IIA.IIA-CIA-Part3-KR.v2026-02-16.q207

□□□□:	IIA-CIA-Part3-KR
□□□□:	Business Knowledge for Internal Auditing (IIA-CIA-Part3 Korean Version)
□□□:	IIA
□□ □□ □□ □:	207
□□:	v2026-02-16
# □□ □:	128
# