well as its compliance with security standards and policies.
Verifying antivirus definitions (option B) is not the primary purpose of obtaining a baseline image, although it may be a part of the baseline configuration. Antivirus definitions are the files that contain the signatures and rules for detecting and removing malware. An IS auditor may verify that the antivirus definitions are up to date and consistent across the operating system, but this does not require obtaining a baseline image.
Identifying local administrator account access (option C) is not the primary purpose of obtaining a baseline image, although it may be a part of the baseline configuration. Local administrator accounts are user accounts that have full control over the operating system and its resources. An IS auditor may identify and review the local administrator accounts to ensure that they are properly secured and authorized, but this does not require obtaining a baseline image.
Verifying the integrity of operating system backups (option D) is not the primary purpose of obtaining a baseline image, although it may be a part of the backup process. Operating system backups are copies of the operating system data and settings that can be used to restore the system in case of failure or disaster. An IS auditor may verify that the operating system backups are complete, accurate, and accessible, but this does not require obtaining a baseline image.
References: : Linux security and system hardening checklist : CISA Certification | Certified Information Systems Auditor | ISACA : CISA Certified Information Systems Auditor Study Guide, 4th Edition : CISA - Certified Information Systems Auditor Study Guide [Book]

NEW QUESTION: 537
□□ □ □□□ □□□□□□ □□ □□□□ □□□□ □□□□□□ □□□ □□□ □ □□ □ □□ □□ □□ □□□ □□□□□?
A. □□□ □□□□ □□ □ □□ □□□
B. □□□ □□
C. □□□ □□
D. □□□□ □□ □
Answer: C (LEAVE A REPLY)

NEW QUESTION: 538
□□ □□□□ □□□□ □□□ □□□□□□□□ □□□ □□□□ □□□□ □□□□ □ □□ □□□□□□□.

□□ □ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□□ □□□□ □□□□.
B. □□ □□ □ □□□ □□ □□ □□ □□ □□ □□□ □□□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□ □□□□□□ □□□□□.
D. □□□ □□ □□ □□□□ □□□□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
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: 539
□□ □ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□ □□□□ □□ □□□ □□□□□□.
D. □□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Data loss can occur due to various reasons, such as accidental deletion, hardware failure, malware infection, theft, or unauthorized access. Data classification procedures can help to identify and protect sensitive data, but they are not sufficient to prevent data loss. The most effective way to protect against data loss is to conduct periodic security awareness training for employees, which can educate them on the importance of data security, the best practices for data handling and storage, and the common threats and risks to data.

NEW QUESTION: 540
□ □□□□ □□□ □□□ □□ □□ □ □□□(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: 541

□□ □ □□ □ □□□□□□ □□□□(EA)□ □□ □□□ □□□□□?

A. □□ IT □□□□ □□□□ □□□□□.

B. □□□□ □□ □□□□□ □□□□ □□

C. □□□□ IT □□□ □□□□ □□□□□.

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

Answer: D (LEAVE A REPLY)

The best answer is D. To structure IT projects to achieve desired business results.

ISACA guidance describes enterprise architecture as a top-down, business-driven discipline focused on business capabilities, strategy, and alignment of people, process, and technology. Enterprise architecture is not primarily about individual systems or day-to-day operations. Its purpose is to ensure that change initiatives and IT investments are organized in a way that supports the enterprise's strategic and business outcomes.

Option A is too narrow because EA is broader than designing single systems. Option B is only one specialized area within the overall architecture landscape. Option C is more aligned with operations management than enterprise architecture. The strongest answer is the one linking EA to business-driven structuring of initiatives and results.

Therefore, the correct answer is D, because enterprise architecture exists to align and structure IT initiatives so the organization can achieve desired business results.

References (Official ISACA):

* ISACA, Developing Business Capabilities Using COBIT 5 - enterprise architecture focuses on business capabilities supporting strategy.
* ISACA Journal, Enterprise Security Architecture-A Top-down Approach - architecture bridges business risk, process requirements, and technical issues.
* ISACA Journal, Information Security Architecture: Gap Assessment and Prioritization - supports business-driven architectural alignment.
* ISACA, Using COBIT 2019 to Plan and Execute an Organization Transformation Strategy - IT governance and management should create value from IT initiatives.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 542
□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □?
A. □□ □□□ □□□ □
B. □□ □□□ □□ □□□ □□□ □
C. □□ □□ □□□ □□□ □□
D. □□□□□ □□□ □□□ □
Answer: (SHOW ANSWER)
The concept of materiality is most important for an IS auditor to apply when planning an audit engagement, because it helps the auditor to determine the scope, objectives, procedures and resources of the audit.
Materiality is the degree to which an omission or misstatement of information could affect the users' decisions or the achievement of the audit objectives. By applying the concept of materiality, the auditor can focus on the most significant and relevant areas of the audit and avoid wasting time and effort on trivial or immaterial matters. The other options are not as important as planning an audit engagement, because they are either based on or affected by the materiality assessment done during the planning phase. References:
ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.31
ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques forIS Audit and Assurance Professionals, section 12022

NEW QUESTION: 543
□□ □□□ □□□ □□ □□□□□ □□□□□ □□□□□ □□□□ □□ □□ □□□ □ □□ □□□□.
A. □□ □□□□ □□□□ □ □□ □□ □□.
B. □□ □□ □□ □□□ □□ □ □□□.
C. □□ □□□ □□□ □□□□ □□ □□.
D. □□ □□ □□□ □□ □□.
Answer: A (LEAVE A REPLY)
The charging method for IS resources is the way that the IS function allocates its costs to the users or business units that consume its services. The charging method can affect the behavior and incentives of the users and the IS function, as well as the efficiency and

effectiveness of the IS resources. Therefore, choosing an appropriate charging method is an important decision for the IS function and its stakeholders.

One of the possible charging methods is to charge specific costs that can be tied back to specific usage. This means that the IS function tracks and measures the actual consumption of each user or business unit for each IS service, and charges them accordingly. For example, if a user uses 10 GB of storage space, 5 hours of CPU time, and 100 MB of network bandwidth, the IS function will charge them based on the unit costs of these resources. This charging method has the advantage of encouraging the most efficient use of IS resources, as it provides clear and accurate feedback to the users about their consumption and costs, and motivates them to optimize their usage and avoid waste or overuse. This charging method also aligns the interests of the IS function and the users, as both parties benefit from reducing costs and improving efficiency.

The other possible charging methods are:

Total utilization to achieve full operating capacity: This means that the IS function charges a fixed amount to each user or business unit based on their proportion of the total operating capacity of the IS resources. For example, if a user or business unit has 10% of the total computing power allocated to them, they will pay 10% of the total IS costs. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates a mismatch between the interests of the IS function and the users, as the IS function benefits from increasing costs and capacity, while the users bear the burden of paying for them.

Residual income in excess of actual incurred costs: This means that the IS function charges a markup or profit margin on top of its actual incurred costs to each user or business unit.For example, if a user or business unit consumes $100 worth of IS resources, the IS function will charge them $120, where $20 is the residual income for the IS function. This charging method has the disadvantage of discouraging efficient use of IS resources, as it increases the costs for the users and reduces their value for money. This charging method also creates a conflict between the interests of the IS function and the users, as the IS function benefits from increasing costs and profits, while the users suffer from paying more than they should.

Allocations based on the ability to absorb charges: This means that the IS function charges different amounts to different users or business units based on their ability to pay or their profitability. For example, if a user or business unit is more profitable or has a higher budget than another user or business unit, they will pay more for the same amount of IS resources. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates an unfair and arbitrary distribution of costs among the users or business units, as some paymore than others for no valid reason. References: 1:

Charging Methods for IT Services - IT Process Wiki 2: IT Chargeback Methods - CIO Wiki 3: IT Chargeback - Wikipedia

NEW QUESTION: 544
□□ □ □□ □□□ □□□□ □□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □ □□ □□□□□?
A. □□□ □□ □ □□□ □□ □□□ □□□□ □□□ □□□□.
B. □□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □□□□.
C. □□□□□ □□□□□□(NDA) □□□ □□□□ □□□ □□□□.
D. □□□ □□□ □□□ □ □□ □□ □□□ □□□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
Failure torevoke access upon terminationposes the greatest security risk, as ex-employees could still access sensitive data or systems.
No Policy to Revoke Access (Correct Answer - A)
A terminated employee retaining access can lead todata breaches or insider threats.
Example:A former employee misuses active credentials to access financial systems.
Lack of Security Awareness Training (Incorrect - B)
Important but does not pose an immediate security risk like an active ex-employee account.
No NDAs (Incorrect - C)
Protects intellectual property but is not as critical as system access.
No Access Revocation for Role Changes (Incorrect - D)
Still a concern, but ex-employees with active access are ahigherrisk.
References:
ISACA CISA Review Manual
NIST 800-53 (Access Control)

NEW QUESTION: 545
□□ □□ □□ □□ □□□□ IS □□ □□□□ □□□ □□ □□□□□□□ □□□□□□ □□□□ □□ □□□ □□□□□□. □□ □□□□ □□ □□□ □□□ □□ □□□ □□ □□□.
A. □□ □□.
B. □□□ □□ □□.
C. IT □□□ □□.
D. IT □□□□□ □□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 546
□□□□ □□□ □□ □□□(CASB)□ □□ □□□ □□□□ □□□□ □□□□□(SaaS) □ □□□ □□□□ □□□□□. □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□ □ □□□□□?

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

NEW QUESTION: 547
IT □□ □□□ □□ □□ □□□(ROI) □□□□ □□□□ □□ □ □□□ □□□ □□□□.
A. □□□ □□□ □□.
B. □□ □□ □□.
C. □□ □□ □□.
D. □□ □□ □□□ □□.
Answer: D (LEAVE A REPLY)
One benefit of return on investment (ROI) analysis in IT decision making is that it provides the basis for allocating financial resources. ROI analysis is a method of evaluating the profitability or cost-effectiveness of an IT project or investment by comparing the expected benefits with the required costs. ROI analysis can help IT decision makers prioritize and justify their IT initiatives, allocate their financial resources optimally, and demonstrate the value contribution of IT to the organization's goals and objectives. Basis for allocating indirect costs, cost of replacing equipment, and estimated cost of ownership are not benefits of ROI analysis in IT decision making. These are more inputs or outputs of ROI analysis that could be used to calculate or estimate the costs or benefits of an IT project or investment. References: [ISACA CISA Review Manual 27th Edition], page 307

NEW QUESTION: 548
□□ □ □□□□□ □□□□ □□ □□ □□□□ □□□□ □ □□ □□□ □□ □□□ □ □ □□□□□?
A. HR
B. □□ □□□
C. □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
The best answer is B. Senior management.
The culture that supports an effective internal control system is set from the top. ISACA's governance and culture guidance consistently treats culture as a management and leadership responsibility. Senior leadership establishes tone, values, expectations, accountability, and behavioral norms that shape how controls are designed, followed, and

enforced across the enterprise. A strong control culture depends on visible commitment from leadership, not just procedural ownership by operational teams.
Option A. HR supports the culture through hiring, training, and policy reinforcement, but HR does not have primary accountability for the overall control environment.
Option C. Line management plays an important role in day-to-day control execution, but enterprise culture is primarily driven by senior leadership.
Option D. Internal audit evaluates and provides assurance over the control system; it does not own or establish the control culture because doing so would impair independence.
Therefore, B is the correct answer because senior management is primarily accountable for establishing the tone and culture that enable an effective and efficient internal control system.
References (Official ISACA):
* ISACA Journal, Auditing Your Organizational Culture.
* ISACA Now Blog, Culture as a Corporate Asset.
* ISACA Digital Video/Podcast, Understanding and Assessing Organization Culture.
* ISACA Journal, Auditing Culture.

NEW QUESTION: 549
□□ □ □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□□□□. □□ □ □□ □□□ □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□□ □□□□□ □□□ □□□□ □□□□□.
B. □□ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□.
C. □□ □□ □□□□□ □□ □□□□ □□□ □ □□□□□.
D. □□□□□ □□ □ □ □ □□ □□□□□ □□□□□□□.
Answer: (SHOW ANSWER)
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. Asurvey 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 ImplementationReview - ISACA, Survey - ISACA, Business Case - ISACA

NEW QUESTION: 550
□□ □ □□ IT □□□□ □□ □ IS □□□ □□□□□ □□ □□ □□□ □□□ □□□□ □?
A. □□ IT □□□□ □□□□□□ □□□ □□ □□
B. □□ □□ □ □□ □□ □□□□□ □□ □□ □□
C. □□, □□ □ □□□□ □□ □□□ □□□□ □□□ □□□□□.
D. IT □□□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
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: 551
□ □□□□ □□ □ □□ □□□□ □□□□ □□ □□ □□ □□□ □ □□ □□□ □□□ □□□ □□□□ □□□□ □□□ □□□□□. □□□ □□□ □□□ □□ □ □□□ □□ □ □□□□□?
A. □□ □□ □□
B. □□□ □□ □□
C. □□□ □□ □□□□□□ □□□ □ □□
D. IT □□ □□ □□
Answer: (SHOW ANSWER)
Real-time replication to a second data center means that any changes made to the primary data center are immediately copied to the secondary data center. This can improve data availability and performance, but also introduces the risk of propagating malicious or erroneous changes to the backup data center. If a cybersecurity attack compromises the primary data center, it may also affect the secondary data center, making it difficult or impossible to recover from the attack using the replicated data. Therefore, option C is the greatest risk associated with this change.
Option A is not correct because version control issues are more likely to occur with batch processing backup, which may create inconsistencies between different versions of the

data. Option B is not correct because real- time replication may reduce system performance at the primary data center, but it may also improve system performance at the secondary data center by reducing latency and network traffic. Option D is not correct because although real-time replication may increase IT investment cost, this is not a risk but a trade-off that the organization has to consider.
References:
Data Replication: The Basics, Risks, and Best Practices1
Best Practices for Data Replication Between Data Centers2
The Good, Bad, and Ugly of Data Replication3

NEW QUESTION: 552
□□□ □□□□□□ □□□ □□ □□□□ □□□ □□ □ □□□□□□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□□ □□ □□□□□ □□□□ □□□□□□□.
B. □□ □□□ □ □□□ □□□ □□□□□ □□□ □ □□□□.
C. □□ □□ □□□□ □□ □□□ □□□ □□□□□□.
D. □□ □□ □□□□□ □□□□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, andintegrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 553

□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□ □□□□ □□□ □□□ □□
B. □□ □□□ □□□ □□ □□□ □□
C. □□□□□ □□□□ □□ □□□□ □□□ □□□ □
D. □□□ □□□ □□ □ □□ □□
Answer: B (LEAVE A REPLY)
The impact if corrective actions are not taken is the most important factor to consider when scheduling follow- up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:
CISA Review Manual(Digital Version), Chapter 2, Section 2.5.31
CISA Review Questions, Answers and Explanations Database, Question ID 207

NEW QUESTION: 554
□□□ □□ □□□□□ □□□ □ □□□ □□□□ □□ □□□ □□□ □□ □ □□□□ □?
A. □□□□ □□ □□ □□ □□ □□
B. □□□□□□ □□ □□ □□
C. □□□ □□□ □□ □□ □□
D. □□□□□□ □□□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
The most important responsibility of data owners when implementing a data classification process is determining appropriate user access levels (option C). This is because:
Data owners are the persons or entities that have the authority and responsibility for the business processes and functions that collect, use, store, and dispose of data1.
Data owners are accountable for ensuring that the data is handled in compliance with the applicable laws, regulations, policies, and standards, such as the GDPR and the PIPEDA1234.
Data owners are in the best position to determine the purpose and necessity of collecting and retaining data, as well as the risks and benefits associated with it1.
Data owners should consult with other stakeholders, such as the risk manager, the database administrator (DBA), and the privacy manager, to establish and implement appropriate data classification policies and procedures2.
Data classification is the process of organizing data in groups based on their attributes and characteristics, and then assigning class labels that describe a set of attributes that hold true for the corresponding data sets345.
Data classification helps organizations to identify, manage, protect, and understand their data, as well as to comply with modern data privacy regulations345.

Data classification also helps to determine appropriate user access levels, which means defining who can access, modify, share, or delete data based on their roles, responsibilities, and needs345.
Determining appropriate user access levels is the most important responsibility of data owners when implementing a data classification process, as it ensures that only authorized and legitimate users can access sensitive or important data. This provides confidentiality, integrity, availability, and accountability of data345.
Reviewing emergency changes to data (option A), authorizing application code changes (option B), and implementing access rules over database tables (option D) are not the most important responsibilities of data owners when implementing a data classification process. These are more related to the operational aspects of data management, which are usually delegated to other roles, such as the DBA or the IT staff. The data owner should oversee and approve these activities, but not perform them directly1.

NEW QUESTION: 555
□□ □□□(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 and Explanations Database, Question ID: 260

NEW QUESTION: 556
□□ □□□ □□ □□□□ □ □□ □□ □□□ □□□□□□ □□ □□□□□ □□ □□ □ □□□□ □□□□.
□□ □ □ □□□ □□ □□□ □ □□ □□ □□□□□?

A. □□□ □□ □□□
B. □□ □□ □□ □□□
C. □□□ □□ □□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
A backlog consumption report is a report that shows the amount of work that has been completed and the amount of work that remains to be done in a project. It is a useful tool for measuring the progress and performance of a web-based customer service application development project, as it can indicate whether the project is on track, ahead or behind schedule, and how much effort is required to finish the project. A backlog consumption report can also help identify any issues or risks that may affect the project delivery. Critical path analysis reports, developer status reports and change management logs are also helpful for evaluating a project, but they are not as helpful as a backlog consumption report, as they do not provide a clear picture of the overall project status and completion rate. References:
[Backlog Consumption Report Definition]
Backlog Consumption Report | ISACA

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 557
Zero Trust □□□□□□ IS □□□□ □□□□ □□□□ □□□□□□ □□□□ □□ □□ □□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□□ □□ □ □□
B. □□ □□□ □□ □□□ □□ □□ □□
C. □□□ □□ □□ □□
D. □□ □□□ □ □□□ □□□□ □□ □□□□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
In Zero Trust architecture (ZTA), the principle is "never trust, always verify." The most important aspect for an IS auditor to evaluate is whether access control policies are properly designed, aligned with industry standards, and consistently enforced. These policies define how identities, devices, and contexts are authenticated and authorized before gaining access.

Option A: Perimeter firewalls are less relevant in Zero Trust, which minimizes reliance on network boundaries.
Option C: Access reviews are important but are periodic, not continuous enforcement.
Option D: Secure remote protocols are necessary but part of broader access policy enforcement.
Option B: Correct - policies are the foundation of Zero Trust security.
ISACA Reference: ISACA's "Zero Trust and Audit Considerations" guidance; CISA Review Manual 27th Edition, Domain 5, section on identity, access, and authentication controls.

NEW QUESTION: 558
□□ □□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□□□. □□ □ □□□ □□ □□□ □□□ □ □□ □ □□ □□ □□ □□□ □□□□□?
A. □□□□ □□ □□□ □□□□ □□□□□□□□ □□□□□ □□□
B. □□ □□□□ □□□ □□□ □□ □□ □□ □ □□ □□
C. □□ □□□□ □□ □□□ □□ □□ □□
D. □□□□ □□ □□□□ □□ □□□□
Answer: (SHOW ANSWER)
While all the options can help reduce the risk of data leakage, providing education and guidelines to employees on the use of social networking sites would be the most effective. This is because it directly addresses the issue at hand - the use of social networking sites for business purposes1. Education and guidelines can help employees understand the risks associated withsocial media use and teach them how to safely and responsibly use these platforms for business purposes1. This includes understanding privacy settings, recognizing phishing attempts, and knowing what information should not be shared on these platforms1.
References:
10 Social Media Guidelines for Employees in 2023 - Hootsuite

NEW QUESTION: 559
□□ □ □□□ □ □□□□□□□ □□□ □ □□□ □□□ □□□□ □ □□ □□□□ □ □ □□□ □□□□□?
A. □□□ □□ □□
B. □□□ □□□
C. □□ □□□ □□(BCP)
D. □□ □□□□
Answer: B (LEAVE A REPLY)
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: 560
□□ □□ □□□ □□ □□, □□ □□□□ □□ □□ □□□ □□□□□ □□□ □□□□ □□□. IS □□□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□□□□. □□ □ □□ □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□ □□□□.
B. □□□ □□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□□□□.
D. □□ □□ □□□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 561
□□□□ □□□ □□ □□□(CASB)□ □□□ □□□□□ □□□□ □□□ □ □□□ □□ □□ □ □□ □□ □□□ □□□ □□ □ □□□□□?
A. □□□ □□ □□□□
B. □□ CASB □□ □□
C. □□ □□ □□ □□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)
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 preventunauthorized 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: 562
□□ □□□ □□□□ 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: 563
□□ □ □□ □□□ □□□□ □□□□ □□ □□ □□ □□□ □□□ □□ □□ □ □□□ □□ □□ □□□□□?
A. □□
B. □□□
C. □□□
D. □□□
Answer: A (LEAVE A REPLY)
Independence would be most impacted if an IS auditor were to assist with the implementation of recommended control enhancements, as this would create a conflict of interest and impair the objectivity and credibility of the IS auditor. Integrity, materiality, and accountability are important attributes of an IS auditor, but they are not directly affected by the involvement in the implementation of control enhancements. References: CISA Review Manual (Digital Version), Chapter 1: Information Systems Auditing Process, Section 1.1: IS Audit Standards, Guidelines and Codes of Ethics

NEW QUESTION: 564
□□ □ □□□□□ RFID□ □□□ □ □□ □□□ □□□□ □□ □□□□ □ □□□ □□ □□□?
A. □□ □□
B. □□□□□

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

NEW QUESTION: 565
IS □□□□ □□ □□ □□□□ □□ □□□ □□ □□ □□□□ □□ □□□□□□. □□ □□ □□□ □ □□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□ □□□ □□□□□.
B. □□ □□□ □ □□□□□.
C. □□□ □□□ □□□□.
D. □□ □□ □□□(IDS)□ □□ □□□□□.
Answer: (SHOW ANSWER)
Fine tuning the intrusion detection system (IDS) is the best recommendation to reduce the number of false positive alerts that overwhelm the log management system, because it can help adjust the sensitivity and accuracy of the IDS rules and signatures to match the network environment and traffic patterns. Establishing criteria for reviewing alerts, recruiting more monitoring personnel, and reducing thefirewall rules are not effective solutions to address theroot cause of the false positive alerts, but rather ways to cope with the consequences. References: CISA Review Manual (Digital Version), Chapter 5, Section5.4.3

NEW QUESTION: 566
□□ □□□(IS) □□ □□□□ □□ □ IT □□□□□ □□□□ □□ □□□ □□ □□□ □ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□ □□ □□□ □□□□□□□.
B. □□□□□□(KPI)□ □□□□□.
C. □□□□□ IT □□ □□□ □□□□□.
D. □□ □3□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best recommendation to improve IT governance within the organization is C. Require executive management to draft IT strategy. IT governance is the process of establishing and maintaining the policies, roles, responsibilities, and accountabilities for managing technology risks within an organization1. One of the key objectives of IT governance is to ensure alignment and integration between technology and business strategies, leading to optimal outcomes and value creation1. Therefore, it is essential that executive management, who are responsible for setting the vision, mission, and goals of the organization, are also involved in drafting the IT strategy that supports and enables them.
By requiring executive management to draft IT strategy, the organization can:
Ensure that the IT strategy is consistent and coherent with the business strategy, and reflects the organization' s priorities, values, and culture2.

Enhance communication and collaboration between IT and business functions, and foster a shared understanding and commitment to the IT strategy2.
Increase accountability and transparency for IT performance and outcomes, and ensure that IT investments are aligned with the organization's risk appetite and value proposition2.

NEW QUESTION: 567
□□□ □□ □□ □□ □□□□□ □□□□ □□□□ □□□ □, □□ □□□ □□□□ □ □□□ □ □□ □□□ □□□ □□ □ □□□□□?
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 exercisemay 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: 568
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: 569
□□ □ □□□□ □□□ □□ □□□ □□□ □ □□ □□□□ □□□ □□ □ □□□□ □ □ □□□□□?
A. □□□ □□□ □□□ □□□ □□□ □□□□ □□□□□ □□□ □□□□□.
B. □□□ □□□ □□□ □□□ □□□ □ □□ □□□ □□□□□.
C. □□ □□ □ □□ □□□ □□ □□□ □□□□□.
D. □□□ □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The role of a document owner when implementing a data classification policy in an organization is to classify documents to correctly reflect the level of sensitivity of information they contain. A document owner is the person who is ultimately responsible for the creation, maintenance, and protection of a document, usually a member of senior management or a business unit1. A data classification policy is a plan that defines how the organization categorizesits data based on its value, risk, and regulatory requirements, and how it handles and secures each data category2.

According to the data classification policy template by Netwrix3, one of the roles and responsibilities of the document owner is to assign data classification labels based on the data's potential impact level. Data classification labels are tags or markings that indicate the sensitivity level of the data, such as public, internal, confidential, or restricted. The document owner should apply the data classification labels to the documents that contain the data, either manually or automatically, using tools and methods such as metadata, watermarks, headers, footers, or encryption. The document owner should also review and update the data classification labels periodically or whenever there is a change in the data's sensitivity level.
By classifying documents to correctly reflect the level of sensitivity of information they contain, the document owner can help to ensure that the documents are handled in accordance with the data classification policy.
This means that the documents are stored, accessed, shared, transmitted, and disposed of in a secure and appropriate manner, based on the rules and controls defined for each data category. This can also help to prevent data loss, leakage, or breach incidents that may cause harm or damage to the organization or its stakeholders.
Therefore, option A is the correct answer.
References:
Data Classification Policy: Definition, Examples, and Free Template2
Data Classification Policy Template - Netwrix3
Data Classification and Handling Policy - University of Hull1

NEW QUESTION: 570
□□□ □□ □□ □□□ □□□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□
B. □□ □□□
C. □□□ □□□
D. □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 571
□□ □ □□ □□ □□ □□ □□□ □□ □□□ □□□□?
A. □□□□ □3□□□□ □□□ □□□ □□□□ □
B. □□ □□□□ □□□ □□□ □□ □□ □□
C. □□ □□□□□□ □□ □□ □□□ □□
D. □□ □□□□ □□□□□ □□ □□□ □□
Answer: D (LEAVE A REPLY)
The most reliable evidence is evidence obtained directly by the auditor through independent performance of procedures. ISACA guidance notes that higher-assurance

audit work is achieved when evidence is produced directly by auditors, or at least strictly under their control, rather than being supplied by the entity being audited.
Option D is correct because independently performing manual procedures gives the auditor direct control over the evidence-gathering process and reduces reliance on the auditee or control owner. In audit theory and in ISACA-aligned practice, evidence obtained directly by the auditor is generally more reliable than evidence merely provided by the auditee.
Option A is strong evidence because it comes from an independent third party, but it is still inspected rather than generated directly by the auditor. It is generally very reliable, but not as strong as auditor-generated evidence through independent reperformance.
Option B is less reliable because system-generated evidence provided by a control owner still depends on the completeness and integrity of what was selected and presented by the auditee.
Option C is the least reliable among the plausible choices because critical data received from an auditee is subject to the greatest dependence on management representation and auditee-controlled extraction.
Therefore, D is the best answer because evidence generated through procedures performed independently by the auditor is the most reliable.
References (Official ISACA):
* ISACA Journal, Capability Maturity Model and Risk Register Integration - "evidence is produced directly by the auditors or, if strictly under the auditors' control, by the entity's staff."
* ISACA Journal, A Factory Model Approach to Technology Control Testing - emphasizes gathering evidence, analyzing it, and substantiating results within a governed testing process.
* ISACA, ITAF update announcement - confirms ITAF as ISACA's professional framework for audit standards and guidance.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 572
□ □□□□ □□□□□ □□ □□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□ □□□□ □□□□□□. □□ □ □□ □□□ □□ □□ □□□ □□□ □□ □ □□□□□?
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: 573
□□□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□ □ □□□□ □□ □□□□ □□□ □□ □ □□□□□?
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: 574
□□□□□ □□□□□□(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: 575
□□□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□□ □□□ □□□□□ □□□□ □□ □□□ □□.
B. □□ □□□ □□□ □□ □□□□ □□□□ □□.
C. □□□□ □□□ □□ □□ □□.
D. □□ □□ □□□ □□ □□□ □□ □□.
Answer: (SHOW ANSWER)
A privacy protection policy is primarily intended to make personnel aware of the organization's responsibilities and rules for handling personal information in accordance with applicable laws, regulations, and contractual obligations. ISACA privacy guidance consistently frames privacy as a compliance-driven and accountability-driven discipline, centered on the proper collection, use, storage, sharing, and protection of personal data under applicable legal requirements.
Option C is therefore the best answer because a privacy policy's core purpose is not just technical protection, but ensuring that employees understand the legal and regulatory requirements governing personal information. ISACA notes that modern privacy programs are strongly shaped by regulations such as GDPR and similar laws, which impose explicit obligations on organizations that collect and process personal data. A privacy protection policy helps communicate those obligations internally.
Option A is incorrect because cybercrime awareness belongs more to a general information security awareness program than to the primary purpose of a privacy protection policy. Privacy and cybersecurity overlap, but privacy policy is specifically about lawful and proper handling of personal information, not general awareness of network-targeting crimes.
Option B is incorrect because encryption is only one possible control for protecting personal data. A privacy policy may mention encryption, but its primary purpose is broader: defining privacy obligations, rights, responsibilities, and compliance expectations. Technical controls support the policy; they are not the policy's central awareness objective.
Option D is also incorrect because system configuration procedures belong to technical standards, baselines, or operating procedures. A privacy protection policy is a governance-level document that sets expectations regarding personal information protection and legal compliance, rather than detailing system configuration steps.

For CISA-style reasoning, when a question asks for the primary objective of a privacy policy, the best answer is the one that addresses the organization's obligation to protect personal data in accordance with legal requirements. That makes C the strongest and most defensible answer.
References (Official ISACA):
* ISACA Privacy Resource Center - privacy guidance focused on compliance and privacy program obligations.
* ISACA, The Evolving World of Data Privacy: Trends and Strategies - discusses legal obligations such as GDPR requirements for personal data protection.
* ISACA Privacy Notice - reflects the role of applicable law in handling personal data.
* ISACA Journal, Creating a Compliant and Accountable Data Culture - emphasizes accountability and compliance in data privacy.

NEW QUESTION: 576
□□ □ □□□□ □□□□ □□ □□□ □□ □□(SLA)□ □□□ □ □□□ □□ □□□□ □?
A. □□□□ □□□□ □□ □ □□□ □□□□□ □□.
B. □□□□ □□□ □ □□ □□ □□ □□
C. □□□□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
D. □□□□ □□□ □□ □□
Answer: B (LEAVE A REPLY)
One of the challenges in developing a SLA for network services is finding performance metrics that can be measured properly and reflect the quality of service expected by the customer. Establishing a well-designed framework for network services is not a challenge, but a good practice. Ensuring that network components are not modified by the client or reducing the number of entry points into the network are security issues, not SLA issues.
References: ISACA, CISA Review Manual, 27th Edition, 2018, page 333

NEW QUESTION: 577
□□□ □□□ □□□ □□□ □□□□.
A. □□□□ □□ □□ □□□□.
B. □□□□ □□□□□.
C. □□□□ □□□ □ □□□ □□□ □□□□□.
D. □□ □□□ □□ □□□□□ □□□ □□□□.
Answer: B (LEAVE A REPLY)
A digital signature is a specific type of e-signature that is backed by a digital certificate. A digital certificate is a document that contains the public key of a signer and is issued by a trusted third party called a certificate authority (CA). A digital signature provides proof of the identity of the signer and the integrity of the signed document.
A characteristic of a digital signature is that it is unique to the message. This means that a digital signature cannot be copied from one document to another without being detected as

invalid. A digital signature is created by applying a mathematical function called a hashing algorithm to the document. A hashing algorithm produces a fixed-length output called a hash or digest from any input data. The hash is unique to the input data; any change in the input data will result in a different hash.
The signer then encrypts the hash with their private key (a secret key that only they know) to create the digital signature. The encrypted hash is attached to the document as the digital signature. The recipient of the document can verify the digital signature by decrypting it with the signer's public key (a key that is publicly available and matches the private key) to obtain the hash. The recipient then applies the same hashing algorithm to the document to generate another hash. The recipient then compares the two hashes; if they match, it means that the document has not been altered and that the signer is authentic.
Therefore, a digital signature is unique to the message because it is derived from the hash of the message, which is unique to the message.
References:
7: Free Online Signature Generator (Type or Draw) | Signaturely
8: What are digital signatures and certificates? | Acrobat Sign - Adobe
9: eSign PDF with Electronic Signature Free Online - Smallpdf

NEW QUESTION: 578
□ □□ □□□ □□□ □□ □□ □□□□□ □□□□ □□□□ □□ □□□ □□□□ □ □ □□□□ □□□ □□ □ □□□□□?
A. □□□□ □□□ □□(BCP)□ □□ 6□□ □□ □□□□□ □□□□□.
B. □ □□ □□ □□□ □□□□□□ □ □□□□.
C. □□□□ □□ □□□□□□□ □ □□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 579
□□ □□ □□ □ □□ □□□ □□□□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□ □□□□ □□□ □□□□ □□
B. □□□ □□□ □□□ □□□ □□□□□ □□ □□□ □□□□ □□
C. □□ □□ □□ □ □□ □□□ □□□ □□□ □ □□□ □□□□□.
D. □□ □□ □□□ □□□□□ □□□ □□□ □□ □ □□□ □□ □□
Answer: (SHOW ANSWER)
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with

relatively high probability of material problems that may affect the achievement of audit goals or business objectives.
Addressing the overall risk associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems. References:
CISA Review Manual, 27th Edition, page 1111
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 580
□□ □ □□□□□□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□?
A. □□ □□□ □□□□ □□□ □□ □□ □□ □□ □□
B. □□□ □□ □□□ □□□□ □□□ □□
C. □□ □□ □□□□ □□□ □ □□□
D. □□□ □□ □□ □□□ □□ IT □□□ □□
Answer: B (LEAVE A REPLY)
The most important prerequisite for the protection of physical information assets in a data center is a complete and accurate list of information assets that have been deployed. Information assets are any data, devices, systems, or software that have value for the organization and need to be protected from unauthorized access, use, disclosure, modification, or destruction4. A data center is a facility that houses various information assets such as servers, storage devices, network equipment, etc., that support the organization's IT operations and services5. A complete and accurate list of information assets that have been deployed in a data center can help to identify and classify the assets based on their importance, sensitivity, or criticality for the organization.
This can help to determine the appropriate level of protection and security measures that need to be applied to each asset. A complete and accurate list of information assets can also help to track and monitor the location, status, ownership, usage, configuration, maintenance, etc., of each asset. This can help to prevent or detect any unauthorized or inappropriate changes or movements of assets that may compromise their security or integrity. Segregation of duties between staff ordering and staff receiving information assets, availability and testing of onsite backup generators, and knowledge of the IT staff regarding data protection requirements are also important prerequisites for the protection of physical information assets in a data center, but not as important as a complete and accurate list of information assets that have been deployed. These factors are more related to the implementation and maintenance of security controls and procedures that depend on having a complete and accurate list of information assets as a starting point.
References: ISACA CISA Review Manual 27th Edition, page 308

NEW QUESTION: 581

□□ □ □□ □□ □ □□ □□□ □□□ □□ □□ □□□□□ □□ □ □□□ □□□□?
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: 582
□ □□□ □□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□□□. □□□□ □□ □ □□ □□ □□□□ □□ □□□□□ □□□ □ □□ □□□ □□□□□?
A. □□□□ □□□□ □□ □□ □□ □□
B. □□ □□ □□□ □□ □□ □□□ □□
C. □□□ □□□□ □□□□□ □□□ □□□□ □
D. □□ □□ □□ □ □□ □□□ □□ □□
Answer: (SHOW ANSWER)
The most effective way for the audit team to leverage the risk management maturity of the organization is to integrate the risk register for audit planning purposes. The risk register is

a document that records the identified risks, their likelihood, impact, and mitigation strategies for a project or an organization. By using the risk register, the audit team can align their audit objectives, scope, and procedures with the organization's risk profile and priorities. This will help the audit team to provide more value-added and relevant assurance and recommendations to the management and stakeholders.
Some of the web sources that support this answer are:
Audit Maturity And Risk Management | Ideagen
Building a Mature Enterprise Risk Management Plan | AuditBoard
CISA CertifiedInformation Systems Auditor - Question0551

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

NEW QUESTION: 584
□□□ □□□ □□ □□□□ □□ □□□□□□□□ □□□ □□□□ □□ IT □□□□ □ □ □□□ USB □□□ □□□□□□. □□ □ □□□ □□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□
B. □□
C. □□□
D. □□□
Answer: C (LEAVE A REPLY)
Disabling USB access for storage devices is a preventive control because it is intended to stop malware introduction before it occurs. ISACA explicitly describes disabling USB access for storage devices as a preventive control that makes it harder for users to introduce threats such as viruses into the environment.
Option C is correct because the control works in advance of the event. It prevents users from connecting removable storage that could carry malicious software or facilitate unauthorized data transfer.
Option A is incorrect because corrective controls act after an incident to restore or remediate conditions. USB blocking does not restore anything after infection.
Option B is not the best answer because although administrative policy may require the control, the specific control being described functionally prevents an unwanted event. In CISA questions, the functional type is the better classification here.

Option D is incorrect because the control is not physical; it is a logical/technical measure enforced through system configuration.
Therefore, C is the best answer because disabling USB storage access is designed to prevent malware from being introduced through physical media.
References (Official ISACA):
* ISACA, Specific Controls You Can Use - disabling USB access for storage devices is described as a preventive control.
* ISACA Journal, Addressing Cybersecurity Vulnerabilities - preventive controls are used to reduce exposure before compromise.

NEW QUESTION: 585
□□ □ □□ □□□ □□□□ □□□ □□□ □ □□□ □□□ □□ □□□ □□□ □ □□ □□ □□□□ □ □□□ □□□□□?
A. □ □□□ □□□□ □□ □ □□□(PKI) □□□ □□□□□.
B. □ □□□ □□□□ □□□ □□ □□□ □□□□□.
C. □ □□□ □□□ □□□ □□□□□ □□□□ □□□□□.
D. □ □□□ 128□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The greatest concern to an IS auditor reviewing an organization's method to transport sensitive data between offices is that the method relies exclusively on the use of asymmetric encryption algorithms. Asymmetric encryption algorithms, also known as public key encryption, use two different keys for encryption and decryption: a public key that is shared with anyone who wants to communicate with the sender, and a private key that is kept secret by the sender. Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, which use the same key for both encryption and decryption, but they are also slower and more computationally intensive. Therefore, relying exclusively on asymmetric encryption algorithms may not be efficient or practical for transporting large amounts of sensitive data between offices. A better method would be to use a combination of symmetric and asymmetric encryption algorithms, such as using asymmetric encryption to exchange a symmetric key and then using symmetric encryption to encrypt and decrypt the data.
The other options are not as concerning as option C. The method relying exclusively on the use of public key infrastructure (PKI) is not a concern, because PKI is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates that are based on asymmetric encryption algorithms. PKI enables secure and authenticated communication between parties who do not have a prior trust relationship. The method relying exclusively on the use of digital signatures is not a concern, because digital signatures are a way of verifying the authenticity and integrity of a message or document by using asymmetric encryption algorithms. Digital signatures ensure that the sender cannot deny sending the message or document, and that the receiver can detect any tampering or alteration of the message or document. The method

relying exclusively on the use of 128-bit encryption is not a concern, because 128-bit encryption is a level of encryption that uses a 128-bit key to encrypt and decrypt data. 128-bit encryption is considered to be strong enough to resist brute-force attacks by modern computers. References: Asymmetric vs Symmetric Encryption: What are differences?, Public Key Infrastructure (PKI), Digital Signature, What is
128-bit Encryption?

NEW QUESTION: 586
□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □ □□□ □ □□□ □□ □ □□□□□?
A. □□□□ □□ □□□□□□ □□□ □□□□□□□□□ □□□□ □□□ □□ □□□ □□.
B. □□ □□ □□□ □□ □□ □□□□□ □□□□□.
C. □□□ □□ □□□□ □□□□ □□□□□□□.
D. □□□□ □□□ □□ □□ □ □□□ □□ □□□ □□ □□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack is that backups were only performed within the local network. This means that the backups could have been encrypted or deleted by the ransomware, making it impossible to restore the data and systems without paying the ransom or losing the data. Backups are a critical part of the recovery process from a ransomware attack, and they should be performed frequently, securely, and off-site or in the cloud to ensure their availability and integrity.
The other options are not as concerning as option C, although they may also indicate some security weaknesses. Antivirus software was unable to prevent the attack even though it was properly updated, but this is not surprising given that ransomware variants are constantly evolving and antivirus software may not be able to detect them all. The most recent security patches were not tested prior to implementation, but this is a trade-off between security and availability that may be justified depending on the severity and urgency of the patches. Employees were not trained on cybersecurity policies and procedures, but this is a preventive measure that may not have prevented the attack if it was initiated by other means such as phishing or exploiting vulnerabilities.
References:
10: Infrastructure-as-a-Service Security Responsibilities - CloudTweaks
5: 3 steps to prevent and recover from ransomware | Microsoft Security Blog
7: How to Recover From a Ransomware Attack - eSecurityPlanet

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□

□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 587
□□ □ □□ □□ □□ □□ □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □ □□□ □□ □□□
B. □□ □□ □□ □ □□ □□□□ □□
C. □□ □□□□ □□ □□
D. □□ □□□ □□ □□□ □□
Answer: A (LEAVE A REPLY)
The primary concern when negotiating a contract for a hot site is the availability of the site in the event of multiple disaster declarations. A hot site is a fully equipped alternative facility that can be used to resume business operations in the event of a disaster. However, if multiple clients of the hot site provider declare a disaster at the same time, there may be a shortage of resources or capacity to accommodate all of them. Therefore, the contract should specify the terms and conditions for ensuring the availability and priority of the hot site for the organization. The other options are not as important as availability, as they do not affect the ability to use the hot site in a disaster situation. Coordination with the site staff in the event of multiple disaster declarations is a logistical issue that can be resolved by communication and planning. Reciprocal agreements with other organizations are alternative arrangements that can be used to share resources or facilities in a disaster, but they may not be as reliable or suitable as a hot site. Complete testing of the recovery plan is a good practice that can help validate and improve the effectiveness of the recovery plan, but it is not a concern for negotiating a contract for a hot site. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3

NEW QUESTION: 588
□□□ □□□ □□□□ □□ □□□ BYOD(Bring Your Own Device) □□□ □□□□ □ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□ BYOD □□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□ □□.
B. BYOD □□□ □□□ □□□ □□□□□.
C. □□ □□ □□□ BYOD □□ □□□ □□ □□□ □□ □□□ □□□□□□.
D. □□□ BYOD □□□ □□□□□ □□□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)
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 throughBYOD 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: 589
□□ □ □□□ IT□ □□ □□□□□?
A. IT □□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□
B. □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□
C. IT □□□ □□ □□ □□ □□□□ □□□□ □□□ □□□□ □□
D. □□□□ □□□ □□□□ □□□□ □□ □□ □□ □□ □□□□ □□□□ □□
Answer: (SHOW ANSWER)
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: 590
□□□□□ □□ □□ □□□□□□□ □□□ □ IS □□□□ □□ □□ □□□□ □□ □ □□ □□ □ □□□□□?
A. □□□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□□.

B. □□□□ □□□ □□□ □□□□□□.
C. □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□□.
D. □□ □□ □□□□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The correct answer is B. Review the terms and provisions in the contract.
When auditing an outsourced application, the auditor should first understand the contractual responsibilities, service scope, control expectations, reporting requirements, audit rights, compliance obligations, and security commitments. ISACA guidance on outsourcing and third-party assurance emphasizes that contracts are foundational because they define what the service provider is obligated to do and what the customer is entitled to review.
Option A is not first because billing validation is secondary to understanding the service arrangement and obligations.
Option C is incorrect because implementing access rights is a management responsibility, not an audit procedure.
Option D is important, but the auditor must first know whether such reporting is required, how it is defined, and under what timelines, all of which are typically governed by the contract or related agreement.
Therefore, the correct answer is B, because contract review establishes the basis for all further audit work over the outsourced HR application.
References (Official ISACA):
* ISACA Journal, Third Party Assurance - highlights the importance of understanding outsourced service arrangements and related assurance expectations.
* ISACA Now Blog, The Challenging Task of Auditing Social Media - states that when a function is outsourced, the contract should be reviewed to ensure it specifies required activities and expectations.

NEW QUESTION: 591
□□□□ □□ □□□□ □□□ □ □□ □□□□ □ □□ □□ □□□□ □□□?
A. □□□ □□□□□ □□□□(UDP)
B. □□□□□□ □□ □□□□(HTTP)
C. □□ □□ □□ □□□□(SFTP)
D. □□ □□□□ □□□□(RDP)
Answer: C (LEAVE A REPLY)
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: 592
□□ □ □□□ □□□ □□□ □□ □ □□□ □□□□ □□ □□□ □□□□□?
A. □□□□□ □□□□□ □ □□□ □□□□.
B. □□□□ □□□□ □□□ □ □□□□.
C. □□□□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□ 1□ □□ □□□□□□ □□□□□.
Answer: A (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: 593
□ □□□ □□ □□ □□ □□□□□□ □□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□.
□□ □□ □□, □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□□. □ □□□ □□□ □□ □□ □□□□ □□□ □□□□□□. □□□□□□ □□ □□□□ □□ □□□□□ □□ □□ □□□ □□□□□□. □□□□ □□ □□□ □□□□ □□ □□ □ □□□ □□ □□□ □□□ □□□□□ □□□□□ □□□□ □□□?
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 and Explanations Database, Question ID: 262

NEW QUESTION: 594

□□ □ □□ □□□ □□□□ □□ □□ □□□(IDS)□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?

A. □□ □□ □□

B. □□ □□□□ □□

C. □□ □□□□

D. □□ □□□□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 595

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

A. SQL □□□

B. □□

C. □□□ □□

D. □□□□ □□□□ □□

Answer: B (LEAVE A REPLY)

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: 596
□□ □ IT □□□□□□ □□□ □□ □□(SLAS)□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□□□□
B. IT □□ □□ □□□ □□□□□.
C. □□□□□ □□ □□ □□
D. IT □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The best way to identify whether the IT help desk is meeting service level agreements (SLAs) is A. Review exception reports. Exception reports are documents that highlight any deviations from the agreed service levels, such as breaches, delays, or failures. They can help the IT help desk to monitor their performance, identify root causes, and implement corrective actions. Reviewing exception reports can also help the IT help desk to communicate with the end users and stakeholders about any service issues and their resolution.
Reference: IT help desk support SLA, Section 4: Reporting and Reviewing Service Levels, Page 3.

NEW QUESTION: 597
□□ □ POS(□□ □□ □□) □□□□□ □□ □□ □□ □□ □□ □□□ □□□□ □□ □□ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□□
B. □□□
C. □□ □□
D. □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 598
□□ □ □□□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□ □ □□□□□?
A. CAAT□ □□ □□□ □ □□□□.
B. □□ □□□ □□
C. □□ □□□□ □□□ □□□□□.
D. □□□□ □□□ □□□□ □□ □□□ □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 599
□ □□□ □□□□ □□ □□ □□(CSA) □□□□□ □□□□ □□□, □□ □□ □□□ □□□□ □□ □□□ □□ □□□□□ □□□□. □□ □ □ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□ □ □□□□□.
B. □□□ □ □□ □□□□□.
C. □□□□□ □□□ □□ □□□ □□ □□□ □ □□□□.
D. □□ □□□□ □□ □□□ □□□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)
The most significant benefit of implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually is that risks are detected earlier. A CSA program is a process that enables business owners and managers to assess and improve their own internal controls on a regular basis, without relying on external auditors or consultants. A CSA program can help identify and mitigate risks, enhance performance, increase accountability, and foster a culture of control within the organization. By leveraging the internal audit function to test its internal controls annually, a small business unit can also obtain independent assurance and validation of its CSA results, as well as recommendations for improvement. This approach can help reduce compliance costs, as external audits may be less frequent or extensive. However, this is not the most significant benefit, as compliance costs are only one aspect of the total cost of risk. Business owners can also focus more on their core roles, as they can delegate some of their control responsibilities to their staff or teams through CSA. However, this is not the most significant benefit, as business owners still need to oversee and monitor their CSA activities and results, and ensure that they align with their strategic objectives and priorities. Line management may also be more motivated to avoid control exceptions, as they are directly involved in assessing and improving their own controls through CSA. However, this is not the most significant benefit, as motivation alone may not be sufficient to ensure effective control design and operation. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 600
□ □□□ □□ □□□ □□ □□ □□□ □□ □□□ SaaS(Software as a Service) □□□ □□□□□□. IS □□□□ □□□ □□□ □□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 601
IT □□ □ □□□□ □□ □□□□□ □□□ □□□ □□□□□ □□□□□□. □□ □ □ □□□ □□□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□ □□ □□□□ □ □ □□ □□ □□□□□?
A. □□□ □□□ □□ □□□□
□□ □□□ □□ □□□□□□ □□□ □□□□ .
B. □□□ □□ □ □□ □□□□ □□□ □□□□□ □□□□.
C. □□□ □□□ □□□ □□ □□ □□□□ □□□□□.
D. □□□ □□□□ □□□□ □□ □□□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
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.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 602
□□ □ □□□□□(IoT) □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □ □□ □ □□ □□ □□ □□ □□□ □□□□□?
A. IoT □□□ □□ □□□ □□ □□□ □□□□□□ □□□.
B. IoT □□□ □□ □ □□□ □□□□□.
C. IoT □□□ □□□ □□□□□□□ □□ □□□□ □□□.
D. IoT □□□ □□ □□□ □□ □□□ □□□□ □□□ □□□ □□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 603
□□ □□□ □□ □□□ □□□ □□□□.
A. □□□ □□ □□□ □□□□ □ □□□ □□□.
B. □□□□ □□ □ □□□□□ □□□□□.
C. □ □□□ □□ □□ □□□ □□□□□.

D. □□, □□ □ IS □□□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

An integrated audit merges financial, operational, compliance, and IT audits into a single coordinated review.

The key benefit is leveraging a multidisciplinary team with combined skill sets, resulting in a more holistic evaluation of risks and controls.

* Option A: Business reviews are important but not the primary benefit.

* Option B: Continuous auditing is a separate methodology.

* Option C: Better review by team leaders may occur, but that's not unique to integrated audits.

* Option D: Correct - the main advantage is combining diverse audit expertise.

ISACA Reference: CISA Review Manual 27th Edition, Domain 1, section on integrated audits and multidisciplinary audit approaches.

NEW QUESTION: 604

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

A. □□ □□□

B. □□□ □□

C. □□ □□

D. □□□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 605

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

A. □□□ □□□ □□

B. □□ □□ □□ □□ □□.

C. □□□□ □□ □□

D. □□□ □□□ □□ □□

Answer: D (LEAVE A REPLY)

The most concerning issue when determining if information assets are adequately safeguarded during transport and disposal is lack of appropriate data classification. Data classification is a process that assigns categories or levels of sensitivity to different types of information assets based on their value, criticality, or risk to the organization. Data classification can help safeguard information assets during transport and disposal by providing criteria and guidelines for identifying, labeling, handling, and protecting information assets according to their sensitivity. Lack of appropriate data classification can compromise the security and confidentiality of information assets during transport and

disposal by exposing them to unauthorized access, disclosure, theft, damage, or destruction. The other options are not as concerning as lack of appropriate data classification in safeguarding information assets during transport and disposal, as they do not affect the identification, labeling, handling, or protection of information assets according to their sensitivity. Lack of appropriate labeling is a possible factor that may increase the risk of misplacing, losing, or mishandling information assets during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. Lack of recent awareness training is a possible factor that may affect the knowledge or behavior of staff involved in transporting or disposing of information assets, but it does not affect the classification of information assets according to their sensitivity. Lack of password protection is a possible factor that may affect the security or confidentiality of information assets stored on devices during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION: 606
□□ □□□ □□□□ □□□□ IS □□□□ □□ □□□□□□ □□ □□ □□□□ □□□ □□□ □□□ □□□□□□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□. □ □□ □□□□ □□□ □□□ □□ □□□?
A. □□ □□□□ □□ □□□ □□□□□□ □□□ □□□□ □□ □□□□□□□ □□□ □□.
B. □□□□ □□□ □□□□ □□ □□□ □□□□□□ □□□□□.
C. □□ □□□□ □□ □□□□ □ □□□ □□□ □□□□□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□□□□ □□□□□.
Answer: (SHOW ANSWER)
When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence1. References:
1(https://www.isaca.org/resources/isaca-journal/issues
/2016/volume-6/enhancing-the-audit-follow-up-process-using-cobit-5)

NEW QUESTION: 607
□ □□□□ □□ □□□□□ □□□□ □□ □□□□□ □□ □□□□□□□ □□□□□ □□□. □□□□ □□□□ □□□ □□ □□□(DNS) □□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □ □□ □□□ □□□□ □□□?
A. □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□ ONS □□□ □□□□□.

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

NEW QUESTION: 608
□□ □ □□□ □□ □□ □□ □□□ □□□□□ □□□ □□□□□?
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: 609
□□ □ IT □□□□□ □□ □□ □□□ □□□ □□ □□□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□□□□?
A. IT □□□ □□ □□ □□□ □□ □□□ □□ □ □□□ □□ □□□ □□□ □□□□.
B. □□□□ □□□□ □□ □□ □□□ □□□ □ □□ □□□□ □□□ □□□ □□□ □ □□□□□.
C. □□ □□□ □□□ □ □□□ □□ □□, □□ □□ □ □□□ □□□□□.
D. □□ □□□□ □□ □□ □□□□□□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 610
IS □□ □□(OA) □□□ □□□ □□□□□.
A. □□□□ □□ □□□ □□□ □□□ □□□□□ □□□□□.
B. □□□□ □□□□□ □□□□ □□ □□□□ □□ □□ □□.
C. □□□ □□□□ □□□ □□□ □□□□ □□□□□.
D. □□□ □□ □□ □□□ □□□□□□□.

Answer: A (LEAVE A REPLY)
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: 611
□□ □ □□□□□□ □□ □□□ □□ □□ □□ □□□□□ □□□ □□ □□□ □□□ □□?
A. □□□ □□□□ □□□□□ □□
B. □□□ □□ □□□ □□□□ □□
C. □□ □□ □□□□□□ □□□□□ □□
D. □□□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
Following a configuration management process to maintain applications is the primary reason for ensuring proper change control. Configuration management is a process of identifying, documenting, controlling, and verifying the configuration items and their interrelationships within an IT system or environment. Following a configuration management process can help to ensure that any changes to the applications are authorized, tested, documented, and tracked throughout their lifecycle. This will help to prevent unauthorized or improper changes that could affect the functionality, performance, or security of the applications. The other options are not the primary reasons for following a configuration management process, but rather possible benefits or outcomes of doing so.
References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
CISA Review Questions, Answers and Explanations Database, Question ID 225

NEW QUESTION: 612
□□ □ □□□□ □□□□ □□□□□□ □□□ □ □□ □□□□ □□□ □ □□ □□□ □□□□□?
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 andselect 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 oftheir 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 differentdurations, 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 theinitial investment required for eachproject, which may not be indicative of their profitability or viability5. References: Portfolio, Program and Project Management Using COBIT 5 - ISACA, Project PortfolioManagement - ISACA, CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

NEW QUESTION: 613
□□ □□□(IS) □□ □□□□ □□□□ □□□ □□□□□ □□ □□ □□□ □□ □□ □ □□ □□□□ □□□□. □□□ □□ □□□ □□ □□□□ □□□ □□ □□□□□□ □ □□ □□□ □□□ □□□ □□ □□□ □, □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□ □□
B. □□□ □□□
C. □□□ □□
D. □□
Answer: (SHOW ANSWER)

NEW QUESTION: 614
□□ □ □□ □□□□ □□□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □□
B. □□ □□ □□
C. □□□□ □□□ □□□□□.

D. □□□ □□□ □□ □ □□

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 615

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

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

B. □□ □□ □□□ □□□□□ □□□□ □□□ □□

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

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

Answer: A (LEAVE A REPLY)

The best answer is A. Using automated tools to collect logs and raise alerts based on use cases.

ISACA's log management guidance emphasizes building log management programs that use automated collection, correlation, and alerting driven by defined use cases. It specifically discusses configuring use cases and alerts so that relevant events generate actionable alerts. This creates value by improving detection, response speed, and operational visibility at scale.

Option B. Reporting results to senior management can be useful, but that is more about governance reporting than day-to-day monitoring and management.

Option C. Selecting logs only from critical systems may reduce volume, but by itself it does not provide the active monitoring and alerting needed to create operational value.

Option D. Encrypting logs before archiving protects confidentiality and integrity, but it does not best help monitor and manage logs in an operational sense.

Therefore, A is the correct answer because automated log collection and alerting based on defined use cases is the most effective way to turn operational logs into actionable organizational value.

References (Official ISACA):
* ISACA Journal, Log Management as an Enabler for Data Protection and Automated Threat Detection.
* ISACA Journal, A Framework for SIEM Implementation.
* ISACA, Securing Artificial Intelligence: Opportunities and Challenges.

NEW QUESTION: 616
□□ □□□ □□ □□□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□ □□□□ □□□ □□□ □□□□□. □□ □□□ □□□ □□□□ □□□ □?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
The best answer is D. Compliance audit.
The auditor is testing whether employee behavior complies with organizational rules or policy regarding the use of the organization's car. ISACA defines IT compliance as adherence to mandated requirements from laws, regulations, contractual obligations, and internal policies. Since the scenario is about checking whether employees are following the organization's rule on permitted use, the audit is primarily a compliance-oriented review.
Option A could be tempting because misuse of a company car might be abusive, but the question does not say the auditor is investigating intentional deception or a suspected fraud scheme. Option B is incorrect because this is not primarily about fair presentation of financial statements. Option C is not the best fit because the audit objective is not evaluation of business function performance, but adherence to policy.
Therefore, the correct answer is D, because the auditor is determining whether employees are complying with the organization's established usage rules.
References (Official ISACA):
* ISACA, IT Compliance - compliance includes adherence to internal policies.
* ISACA, An Integrated Approach to Security Audits - audits assess adherence to required controls and obligations.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 617
□□□ □□□□ □□□ □□□□ □□ □□□ IT □□□□ □□□ □ □□ IS □□□□ □ □ □□□ □□□□□?
A. □□□ □□ □□ □□(SDLC) □□ □□
B. □□□ IT □□ □ □□ □□
C. IT □□ □ □□ □□
D. □□ □ □□ □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 618
□□ □□ □□ □□ □□□ □□□□ □□ □□ □□ □□□(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 and Explanations Database

NEW QUESTION: 619
□□ □□ □□□□ □ □□□ IT □□□ □□ □□ □□ □□ □□ □□□□ □□□□□□ □. □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□□ □□□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□□ □□
D. □□ □□□□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
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: 620
□□□ □□□ □ □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□□.
A. □□ □□.
B. □□ □□.
C. □□ □□.
D. □□□ □□ □□ □□.
Answer: A (LEAVE A REPLY)
The best answer is A. Business risk.
ISACA guidance ties data classification directly to the organization's risk context. ISACA notes that data classification defines the threshold beyond which damage to the organization may occur, and recent ISACA guidance also states that data-centric controls should align directly to business risk. That means classification should first reflect how sensitive the information is from the standpoint of business impact, not simply standards, policy wording, or retention schedules.
Option B is useful as a reference, but industry standards are secondary to the organization's own risk exposure and business impact. Option C is also secondary because security policy should itself be based on business risk. Option D matters for lifecycle governance, but retention requirements do not drive the fundamental sensitivity classification of information.
References (Official ISACA):
* ISACA Journal, Security Adjustments to Strengthen the Bond Between Risk Registers and Information.
* ISACA, Detect, Prevent, Comply: The Three Pillars of Modern DLP Use Cases.
* ISACA, Navigating Risk When Transitioning to the Cloud.

NEW QUESTION: 621
□□ □ □□ □□□ □□□□□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□
C. □□ □□ □□(CSA)
D. □□□□ □□□
Answer: (SHOW ANSWER)
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management

processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References: ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION: 622
□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□ □□(ERP) □□ □ □□□ □□ □□□□□□ □□□□ □□□□. □ □□□ □□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□ □□□□ □□ □□
B. □□□□ □□ □□□ □□□ □ □□ □□
C. ERP □□ □□
D. □□ □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 623
□□ □□ □□□(IDS)□ □□□ □□□ □, □□ □□□ □□□□ □□□ □□ □□□ □□ □ □□□ □□□ □□□.
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: 624
□□ □ □□□□□ □□ □□□□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □ □ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□ □□ □□

B. □□ □□ □ □□ □□
C. □□ □□ □ □□ □□ □□
D. □□□ □□ □ □□ □□
Answer: B (LEAVE A REPLY)
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: 625
□□ □□□(IS) □□□□ □ □□□ □□ □□□ □□(BCP)□ □□ 18□□ □□ □□□□ □□ □□□, □□ □□ □□□ □□□□□ □□□ □□ □□□□□. □□ □ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□ □□(BIA)□ □□□ □□ □ □□□ □□□□□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□ □□□ BCP□ □□□ □□□ □□□□□.
C. □□ □□ □□(RTO)□ □□□ □□□ □□□□ □□ □□□□ □□□□□.
D. □□ □□□ □□ □□□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The IS auditor should first determine whether the business impact analysis (BIA) is current with the organization's structure and context. The BIA is a critical component of the BCP and should reflect the current state of the organization. If the BIA is not up-to-date, it may not accurately reflect the impact of a disruption to the organization's operations, including the closure of a production plant12.
References: ISACA's Information Systems Auditor Study Materials1

NEW QUESTION: 626
□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□ □ □□□ □□ □□□, □□ □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□□□□. □□ □ □□□ □□ □ □□ □□ □□□ □□ □□ □□□□□?
A. □□□ □□
B. □□ □□□ □□□(VLAN)
C. □□□
D. □□ □□
Answer: C (LEAVE A REPLY)
The best option to support the organization's objectives of protecting data confidentiality while transporting data is encryption. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can

access the original data. Encryption protects the confidentiality of data in transit by preventing unauthorized interception,modification, or disclosure of the data. Encryption can also help comply with data privacy and security regulations, such as the GDPR and HIPAA.
The other options are not as effective as encryption in protecting data confidentiality while transporting data.
Cryptographic hashes are mathematical functions that generate a fixed-length output from an input, but they do not encrypt the data. Hashes are used to verify the integrity and authenticity of data, but they do not prevent unauthorized access to the data. Virtual local area network (VLAN) is a logical grouping of network devices that share the same broadcast domain, but they do not encrypt the data. VLANs can improve network performance and security by isolating traffic, but they do not protect the data from being intercepted or modified by external attackers. Dedicated lines are physical connections that provide exclusive access to a network or service, but they do not encrypt the data. Dedicated lines can offer higher bandwidth and reliability, but they do not guarantee the confidentiality of the data from being compromised by physical tampering or eavesdropping.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2 Data Security and Confidentiality Guidelines - Centers for Disease Control and Prevention3 Information Security | Confidentiality - GeeksforGeeks4

NEW QUESTION: 627
□□ □ □□□ □□ □□ □□ □□□□□ □□□ □□□□ □ □□ □□□ □□ □□□□ □?
A. □□□ □□ □□ □□□ □□□ □□
B. □□ □□ □□ □□ □□
C. □□ □□ □□ □□ □□
D. □□ □□□ □ □□ □□ □□ □□
Answer: B (LEAVE A REPLY)
The effectiveness of an information security awareness program is best measured by assessing real-world behavior rather than subjective feedback or indirect metrics. Social engineering exercises simulate real-world attack scenarios, testing whether employees can identify and respond appropriately to security threats. This directly evaluates the program's impact on employee behavior and awareness.
* Measuring User Satisfaction (Option A): While useful for feedback, satisfaction does not measure the effectiveness of awareness in preventing security incidents.
* Reviewing Security Staff Performance Evaluations (Option C): This focuses on staff capabilities rather than the awareness program's effectiveness.

* Analyzing Help Desk Calls (Option D): This might provide insight into recurring issues but does not directly measure the program's success in changing user behavior.
Conducting social engineering exercises aligns with best practices for assessing organizational security awareness.
Reference: ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

NEW QUESTION: 628
□□ □□□(IS) □□□□ □□□ IT □□ □□□□ □□□ □□ □□□□□□□(PDCA) □□□□ □□□□, □□□□ □ □□□ □□□□ □□□□ □□□ □□□□□. □□□ □ □□□ □□□□ PDCA □□□□□ □□ □□ □ □□ □□□ □□ □□□ □□□ □□□?
A. □□
B. □□
C. □□
D. □□
Answer: B (LEAVE A REPLY)
In the PDCA cycle, the " Plan " phase is where targets and objectives are defined. Focusing on this phase allows the auditor to evaluate the accuracy and appropriateness of the defined targets before they are implemented and measured in subsequent phases.
References
ISACA CISA Review Manual 27th Edition, Page 315-316 (PDCA Cycle)

NEW QUESTION: 629
□□ □□□(IS) □□□□ □□□ □□□ □□ □□(DLP) □□□□ □□ □□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□□. □□□□ □□ □□□□ □□□ □□□ □□□.
A. □□□ □□ □□□□ □□ □□ □□□□ □□□□ □□ □ □□□□.
B. □□ □□□ □□□ □□ □□□□ □□ □□□□ □□ □ □□□□.
C. □□ □□□□ □□□ □□□□ □□ □ □□□□.
D. □□□□ □□ □□ □□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 630
□ □□□ □□□ □□□ □□ □□ □□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□□□□.
□□□ IT □□□□ □□ □□ □□ □□□□ □□□□. □□ □ □□ □□□ □□ □□□ □ □□□ IT □□ □ □□ □□ □□□ IS □□□□ □□ □□ □ □□□ □□ □ □□ □□□ □□□?
A. □ □□□□ □□ □□ □□ □□ □□□ □□ □□ □□
B. □ □□□ □□□□ □□□□□ □□□ □□ □□ □□ □□
C. □□ □□□ IT □□ □ □□□ □□ □□ □□

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

Answer: B (LEAVE A REPLY)

Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk- based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1.

By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope,and procedures accordingly. This can help to address the unique needs and expectations of eachentity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.

The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.

References:

ISACA, CISA Review Manual, 27th Edition, 2019

ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription Risk-Based Audit Planning: A Guide for Internal Audit1 Risk-Based Audit Approach: Definition and Example

NEW QUESTION: 631

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

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 and Workplace Physical Security Assessment Checklist
Physical Security: Planning, Measures and Examples

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 632
□□ □□□□□ □□□ □□ □□□□□ □□ □□ □ □□ □□□ □□□□□ □□□□□ □□. □□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□□ □□□□ □□□ □□□□□□. □□□□ □□ □□□□□□□ □□□ □□ □□ □□□□ □□□□□□ □□□□□. □□□□ □□□□ □□ □□□ □□□ □□ □?
A. □□□□ □□ □□□□ □□□ □□□□□.
B. □□□ □□□□□ □□ □ □□□□ □□□□ □□□ □□ □□□□□.
C. □□ □□□□ □□□□ □□ □□□□ □□□□ □□□ □□□□□□.
D. □□□ □□□□□ □□ □□□□ □□□ □□ □□□□□.
Answer: D (LEAVE A REPLY)
Regression testing is crucial to ensure that new changes do not negatively impact existing functionalities. The IS auditor should recommend that regression testing be conducted to confirm that the system operates correctly after changes are made.
References
ISACA CISA Review Manual 27th Edition, Page 256-257 (Testing Strategies)

NEW QUESTION: 633
□ □□□□ □□ □□□ □□ □□□ □□ □□□□□□ □□□□ □□□□□ □□□. □ □ □□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□□□ □□□.
A. □□□□ □□ □□□ □□ □□ □□□ □.
B. □□□ □□□□ □□.
C. □ □□□□ □□□□ □□□ □□.

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

NEW QUESTION: 634
□ □□□ □ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□□. □□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□□□□□□. □□ □□□ □□ □□ □□ □□□□ □□□ □□□□.
A. □□ □□□ □□□ □□ □□ □□□ □□□ □ □□□□.
B. □□ □ □□ □□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□□.
C. □□□ □□ □□ □ □□□ □□ □□□□□□□.
D. □□ □□□ □□ □□□ □□□□ □□□□□□□.
Answer: A (LEAVE A REPLY)
An IS auditor's primary concern would be whether the recovery site devices can handle the storage requirements. The storage requirements are determined by the amount and type of data that needs to be backed up and restored in case of a disaster at the primary data center. The recovery site devices should have enough capacity, performance, reliability, and compatibility to meet these requirements.
If the recovery site devices cannot handle the storage requirements, then there is a risk that some data may not be backed up properly or may not be available for recovery when needed. This couldresult in data loss, corruption, or inconsistency, which could affect the business continuity and integrity of the organization.
Therefore, an IS auditor should verify that:
The recovery site devices have sufficient storage space to accommodate all the data that needs to be backed up from the primary data center.
The recovery site devices have adequate bandwidth and speed to transfer and access data efficiently and effectively.
The recovery site devices have appropriate security features and controls to protect data from unauthorized access or modification.
The recovery site devices are compatible with the primary data center devices in terms of hardware, software, format, and protocol.
References:
10: What Is a Disaster Recovery Site? Hot, Cold and Warm Site
11: Disaster recovery site - What is the ideal distance to mitigate risks? - Advisera
12: Offsite Data Backup Storage vs Disaster Recovery (DR) - LINBIT

NEW QUESTION: 635
□□ □□□□ □□ □□□□ □□□ □□□ □□□ □□ □□□(DNS) □□□ □□□□□?
A. □□
B. □□
C. □□
D. □□

Answer: A (LEAVE A REPLY)
Penetration testing is a method of evaluating the security of a system or network by simulating an attack from a malicious source. Penetration testing typically consists of four phases: planning, discovery, attacks, and reporting. In the discovery phase, penetration testers gather information about the target system or network, such as host detection, domain name system (DNS) interrogation, port scanning, service identification, operating system fingerprinting, vulnerability scanning, etc. This information can help to identify potential entry points, weaknesses, or vulnerabilities that can be exploited in the subsequent attack phase. Host detection and DNS interrogation are techniques that can be used in the discovery phase to determine the active hosts and their IP addresses and hostnames on the target network. References: [ISACA CISA Review Manual 27th Edition], page 368.

NEW QUESTION: 636
□ □□ □□□ □□ □□□ □□□ □□□□□ □□□□□□. □□ □□□ □□ □□ □□ □ □□ □□□□ □□□ □ □ □□ □□ □□□(IS) □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
The type of IS audit that would provide the greatest level of assurance that the department's objectives have been met after implementing new technologies and processes is an integrated audit. An integrated audit is an audit that combines financial, operational, compliance, and IT auditing aspects to provide a holistic view of the organization's performance and risks. An integrated audit can evaluate whether the new technologies and processes are aligned with the organization's goals, strategies, policies, and controls, and whether they are delivering value, efficiency, effectiveness, and reliability. The other types of IS audits (A, C and D) would not provide the same level of assurance, as they would only focus on specific aspects of the organization's activities, such as performance, cyber security, or financial reporting, which may not capture the full impact of the new technologies and processes. References: CISA Certification | Certified Information Systems Auditor | ISACA, CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.2: Types of IS Audit Engagements

NEW QUESTION: 637
□□ □ □□□ □□□□□□ □□□□(EA) □□□□□ □□□□ □□ □□□(IS) □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□ □□□□ CIO□ □□□ □□□□.
B. IT □□□□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□.
C. EA □□□□□ IT □□□ □□ □□□□□ □□□□□.

D. □□ □□ □□ □□□ EA □□□□□□ □□□□□.

Answer: B (LEAVE A REPLY)

IT application owners having sole responsibility for architecture approval (B) is a major concern because it indicates a lack of oversight and segregation of duties. EA decisions should be reviewed by a cross-functional governance body to ensure alignment with security, compliance, and business objectives.

Other options:

The CIO chairing the review board (A) may indicate centralized leadership but is not inherently a risk.

EA governing non-IT projects (C) may indicate scope expansion but is not a security risk.

Security requirements being reviewed (D) is a best practice and not a concern.

Reference: ISACA CISA Review Manual, IT Governance and Management of IT

NEW QUESTION: 638

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

A. □□ □□ □□ □□

B. □□□□ □□ □□ □□

C. □□□□ □□ □□□□ □□

D. □□ □□

Answer: B (LEAVE A REPLY)

Scope creep is the uncontrolled expansion of a project's scope, which can result in delays, cost overruns, and quality issues. To mitigate the risk of scope creep, an IS auditor should look for projectchange management controls, which are processes and procedures for managing changes to the project's scope, schedule, budget, and quality. Project change management controls ensure that changes are properly requested, approved, documented, communicated, and implemented. Source code version control, existence of an architecture review board, and configuration management are also important for software development, but they do not directly address the risk of scope creep.

References: ISACA Frameworks: Blueprints for Success, Project Management Institute: A Guide to the Project Management Body of Knowledge

NEW QUESTION: 639

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

A. □□ □□ □□(RPO) □□□□

B. □□□□ □ □□□ □□□

C. □□ □□ □□

D. □□□ □□ □ □□ □□

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

For organizations with multiple regional offices, the primary audit focus should be on processes and system dependencies. Dependencies determine recovery sequencing, resource prioritization, and interconnectivity between systems across regions.
* RPO monitoring (A): Important but a subset of overall recovery planning.
* Training (C): Necessary but not the first priority when evaluating plan adequacy.
* Data backup/storage (D): Technical component but less comprehensive than analyzing dependencies.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on disaster recovery planning and interdependencies.

NEW QUESTION: 640
□□ □ □□ □□ □□(DRP) □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □?
A. □□□ □□□ □□□ □□□ □□□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□ □□□□□.
C. □□ □□□ □□□□ □□□□□.
D. □□□□□ □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated. Test objectives should be aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

NEW QUESTION: 641
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 and 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: 642
□□ □ □□□ □□□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□ □□ □□□□ □□□
B. □□ □□□□ □□□ □□ □
C. □□□ □□ □□□□ □□□□□ □□□□□.
D. □□ □□□□ □□□□□□
Answer: A (LEAVE A REPLY)
Imaging the affected system is the best way to protect evidence in a forensic investigation, because it creates a bit-by-bit copy of the original data that can be analyzed without altering or compromising the original source. Imaging preserves the integrity and authenticity of the evidence and allows for verification and validation of the results34. Powering down or rebooting the affected system can cause data loss or corruption, while protecting the hardware does not prevent unauthorized access or tampering with the software or data. References: 3: CISA Review Manual (Digital Version), Chapter 6, Section 6.4.1 4: CISA Online Review Course, Module 6, Lesson 4

NEW QUESTION: 643
IT □□ □□□ □□□ □, □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□ □□□.
A. IT □□ □□.
B. □□□ □□□□ □□ □□□.
C. □□ IT □□.
D. □□ □□ □□□ □□ □□□□□.
Answer: C (LEAVE A REPLY)
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 and Assessment - Governance3 4: Time To Conduct A Strategy Review? Here's How To Get Started1

NEW QUESTION: 644
□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□ □□□□ □□□□ □□□ □□□ □ □□ □□□□□ □□□□□ □□□□ □□□ □□□ □□ □□□□□. □□ □ □□□ □ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□□ □□ □□
D. □□ □□
Answer: (SHOW ANSWER)
Problem management is the best way to enable the organization to resolve the issue of repeated failures of critical data processing services, as it focuses on identifying and eliminating the root causes of incidents and preventing their recurrence. Problem management involves analyzing incidents, performing root cause analysis, finding solutions, implementing changes and documenting lessons learned. Incident management is not the best way to resolve the issue, as it focuses on restoring normal service operation as quickly as possible after an incident occurs, but does not address the underlying causes or prevent future incidents. Service level management is not the best way to resolve the issue, as it focuses on defining, monitoring and reporting on the service levels agreed upon between service providers and customers, but does not address the causes or solutions of incidents. Change management is not the best way to resolve the issue, as it focuses on ensuring that changes are implemented in a controlled and coordinated manner, but does not address the identification or elimination of incidents. References:
[Problem Management Definition]
[Incident Management Definition]
[Service Level Management Definition]
[Change Management Definition]
IT Service Management | ISACA

NEW QUESTION: 645
□□ □ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□ □□□□□?
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 signingin 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 theydo 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

NEW QUESTION: 646

□□□ □□□ □□ □□□ □□ □□(DIP) □□□□ □□□ □ □□ □ □□ □□ □□□□ □ □□□ □□□□□?

A. □□ □□□□ □□□ □□□ □□□□□ □□□□□.

B. □□□ □□□ □□□ □□ □□ □□□ □□□□□.

C. DLP pcJc.es □ □□□□ □□□□□.

D. □□□ □□ □ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

The first step when developing a data loss prevention (DLP) solution for a large organization is to conduct a data inventory and classification exercise. This step is essential to identify the types, locations, owners, and sensitivity levels of the data that need to be protected by the DLP solution. A data inventory and classification exercise helps to define the scope, objectives, and requirements of the DLP solution, as well as to prioritize the data protection efforts based on the business value and risk of the data. A data inventory and classification exercise also enables the organization to comply with relevant laws and regulations regarding data privacy and security.

The other options are not the first step when developing a DLP solution, but rather subsequent steps that depend on the outcome of the data inventory and classification exercise. Identifying approved data workflows across the enterprise is a step that helps to design and implement the DLP policies and controls that match the business processes and data flows. Conducting a threat analysis against sensitive data usage is a step that helps to assess and mitigate the risks associated with data leakage, theft, or misuse. Creating the DLP policies and templates is a step that helps to enforce the data protection rules and standards across the organization.

References:

ISACA CISA Review Manual 27th Edition (2019), page 247

Data Loss Prevention-Next Steps - ISACA1

What is data loss prevention (DLP)? | Microsoft Security

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 647
□□□ □□□□□ □□□□ □□□□□□ □□□ □□□□ □□ □□□(IS) □□□□ □□ □□□□ □□□□ □□ □□□□ □□□□□□. □□ □ IS □□□□ □□□ □ □□ □□ □ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□ □□□ □□ □□□□□ □□□□□□.
C. □□ □□ □□ □□□ □□□□□.
D. □□□ □□□□□ □□.
Answer: A (LEAVE A REPLY)
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: 648
□□□ IT □□ □□□□ □□ □□ □□□ □□□□□ □□□.
A. □□□
B. □□ □□
C. □□□□ □□ □□
D. □□□□ □□□□ □□□
Answer: A (LEAVE A REPLY)
An IT risk assessment is the process of identifying and assessing the threats facing an organization's information systems, networks, and data. An IT risk assessment helps an organization to understand its current risk profile, prioritize its risks, and implement appropriate controls to mitigate them. An IT risk assessment also helps an organization to comply with relevant laws and standards, such as ISO 27001 or CMMC.
One of the key steps in an IT risk assessment is the identification of vulnerabilities. Vulnerabilities are the weaknesses or gaps in an organization's information security that could be exploited by internal or external threats. Vulnerabilities can exist in various aspects of an organization's information security, such as:
Hardware: The physical devices and components that store or process information
Software: The applications and programs that run on hardware devices Network: The

communication channels and protocols that connect hardware devices Data: The information that is stored or transmitted by hardware devices or software applications People: The users or personnel who access or manage information systems or data Processes: The procedures or workflows that govern how information systems or data are used or maintained By identifying vulnerabilities in each of these aspects, an organization can assess its exposure to potential threats, such as hackers, malware, natural disasters, human errors, or sabotage. By identifying vulnerabilities, an organization can also determine its risk level for each threat scenario, based on the likelihood and impact of a successful attack. By identifying vulnerabilities, an organization can also identify the existing or required controls to prevent or reduce the impact of an attack.
Therefore, an IT risk assessment should include the identification of vulnerabilities as a crucial component.
References:
4: What Is an IT Risk Assessment? (Plus Benefits and Components) | Indeed.com
5: How to Perform a Successful IT Risk Assessment - Hyperproof
6: IT Risk Resources | ISACA

NEW QUESTION: 649
□□ □□□□ IS □□□□ □□ □□□ □□ □□□□□□.
□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□,
□□□□ □□ □□□□. □□ □ □□ □□ □□□ □□□□□?
□□□□ □□ □□□ □□□□□ □□ □□□□?
A. □□ □□□ □□□ □□□ □□□□□□.
B. □□ □□ □□□ □□□ □□□ □□□□□□.
C. □□ □□□ □□□ □□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties. The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

NEW QUESTION: 650
□□ □ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
'□ □□ □□ □□□□□ □□□□□?
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: 651
□□ □ □□□ □□□□□□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□ □ □□□□□ □□□ □□□□ □□□□□.
B. □□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□□ □□ □□□□.
C. □□□□ □□□ □□□ □□□□□□.
D. □□ □□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 652
□□□ □□□ □□□ □□ □□ □□□□ □ □□□□ □□□ □□□ □□□ □□□□□.
□□ □ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□ □□□□ □□ □ □ □□ □□□ □□□ □□□ □□□□□?
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: 653
□□□□ □□ □□ □□ □, □□□□ □□□□ □□ □□□□ □□□ □□ □□ □□□ □ □□□ □□ □□ □□□ □□□□□?
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: 654
□□□ □□□□ □□ □□□□ □□□□ □□ □□□□ □□ □ □□ □□□□ □□□□□ □?
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: 655
□□ □□□□□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□□.
A. □□□ □□ □□ □□□ □□□□.
B. □□□□ □□□□ □□□□□.
C. □□□ □□ □□□.
D. □□□ □□□ □□.
Answer: C (LEAVE A REPLY)

Job scheduling is a core operational control that ensures workloads are executed in an orderly and efficient manner, balancing demands across processing resources. Its primary benefit is optimization of system resources-CPU, memory, I/O, and network bandwidth-leading to improved throughput and consistent service levels. While scheduling may indirectly reduce downtime (A) or support scalability (B), its direct impact is ensuring resources are allocated efficiently. Decreasing complexity (D) is not the key purpose of scheduling. ISACA's DSS01 (Managed Operations) recognizes workload and job scheduling as crucial practices for sustaining reliable, high-performance IT services.
References (ISACA): COBIT 2019, DSS01 Managed Operations.

NEW QUESTION: 656
IS □□ □□□□ □□ □□□ □□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□.
IS □□ □□□□ □□□ □□□□□ □□ □□ □ □□ □□□ □□□□□ □□□□ □□ □?
A. □□□□□ □□□ □□□ □□ □□□ □□
B. □□ □□ □□ □□ □□□ □□□ □□ □□ □□□
C. □□□ □□□□ □□ □□ □□□ □□□ □□ □□
D. □□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□
Answer: D (LEAVE A REPLY)
The IS audit manager should specifically review the detailed evidence of the successes and weaknesses of all contingency testing to substantiate the conclusions of the audit of the corporate disaster recovery test. This is because the detailed evidence can provide the audit manager with a clear and objective picture of how well the disaster recovery plan was executed, what issues or gaps were encountered, and what recommendations or actions were taken to address them. The detailed evidence can also help the audit manager to verify the accuracy, completeness, and validity of the audit findings, as well as to evaluate the adequacy and effectiveness of the disaster recovery controls.
The other options are not as specific or relevant as the detailed evidence of all contingency testing. Overviews of interviews between data center personnel and the auditor may provide some useful information, but they are not sufficient to substantiate the conclusions without supporting evidence from the actual testing. Prior audit reports involving other corporate disaster recovery audits may provide some benchmarking or comparison data, but they are not directly related to the current audit scope and objectives. Summary memos reflecting audit opinions regarding noted weaknesses may provide some high-level insights, but they are not enough to substantiate the conclusions without detailed evidence to back them up.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2411
Disaster Recovery Audit Work Program2

NEW QUESTION: 657

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

A. □□□ □□□ □□□□□□□□.

B. □□□ □□□ □□□□□.

C. □□□ □□ □□□ □□□□ □□□□ □□□□.

D. □□□□ □□□□ □□□□□□□.

Answer: (SHOW ANSWER)

Data classification is the process of organizing and labeling data into categories based on file type, contents, and other metadata. Data classification helps organizations answer important questions about their data that inform how they mitigate risk and manage data governance policies. Data classification also enables appropriate protection measures, and efficient search, retrieval and use of each data category12.

While evaluating the data classification process of an organization, an IS auditor's primary focus should be on whether data is correctly classified. This means that the data is assigned to the appropriate classification level based on its sensitivity, importance, integrity, availability, compliance requirements, and business value. Correct data classification ensures that the data is protected according to its risk level, and that the organization can comply with relevant laws and regulations that apply to different types of data3.

The other three options are not the primary focus of an IS auditor while evaluating the data classification process, although they may be relevant or useful for certain aspects of data management. Data classifications are automated means that the organization uses software tools or algorithms to analyze and label data based on predefined rules or criteria. This can improve the efficiency and consistency of data classification, but it does not guarantee that the data is correctly classified. The IS auditor still needs to verify the accuracy and validity of the automated classifications, and check for any errors or anomalies.

A data dictionary is maintained means that the organization keeps a record of the definitions, formats, sources, and relationships of the data elements in its systems or databases. This can enhance the understanding and usability of the data, but it does not ensure that the data is correctly classified. The IS auditor still needs to examine the content and context of the data, and compare it with the classification criteria and policies.

Data retention requirements are clearly defined means that the organization specifies how long it will keep different types of data, and when it will delete or archive them. This can help reduce storage costs, improve performance, and comply with legal obligations, but it does not ensure that the data is correctly classified. The IS auditor still needs to assess whether the data is stored and protected according to its classification level, and whether the retention periods are appropriate for each type of data.

Therefore, data is correctly classified is the best answer.

References:

Data Classification: The Basics and a 6-Step Checklist - NetApp

What is Data Classification? Guidelines and Process -Varonis
Data Classification and Handling Procedures Guide

NEW QUESTION: 658
□□ □ □□□ □□□□□ □□ □□□□□ □□ □□ □□ □□ □□ □□ □□□ □□□ □□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□ □□□ □ □□ □□ □□ □□
B. □□□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □
C. □□ □□ □□□ □□□ □ □□ □□□□ □ □□□□ □□□□□.
D. □□□□ □□□□ □□□□□ □□ □□□□(SDLC) □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 659
□□□ □□□ □□□□□ □□□□ □□, □□□□□□ □□□ □□ □□□□ □□□□ □ □ □□□□ □□□ □□ □ □□□□□?
A. □□ □ □□□□
B. □□□ □□□
C. □□□
D. □□□ □□□□□ □□□□□
Answer: A (LEAVE A REPLY)
The correct answer is A. Overwriting multiple times. Overwriting is a method of securely erasing data from a hard disk by replacing the existing data with random or meaningless data, making it difficult or impossible to recover the original data1. Overwriting multiple times, also known as multiple-pass overwriting, is a more effective way of disposing of sensitive data than overwriting once, as it reduces the possibility of residual traces of data that could be recovered by advanced techniques2. Overwriting multiple times can be done by using specialized software tools that follow certain standards or algorithms, such as the US Department of Defense's DoD 5220.22-M or the Gutmann method3.

NEW QUESTION: 660
□ □□□ □3□ □□□ □□□□□□□ □□□□ □□□ □□□ □□ □□□ □□□□□ □ □□□ □□□□□. □□ □ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □?
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: 661

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

A. □□□ □□□ □□□ □□□□ □□□□ □□□□.

B. □□□ □□□□ □□ □□□ □□□□□.

C. □□□ □□□ □□□□ □□□□.

D. □□ □□□ □□ □□□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

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

Therefore, it is essential that logs are stored in a separate host that is isolated and secured from the network and the firewall itself, to prevent unauthorized access or modification of the logs. Automated alerts are being sent when a risk is detected is a good practice for enhancing the security and efficiency of a firewall, but it is not the most important thing for an IS auditor to verify, as alerts may not always be accurate, timely, or actionable. Insider attacks are being controlled is a desirable outcome for a firewall, but it is not the most important thing for an IS auditor to verify, as insider attacks may involve other factors or methods that bypass or compromise the firewall, such as social engineering, credential theft, or physical access. Access to configuration files is restricted is a critical control for ensuring the security and integrity of a firewall, but it is not the most important thing for an IS auditor to verify, as configuration files may not reflect the actual state or performance of the firewall.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 662
□□□ □□□ □□□□(XSS) □□□ □□□ □□ □□□□ □□□□ □□ □□ □□□□.
A. □□□□□□ □□□ □□ □□.
B. 3□□ □ □□□□.
C. □□□ □□ □□.
D. □□□□ □□ □□□□□ □□.
Answer: C (LEAVE A REPLY)
Secure coding practices are the best way to prevent cross-site scripting (XSS) attacks, because they can ensure that the web application validates and sanitizes user input and output data to prevent malicious scripts from being executed on the web browser. XSS attacks are a type of web application vulnerability that exploit the lack of input validation or output encoding in webpages that accept user input or display dynamic content.
Application firewall policy settings, a three-tier web architecture, and use of common industry frameworks are not effective controlsto prevent XSS attacks, because they do not address the root cause of the vulnerability in the web application code. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

NEW QUESTION: 663
□□ □ RSA □□□□ □□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □ □□□□ □□ □□ □□□□□?
A. □□□□□□ □□□□ □□ □□□ □□□ □□□□
B. □□ □□□ □□
C. □□□□ □□ □ □□
D. □□□□ □□ □ □□
Answer: D (LEAVE A REPLY)
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: 664
□□ □ IT □□□□□ □□□□ □□□ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□
B. □□ □□□□ □□
C. □□□□ □□ □□
D. □□□□ □□
Answer: (SHOW ANSWER)
The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture.
References: ISACA, CISA Review Manual,
27th Edition, 2018, page 41

NEW QUESTION: 665
IT □□□□ □□□□□□ □□□□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□ □.
A. IT □□ □□□ □□□□□.
B. □□ IT □□□ □□ □□□ □□□□□.
C. IT □□ □□□□ □□□□□.
D. IT □□□ □□□□□.
Answer: (SHOW ANSWER)
IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. The board of directors of an organization is ultimately accountable for IT governance and has the authority to approve the IT strategy.

The board of directors does not need to address technical IT issues, be informed of all IT initiatives, or have an IT strategy committee, as these tasks can be delegated to other stakeholders or committees within the organization.

NEW QUESTION: 666
□□□ □□□ □□□ □□ □□□□ □□□□□ □□ □□□ □□ □□ □□□ □□ □ □ □□□□?
A. □□ □□ □□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□□□.
B. □□□ □□ □□□□□ □□□□ □□□ □□□□ SFTP(□□ □□ □□ □□□□)□ □□□□ □□□□□.
C. □□□ □□□□ □ □□□ □□ □□□ □□ □□□ □□ □□□□□.
D. □□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best detective control for a job scheduling process involving data transmission is job failure alerts that are automatically generated and routed to support personnel. Job failure alerts are notifications that indicate when a scheduled job or task fails to execute or complete successfully, such as due to errors, interruptions, or delays. Job failure alerts can help detect and correct any issues or anomalies in the job scheduling process involving data transmission by informing and alerting the support personnel who can investigate and resolve the problem. The other options are not as effective as job failure alerts in detecting issues or anomalies in the job scheduling process involving data transmission, as they do not provide timely or specific information or feedback. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management is a reporting technique that can help measure and improve the performance and reliability of the job scheduling process, but it does not provide immediate or detailed information on individual job failures.
Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP) is a preventive control that can help ensure the timeliness and security of the job scheduling process involving data transmission, but it does not detect any issues or anomalies that may occur during the process. Jobs are scheduled and a log of this activity is retained for subsequent review is a logging technique that can help record and track the status and results of the job scheduling process involving data transmission, but it does not provide real-time or proactive information on job failures. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 667
□□ □ □□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □ □ □□□□□?
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, and Benefits

9 Best Document Management Systems of 2023

NEW QUESTION: 668

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

A. □□□ □□(DoS)

B. SQL □□□
C. □□ □□
D. □□□
Answer: B (LEAVE A REPLY)
A SQL injection attack is a type of attack that targets security vulnerabilities in web applications to gain access to data sets. A SQL injection attack exploits a flaw in the web application code that allows an attacker to inject malicious SQL statements into the input fields or parameters of the web application. These SQL statements can then execute on the underlying database server and manipulate or retrieve sensitive data from the database. A SQL injection attack can result in data theft, data corruption, unauthorized access, denial of service or even complete takeover of the database server. A denial of service (DOS) attack is a type of attack that aims to disrupt the availability or functionality of a web application or a network service by overwhelming it with excessive requests or traffic. A phishing attack is a type of attack that uses deceptive emails or websites to trick users into revealing their personal or financial information or credentials. A rootkit is a type of malware that hides itself from detection and grants unauthorized access or control over a compromised system. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 669
□□ □□□ □□□□ □□□□□□ □□□□ □□ □ □□□ □□□□□ □□□□□.
□□ □ □□□□ □□□□ □□□□ □□ □□□□□?
A. □□□□ □□□ □□ □□ □□ □□□ □□□□□□.
B. □□□□ □□ □□ □□ □□□□ □□ □□□□ □□□□□□.
C. □□□□ □□ □□□ □□ □□□ □□□□□□.
D. □□□□ □□□□ □□ □□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
If an auditor implemented a control, they would later be reviewing their own work, which creates a self- review threat and compromises independence. Participating in the project without operational responsibilities (B) or providing advice (C) is acceptable as long as the auditor does not take ownership of decisions.
Designing audit modules (D) is also permissible since they are for audit use and do not affect operational processes. ISACA's Code of Professional Ethics and IS Audit Standards emphasize independence and objectivity as fundamental requirements to maintain credibility and avoid conflicts of interest.
References (ISACA): ISACA Standards for IS Audit and Assurance; ISACA Code of Professional Ethics.

NEW QUESTION: 670
□□□ □□□□□ □□□□ □□□ □□□ □□□□ □□□□□□□. □□ □ □□□ □□ □ □□ □□□□□ □□□ □ □□ □□□ □□□□□?

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: 671
IT □□□□□ □□□□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□□ □□□□□
B. □□□□ □□□□.
C. □□□ □□□□□□.
D. □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities.
References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 672
□□□□□□ □□□ □□□ □□□ □□ □□ □□□(IS) □□□□ □□ □□□□□□□ □□□□□ □□□□□□□. □□□□ □□□ □□ □□□ □□□□ □□□.
A. □□ □□□ □□□ □□ □□□ □□□□□.

B. □□□□□□□ □□ □□□ □□□□ □□□ □□□□□.
C. □□ □□□□ □□ □□ □□□ □□□□.
D. □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 673
□□□ □□□□□□ □□□ □□ □□□□ □□□ □□ □ □□□□□□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□ □□□ □ □□□ □□□ □□□□□ □□□ □ □□□□.
B. □□ □□ □□□□□ □□□□□ □□□□□ □□□□□.
C. □□□ □□□ □□ □□□□□ □□□□ □□□□□□□.
D. □□ □ □□ □□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
Unauthorized data modifications during conversion (D) are the most critical concern because they compromise data integrity, leading to inaccurate or corrupted information in the new system. Data migration should be performed with strict controls, including validation, reconciliation, and audit trails.
Other options:
Lack of online backups (A) is a risk but not as severe as compromised data integrity. Offline backups may still exist.
Undocumented change management (B) is a process deficiency but does not directly affect data accuracy.
Manual data conversion (C) increases risk but does not automatically indicate unauthorized changes.
Reference: ISACA CISA Review Manual, Information Systems Acquisition, Development, and Implementation

NEW QUESTION: 674
□□ □ □□ □□ □□□□□ □□ □□□ □□□□ □□□□ □□ □□□□□?
A. □□ □□ □□ □□□ □□ □□ □□□□□ □□□□ □□□□.

B. □□□ □□□□ □□□ □□□□ □□ □□□□□□ □□□□ □□□□.
C. □□ □□ □□ □ □□□ □□□□□□□.
D. □□ □□□□□ □□ □ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
According to the ISACA's Information Security Governance Guidance for Boards of Directors and Executive Management, the highest level of maturity of an information security program is Level 5: Optimized, which means that the program is aligned with the business objectives and strategy, and continuously monitors and improves its performance and effectiveness. A framework is in place to measure risks and track effectiveness, and the program is proactive, adaptive, and innovative.
The other options represent lower levels of maturity:
A training program is in place to promote information security awareness. This is Level 2: Repeatable, which means that the program has some basic policies and procedures, and provides awareness training to employees.
Information security policies and procedures are established. This is Level 3: Defined, which means that the program has formalized policies and procedures, and assigns roles and responsibilities for information security.
The program meets regulatory and compliance requirements. This is Level 4: Managed, which means that the program has established metrics and reporting mechanisms, and complies with relevant laws and regulations.
References: : ISACA. (2001). Information Security Governance Guidance for B

NEW QUESTION: 675
□□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□□ □□□□□.
B. □□ □□□ □□□□□ □ □□□ □□□.
C. □□ □□□ □□□□ □□□□.
D. □□ □□ □□□ □□□□ □□□.
Answer: (SHOW ANSWER)
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: 676

□□ □ □□□□ □□□(IM) □□□□ □□□ □□□□ □□□ □□□□ □ □□ □□□□ □□□ □□□□□?

A. □□□□ □□□□□ □□ □□ □□

B. □□ IM □□□ □□

C. □□□ □□□□ □□□ □□□□ □□

D. □□□□ □□□ □□□ □□□

Answer: C (LEAVE A REPLY)

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

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 677

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

A. □□ □□□□ □□□□

B. □□ □□ □□(KPI) □□

C. IT □□ □□ □□

D. IT □□□□ □□□□□ □□

Answer: (SHOW ANSWER)

Leveraging an IT governance framework is the best way to enable alignment of IT with business objectives, as it provides a set of principles, standards, processes, and practices that guide the effective delivery of IT services that support the organization's strategy and goals. Benchmarking against peer organizations, developing key performance indicators (KPIs), and completing an IT risk assessment are useful activities that can help measure and improve the performance and value of IT, but they are not sufficient to ensure alignment without a governance framework. References: CISA Review Manual (Digital Version), Chapter 1:

Information Systems Auditing Process, Section 1.2: IT Governance

NEW QUESTION: 678
□□ □□□ □□ □□□□ □□ □□ □□ □□(CRM) □□□□ □□ □□□ □□□□ □ □□□.
□□ □ □□ □ □□□□□ □□□□□?
A. □□ □□□□ □□□□□ □□ □□□□.
B. □□ □□□ □□□□□ □□ □□□□.
C. □□ □□□□ □□□□ □□□□ □□□□.
D. □□□ □□□□□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)
The greatest concern for an IS auditor evaluating the access controls for a shared customer relationship management (CRM) system is that audit logging is not enabled. Audit logging is a process that records and tracks the activities and events that occur on a system, such as who accessed what data, when, how, and why.
Audit logging can help monitor and verify the compliance and effectiveness of the access controls, as well as detect and investigate any unauthorized or suspicious access or actions. Audit logging can also provide evidence and accountability for the security and integrity of the system and the data.
Without audit logging, the IS auditor would not be able to audit the access controls for the shared CRM system, as there would be no reliable or traceable records of the access history or patterns. Without audit logging, the organization would also not be able to identify or respond to any potential breaches or incidents that may compromise the confidentiality, availability, or accuracy of the CRM data. Without audit logging, the organization would also not be able to demonstrate or prove itscompliance with any applicable policies, regulations, or standards that may require audit logging for CRM systems.
Single sign-on is not enabled is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a potential improvement or enhancement. Single sign-on is a process that allows users to access multiple systems or applications with one set of credentials, such as a username and password. Single sign-on can help simplify and streamline the user experience, as well as reduce the risk of password fatigue or compromise. However, single sign-on is not a mandatory or essential requirement for access controls, and it may also introduce some challenges or risks, such as dependency on a single point of failure or vulnerability.
Security baseline is not consistently applied is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a minor issue or gap. Security baseline is a set of minimum security standards or requirements that apply to a system or application, such as password policies, encryption protocols, or firewall rules. Security baseline can help ensure that the system or application meets a certain level of security and compliance. However, security baseline is not a sufficient or comprehensive

measure for access controls, and it may also need to be customized or adjusted according to the specific needs and risks of each system or application.
Complex passwords are not required is not a great concern for an IS auditor evaluating the access controls for a shared CRM system, but rather a common practice or recommendation. Complex passwords are passwords that are composed of a combination of different types of characters, such as letters, numbers, symbols, and cases. Complex passwords can help prevent or deter brute-force attacks or guessing attempts by making the passwords harder to crack or predict. However, complex passwords are not a guarantee or guarantee of security, and they may also have some drawbacks or limitations, such as user inconvenience, memorability issues, or reuse across multiple systems or applications.
References:
Customer Relationship Management Risks and Controls - CRM Simplified 1
Customer relationship management: A guide - Zendesk 2
How to Protect Your Customer Relationship Management (CRM) Data from Hackers 3
What is CRM? | A Definition by Salesforce 4

NEW QUESTION: 679
□□ □ □□□ □□□□□ □□ □□□□ □□□ □□□□□ □□□□ □□□ □□□□ □?
A. □□□□□ □□□ □□□ □ □□□□.
B. □ □□ □□□ □□
C. □□ □□□□ □□ □□□ □ □□□□.
D. □□□□ □□□ □□□□ □□□
Answer: B (LEAVE A REPLY)
The advantage of using agile software development methodology over the waterfall methodology is that it allows for quicker deliverables. Agile software development is an iterative and incremental approach that emphasizes customer feedback, collaboration, and adaptation. Agile software development delivers working software in short cycles, called sprints, that typically last from two to four weeks. This enables the development team to respond to changing requirements, deliver value faster, and improve quality. Waterfall software development is a linear and sequential approach that follows a predefined set of phases, such as planning, analysis, design, implementation, testing, and maintenance. Waterfall software development requires a clear and stable definition of the project scope, deliverables, and expectations before starting the development process. Waterfall software development can be slow, rigid, and costly, especially if changes occur during the later stages of the project. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.1: Project Management Practices

NEW QUESTION: 680

□□□□ □□□ □□□□□□ □3□ □□□ □□□□□ □□ □□ □□□ □□□ □□□
□ □□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □3□□ □□□□ □□ □ □□ □□ □□□ □□□□□□.
B. □3□ □□□□□ □□□ □□□ □□□□□□.
C. □□□ □3□ □□□□ □□□□□ □□□□□.
D. □□□ □□□□ □□□ □□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
The first step when planning an IS audit of a third-party service provider that monitors network activities is to review the roles and responsibilities of the third-party provider. This will help to establish the scope, objectives, and expectations of the audit, as well as to identify any potential risks, issues, or gaps in the service level agreement (SLA) between the organization and the provider. Reviewing the third party's monitoring logs and incident handling, evaluating the organization's third-party monitoring process, and determining if the organization has a secure connection to the provider are important steps, but they should be performed after reviewing the roles and responsibilities of the provider. References: CISA Review Manual (Digital Version)1, page 269.

NEW QUESTION: 681
□□ □ □□ □□□ □□□□ VoIP(Voice-over-IP) □□□ □□□□ □□□□ □ □□ □□ □ □□□ □□□□□?
A. □□□ □□□
B. □□ □□
C. □□□□□ □□□
D. □□ □□
Answer: (SHOW ANSWER)
The most important issue for an IS auditor to consider with regard to Voice-over IP (VoIP) communications is the homogeneity of the network, because it affects the quality, security, and reliability of the VoIP service. Ahomogeneous network is one that uses a single protocol or standard for VoIP communication, such as Session Initiation Protocol (SIP) or H.32312. A homogeneous network can reduce thecomplexity, latency, and interoperability issues that may arise from using different or incompatible protocols or devices forVoIP communication12. Continuity of service, identity management, and nonrepudiation are also important issues for VoIP communications, but not as important as the homogeneity of the network. References: 1: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.3 2: CISA Online Review Course, Module 4, Lesson 4

NEW QUESTION: 682
□□ □ □□□□ □□ □□□(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: 683
□□□ IT □□ □□ □□□□□ □□□□ □□ IS □□□□ □□ □□□ □□ □□ □□□ □ □ □□□ □□□ □□□□.
A. □□ 6□□ □□ □ □ □□□□□□□.
B. □□ □□□□ □□□□ □□ □□□ □□□□□□.
C. □□□ □□□□ □□□ □□□□□□.
D. IT □□□ □□□ □□□□ □□□□□□.
Answer: B (LEAVE A REPLY)
Capacity management must consider business changes to ensure IT resources can meet future demand. If changes to critical systems are omitted from planning, capacity forecasts will be inaccurate, leading to risks of downtime, bottlenecks, and unplanned outages. A six-month review (A) might be acceptable depending on system dynamics. Lack of administrator input (C) and reliance on service management (D) reduce planning quality but are less critical than missing major business drivers. COBIT DSS01 (Managed Operations) and APO02 (Managed Strategy) emphasize alignment between IT capacity and business requirements.
References (ISACA): COBIT 2019, DSS01 Managed Operations; APO02 Managed Strategy.

NEW QUESTION: 684
□□ □ □□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□□?
A. □□□ □□ □□ □□ □□ □□
B. □□□ □□□ □□□□ □□□ □□□ □□
C. □□□□ □□ □□ □□□ □□ □ □□

D. □□□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

Forensic investigations require unaltered digital evidenceto be admissible in court.Write-protectionensures 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: 685

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

A. □□□ □□ □□□ □□ □□□□ □□□□□.

B. □□□ □□ □□□ □□□ □□□ □□□□□ □□□□□□□.

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

D. □□ □□□ □□□ □□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)

This is because analyzing the data against predefined specifications is a method of data quality assessment that can help the organization achieve a reasonable level of data quality. Data quality assessment is the process of measuring and evaluating the accuracy, completeness, consistency, timeliness, validity, and usability of the data. Predefined specifications are the criteria or standards that define the expected or desired quality of the data. By comparing the actual data with the predefined specifications, the organization can identify and quantify any gaps, errors, or deviations in the data quality, and take corrective actions accordingly12.

Reviewing data against data classification standards (A) is not the best answer, because it is not a method of data quality assessment, but rather a method of data security management. Data classification standards are the rules or guidelines that define the level of sensitivity and confidentiality of the data, and determine the appropriate security and access controls for the data. For example, data can be classified into public, internal, confidential, or restricted categories. Reviewing data against data classification standards can help the organization protect the data from unauthorized or inappropriate use or disclosure, but it does not directly improve the data quality3.

Outsourcing data cleansing to skilled service providers (B) is not the best answer, because it is not a recommendation to help the organization achieve a reasonable level of data

quality, but rather a decision to delegate or transfer the responsibility of data quality management to external parties. Data cleansing is the process of detecting and correcting any errors, inconsistencies, or anomalies in the data. Skilled service providers are third-partyvendors or contractors that have the expertise and resources to perform data cleansing tasks. Outsourcing data cleansing to skilled service providers may have some benefits, such as cost savings, efficiency, or scalability, but it also has some risks, such as loss of control, dependency, or liability4.
Consolidating data stored across separate databases into a warehouse is not the best answer, because it is not a method of data quality assessment, but rather a method of data integration and storage. Data integration is the process of combining and transforming data from different sources and formats into a unified and consistent view. Data warehouse is a centralized repository that stores integrated and historical data for analytical purposes. Consolidating data stored across separate databases into a warehouse can help the organization improve the availability and accessibility of the data, but it does not necessarily improve the data quality.

NEW QUESTION: 686
IS □□□□ □3□ □□□□□ □□ □□ □□(KPI) □□□ □□□□□. □□ □ □□□□ □□ □□□□ □ □□□ □□□□□?
A. KPI □□□□ □□□□ □□ □□□□.
B. KPI□ □□□□ □□□□ □□□□□.
C. □□ KPI□ □□□□□ □□ □□□□.
D. KPI□ □□□□□ □□ □□□□.
Answer: B (LEAVE A REPLY)
KPIs are not clearly defined is the most concerning finding for an IS auditor, because it implies that the third- party vendor does not have a clear understanding of what constitutes success or failure in their performance.
This can lead to inaccurate or misleading reporting, poor decision making, and lack of accountability. KPIs should be SMART (specific, measurable, achievable, relevant, and time-bound) and aligned with the business objectives and expectations of the stakeholders12. References: 1: CISAReview Manual (Digital Version), Chapter 5, Section 5.3.2 2: CISA Online Review Course, Module 5, Lesson 3

NEW QUESTION: 687
□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□ □□ □□(PII)□ □□□□□. □3□ □□ □□ □□□□□ □□□□ □□ □□□(IS) □□□□ □□ □□□ □□ □□□ □□□ □□?
A. □□□□□ □□ □ □□□□ □□□□ □□□□ □□□□□.
B. □□ □□□ □□□□□□ □□□□ □□□ □□□□ □□□□.
C. □□□□□ □3□□ □□ □□ □□□□ □□□□□□.
D. □□ □□□□□ □3□ □□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The greatest concern is if the vendor is excluded from the organization's third-party due diligence process.
Without proper due diligence, the organization has no assurance that the vendor meets minimum security and privacy requirements, exposing PII to significant risk.
Option A: External-facing services carry risk but can be mitigated by proper controls.
Option B: Lack of dedicated privacy staff may increase risk, but controls may still exist.
Option C: Fourth-party hosting adds risk but is acceptable if included in due diligence.
Option D: Correct - exclusion from due diligence represents a fundamental breakdown in vendor risk management.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on third-party/vendor risk management and data privacy.

NEW QUESTION: 688
□□ □□□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□□□□ □□□ □□□ □□□□ □□□
B. □□ □□□□ □□□ □□ □□
C. □□ □□ □□ □□
D. □□ □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Automated monitoring tools increase the likelihood of detecting suspicious activity (Option A) by continuously analyzing security logs for anomalies.
ISACA CISA Reference: Security Information and Event Management (SIEM) solutions are recommended for privileged access monitoring.

NEW QUESTION: 689
□□□ □□ □□□ □□ □□□ □□□ □□ □□ □ □□ □□ □□□ □□□ □□□ □□ □□□□ □□□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□□□□ □□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□.
B. □□ □□ □□□ □□ □□□□ □□□ □ □□□□□□ □□□.
C. □□ □□□ □□□ □□□ □□ □□□ □□□ □ □□□ □□□.
D. □□ □□ □□□□ □□□ □□□□ □□□ □ □□□ □□□□ □□□ □□□ □□□ □□.
Answer: (SHOW ANSWER)
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 and 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: 690

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

A. □□□□ □□□ □□(BCP) □□□

B. □□ □□ □□(BIA)

C. □□ □□ □□(DRP) □□□

D. □□ □□

Answer: B (LEAVE A REPLY)

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects or consequences of disruptions or disasters on an organization's critical business functions or processes. A BIA can help prioritize the recovery of critical functions by assessing their importance and urgency for the organization's operations, objectives, and stakeholders, and determining their recovery time objectives (RTOs), which are the maximum acceptable time for restoring a functionafter a disruption. A business continuity plan (BCP) testing is a process that verifies and validates the effectiveness and readiness of a BCP, which is a document that outlines the strategies and procedures for ensuring the continuity of critical business functions in the event of a disruption or disaster. A BCP testing does not prioritize the recovery of critical functions, but rather evaluates how well they are recovered according to the BCP. A disaster recovery plan (DRP) testing is a process that verifies and validates the effectiveness and readiness of a DRP, which is a document that outlines the technical and operational steps for restoring the IT systems and infrastructure that support critical business functions in the event of a disruption or disaster. A DRP testing does not prioritize the recovery of critical functions, but rather evaluates how

well they are supported by the IT systems and infrastructure according to the DRP. A risk assessment is a process that identifies and analyzes the potential threats and vulnerabilities that could affect an organization's critical business functions or processes. A risk assessment does not prioritize the recovery of critical functions, but rather estimates their likelihood and impact of being disrupted by various risk scenarios.

NEW QUESTION: 691
□□ □ □□ □ AI □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □ □□ □□□□□?
A. □□ □□ □□□ □□ □□□ □□□□□□□.
B. □□ □ □□ □□□ □ □□ □□□ □□ □ □□ □□□□□□□.
C. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □ □□□□.
D. □□□□ □□□ □□□□ □ □□□ □□ □□ □ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The greatest concern is the lack of documentation for the basic assumptions and formulas used to develop the decision logic. In AI and algorithmic systems, undocumented assumptions, logic, and model foundations undermine transparency, explainability, validation, governance, auditability, and the ability to assess whether outputs are reliable and appropriate. ISACA's AI audit guidance specifically emphasizes questioning assumptions and identifying conditions that are taken for granted within AI systems.
Option D is correct because without documented assumptions and formulas, neither management nor the auditor can effectively understand how the AI system reaches conclusions, validate whether it is working as intended, assess bias or error, or confirm whether controls are adequate. ISACA's AI-related guidance highlights that assumptions embedded in AI systems must be examined because changing environments, unreliable data, or hidden logic can create serious control weaknesses.
Option A is not the greatest concern by itself. Outsourcing development to vendors may introduce third-party risk, but vendor use is common and can be controlled through contracts, review, validation, and oversight.
The mere fact of outsourcing does not create as severe a control weakness as undocumented decision logic.
Option B is a potential concern because annual review might be too infrequent depending on the system's risk and rate of change. However, even with infrequent review, the organization would still have documented policy and decision logic to examine. A complete lack of documentation of assumptions and formulas is more serious because it prevents meaningful review altogether.
Option C is also a concern, but vendor maintenance access can be managed through access controls, logging, approvals, segregation, and monitoring. Access by contracted developers is not inherently unacceptable. The more fundamental weakness is the absence of documented logic foundations, which affects governance and auditability at the core.

Therefore, the greatest concern is D because undocumented assumptions and formulas make the AI system insufficiently transparent and far harder to audit, validate, and control.
References (Official ISACA):
* ISACA Journal, AI Risk and Mitigation: Tips and Tricks for Auditing in the AI Era - stresses questioning assumptions and identifying taken-for-granted conditions in AI systems.
* ISACA Journal, Algorithms and the Auditor - supports the auditor's role in questioning algorithmic reliability and possible errors.
* ISACA White Paper, Leveraging COBIT for Effective AI System Governance - highlights risk assessment and governance throughout the AI life cycle.

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 692
□□ □ □□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□ □ □□□ □□ □□□ □□□?
A. □□□ □□□ □□□ □□□ □□□ □□□ □□□□.
B. □□□□ □□□ □□□ □□□ □□□ □ □□□□□.
C. □□ □□□ □□ □□□ □□□□□□.
D. □□ □□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The evidence collected during a digital forensic investigation would not be admissible in court if the logs failed to identify the person handling the evidence. This would violate the chain of custody principle, which requires that the evidence be properly documented, secured, and tracked throughout the investigation process.
The chain of custody ensures that the evidence is authentic, reliable, andtrustworthy, and that it has not been tampered with or altered. The person who collected the evidence, whether qualified or not, is not relevant to the admissibility of the evidence, as long as they followed the proper procedures and protocols. The evidence collected by the internal forensics team can be admissible in court, as long as they are independent, objective, and competent. The evidence does not need to be fully backed up using a cloud-based solution prior to the trial, as long as it is preserved and protected from damage or loss. References: ISACA Journal Article: Digital Forensics: Chain of Custody

NEW QUESTION: 693

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

NEW QUESTION: 694
□□ □□□□□ □□□□ □ □□ □□ □□ □□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□. □□ □ □□ □□□ □□□ □□ □□ □□ □□ □□ □ □□□□ □ □□ □□□ □□ □□ □□□□□?
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 virtualfirewall 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: 695
□□□ □□ □□(DLP) □□□ □□ □ □□□ □□□□ □□ □□□(IS) □□□□ □□ □ □□□ □□□ □□ □ □□□□□?
A. □ □□□ □□ □□□ □□ □□□ □□□ □□□□□□□.
B. □□□□ □□□ □□□□ □□□□ □ □□□□□.
C. □□ □□ □□□ □□ □□ □□□ □□□ □□□□□.
D. □□□ □□ □□□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
A data loss prevention (DLP) tool implemented in monitor mode only observes and logs potential data leakage but does not actively prevent it. This leaves the organization vulnerable to data breaches, making it the most critical concern in a pre-implementation review.
Crawlers for Sensitive Data (Option B):While crawlers may pose a performance impact, they are essential for discovering sensitive data.
Deep Packet Inspection (Option C):Though it introduces privacy considerations, it is a standard DLP functionality for inspecting data in transit.
Encryption Key Management (Option D):While important for security, improper management does not immediately prevent DLP functionality.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 696
□□ □ □□ □□□ □□□□ □□□ IT □□□ □□□ □ □□ □□□□ □ □□□ □□□ □□?
A. □□ □□□ □□□ IT □□□□□ □□ □ □□□□□.
B. □□□ □□□□□ □□ □ □□□□□□ □□□□.
C. □□ □□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□ IT □□□ □□□□ □□□.
Answer: (SHOW ANSWER)
The best answer is B. The policies are not regularly reviewed and updated.
ISACA guidance notes that, when auditing policy documents, one of the quickest indicators of trouble is the absence of current reviews, changes, approvals, and alignment with actual practice. If policies are outdated, they may no longer reflect the organization's control environment, regulatory obligations, technologies, or business processes. That creates a direct governance and compliance risk.

Option A is generally a positive sign, not a concern, because formal review and approval supports governance. Option C can matter, but lack of direct mapping to best practices is usually less serious than having stale policies that no longer reflect reality. Option D is not ideal if policies exclude broader stakeholders, but IT policies are often primarily directed toward IT staff while still being supported by wider governance documents. The most serious issue is that outdated policies may be ineffective, unenforceable, or inconsistent with current controls.
References (Official ISACA):
* ISACA, Do Your Policy Documents Represent Current Practices?
* ISACA Journal, IS Audit Basics: The Auditors, IS/IT Policies and Compliance

NEW QUESTION: 697
□□ □ □□ □□□□□□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□ □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □ □□□ □□ □□
B. □□ □ □□□ □□ □□□
C. □□ □ □□□ □□□□ count □□□ □□□□ □□□□□.
D. □□ □ □□□ □□□ □□ □□□ □□□ □□□
Answer: (SHOW ANSWER)
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: 698
□□□□ □□ □□□ □□□□ □□□□□□ □□ □□□□□ □□□ □□□ □□□□.
A. □□□ □□.
B. □□□ □□□.
C. □□.
D. □□ □ □□□(PKI).
Answer: (SHOW ANSWER)

NEW QUESTION: 699
□□ □ □□□□ □□ □□ □□(DRP)□ □□□□ □□□ □□ □ □□□□ □□ □□□□ □?
A. □□□ □□ □□□ □□□
B. □□ □□ □□
C. □□□ □□ □□
D. □□ □□ □□□
Answer: D (LEAVE A REPLY)
A disaster recovery plan (DRP) is a set of procedures and resources that enable an organization to restore its critical operations, data, and applications in the event of a disaster1. A DRP should be aligned with the organization's business continuity plan (BCP), which defines the strategies and objectives for maintaining business functions during and after a disaster1.
To ensure that a DRP is effective, it should betested regularly and thoroughly to identify and resolve any issues or gaps that might hinder itsexecution2345. Testing a DRP can help evaluate its feasibility, validity, reliability, and compatibility with the organization's environment and needs4. Testing can also help prepare the staff, stakeholders, and vendors involved in the DRP for their roles and responsibilities during a disaster3.
There are different methods and levels of testing a DRP, depending on the scope, complexity, and objectives of the test4. Some of the common testing methods are:
Walkthrough testing: This is a step-by-step review of the DRP by the disaster recovery team and relevant stakeholders. It aims to verify the completeness and accuracy of the plan, as well as to clarify any doubts or questions among the participants45.
Simulation testing: This is a mock exercise of the DRP in a simulated disaster scenario. It aims to assess the readiness and effectiveness of the plan, as well as to identify any challenges or weaknesses that might arise during a real disaster45.
Checklist testing: This is a verification of the availability and functionality of the resources and equipment required for the DRP. It aims toensure that the backup systems, data, anddocumentation are accessible and up- to-date45.

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

NEW QUESTION: 700
□□ □□□□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□□□ □ □□□□ □□ □□□ □□□□□.
B. □ □□□□ □□□ □□□□ □□□ □□□□□ □□□□□.
C. □□ □□□ □□□□ □□□ □□
D. □ □□□□ □□ □□□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The primary purpose of performing a parallel run of a new system is to validate the new system against its predecessor. A parallel run is a strategy for system changeover where a new system slowly assumes the roles of the older system while both systems operate simultaneously. This allows for comparison of the results and outputs of both systems to

ensure that the new system is working correctly and reliably. A parallel run can also help identify and resolve any errors, discrepancies, or inconsistencies in the new system before the old system is discontinued.
The other options are not the primary purpose of performing a parallel run of a new system. A. To train the end users and supporting staff on the new system. Training is an important part of system implementation, but it is not the main reason for doing a parallel run. Training can be done before, during, or after the parallel run, depending on the needs and preferences of the organization. B. To verify the new system provides required business functionality. Verifying the business functionality of the new system is part of user acceptance testing (UAT), which is a formal and structured process of testing whether the new system meets the specifications and expectations of the users and stakeholders. UAT is usually done before the parallel run, as a prerequisite for system changeover. C. To reduce the need for additional testing. Reducing the need for additional testing is not the primary purpose of performing a parallel run, but rather a possible benefit or outcome of doing so. A parallel run can help ensure that the new system is thoroughly tested and validated in a real-worldenvironment, which may reduce the likelihood of encountering major issues or defects later on.
However, additional testing may still be needed after the parallel run, depending on the feedback and evaluation of the users and stakeholders.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
IS

NEW QUESTION: 701
□□ □ □□□ □□□□□ □□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□□ □□ □□ □□□□ □□□□□.
B. □□□□ □□□□□ □□□ □□□□□.
C. □□ □□□ □□□□ □□□□□ □□□□□□.
D. □□ □□□ □□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The most efficient way to identify segregation of duties violations in a new system is to review a report of security rights in the system. Segregation of duties is a control principle that aims to prevent or detect errors, fraud, or abuse by ensuring that no single individual has the ability to perform incompatible or conflicting functions or activities within a system or process. A report of security rights in the system can provide a comprehensive and accurate overview of the roles, responsibilities, and access levels assigned to different users or groups in the system, and can help to identify any potential segregation of duties violations or risks. The other options are not as efficient as reviewing a report of security rights in the system, because they either rely on observation or testing rather than analysis, or they focus on existing rather than potential violations. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

NEW QUESTION: 702
□□ □□□(IS) □□□□ □□□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□□. □□ □ IS □□□□ □□□ □ □□ □□ □□□ □□ □□□ □ □□□□?
A. □□ □□ □□□□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□ □□□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 703
□□ □ □□ □□ □□ □□□□□ □□ □□ □□ □□ □□□□ □□ □□ □□□□ □□ □ □□□□ □□ □ □□□ □□□□□?
A. □□ □□ □□ □ □□ □□□ □□□
B. □□ □□□□ □□ □□ □□
C. □□□□□ □□□ □□□ □□□□ □□□
D. □□ □□□ □□ □□ □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 704
□□ □□□□ □□□□ □ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□□ □.
A. □□□□ □□□□□ □□□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □□□ □ □□ □□□□ □ □□
D. □□ □□ □□□□ □□□ □□ □□□ □□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
A firewall between internal network segments improves security and reduces risk by inspecting all traffic flowing between network segments and applying security policies. This will prevent unauthorized or malicious access, data leakage, or network attacks from compromising the network resources or data. Logging all packets passing through network segments may provide audit trails and evidence, but not prevent or mitigate security incidents. Monitoring and reporting on sessions between network participants may help to identify anomalous or suspicious activities, but not block or filter them. Ensuring all connecting systems have appropriate security controls enabled may enhance the overall network security posture, but not isolate or segregate different network segments. References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, section "Book COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution | Digital | English"

NEW QUESTION: 705
□□ □ □□ □□ □□□□□ □□□□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□ □□ □□
B. IT □□□□ □□□ □□ □□ □□ □□
C. □□□□□ □□□ □□
D. □□□ □□□ □□ □ □□
Answer: A (LEAVE A REPLY)

Decreased time for incident resolution is the best indicator that an incident management process is effective.
Incident management is a process that aims to restore normal service operation as quickly as possible after an incident, which is an unplanned interruption or reduction in quality of an IT service. Decreased time for incident resolution means that the incident management process is able to identify, analyze, respond to, and resolve incidents efficiently and effectively. The other indicatorsdo not necessarily reflect the effectiveness of the incident management process, as they may depend on other factors such as the nature, frequency, and severity of incidents. References: CISA Review Manual, 27th Edition, page 372

NEW QUESTION: 706
□□ □ □□ □□□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□ □□
C. □□ □□ □ □□ □□
D. □□ □□□□ □□□ □□
Answer: A (LEAVE A REPLY)
Issuing authentication tokens is the most reliable method of preventing unauthorized logon, as it provides a strong form of authentication that requires users to present something they have (the token) and something they know (the personal identification number or PIN) to access the system. Authentication tokens are physical devices that generate a one-time password or code that changes periodically and is synchronized with the authentication server. This makes it difficult for attackers to steal or guess the credentials of legitimate users. Reinforcing current security policies, limiting after-hours usage and installing an automatic password generator are not as reliable as issuing authentication tokens, as they do not provide a strong form of authentication and may still be vulnerable to unauthorized logon attempts. References:
[Authentication Token Definition]
Authentication | ISACA

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html
(**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)

NEW QUESTION: 707
□□ □ □□ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□□ □□□□ □□□□ □□

B. □□ □□ □□ □□□□□ □□□□ □□□□ □□□ □□□ □□
C. □□ □□ □□ □ □□□ □□ □□□ □□□□ □□
D. □□ □□ □□□ □□□ □□□ □□□ □□
Answer: D (LEAVE A REPLY)
The main purpose of an information security management system (ISMS) is to reduce the frequency and impact of information security incidents. An ISMS is a systematic approach to managing information security risks, policies, procedures, and controls within an organization. An ISMS aims to ensure the confidentiality, integrity, and availability of information assets, as well as to comply with relevant laws and regulations. The other options are not the main purpose of an ISMS, but rather some of its possible benefits or components. References:
CISA Review Manual (Digital Version), Chapter 7, Section 7.11
CISA Review Questions, Answers and Explanations Database, Question ID 205

NEW QUESTION: 708
□□ □ □□ □□□□□ □□□ □□□ □□ □□□ □□□□□ □□□□□?
A. □□ □□ □□□□□ □□□ □□ □□□
B. □□□ □□□ □□□□ □□ □□ □□ □□□ □□
C. □□□ □ □□ □□□ □□
D. □□□□□ □□ □□ □□
Answer: B (LEAVE A REPLY)
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: 709
□□ □ □□ □□□ □□□□ □□ □□ □ □□□ □□□ □ □□ □□□□ □□□□ □ □ □□ □□□□□?
A. □□□□ □□□ □□ □□□□□ □□ □□□ □□□ □□□□ □□□ □□
B. □□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□
C. □□□ □□□ □□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□ □□
D. □□□ □□ □□□ □□ □ □□ □□ □□ □□□ □□□□ □□□□□ □□
Answer: B (LEAVE A REPLY)

CISA-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CISA-KR □□! DumpTop □ □□ **CISA-KR** □□ □□□ □□□□□□, DumpTop CISA-KR □□ □□ □ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop CISA-KR □□□ □□□□□. https://www.dumptop.com/ISACA/CISA-KR-dump.html (**1518** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)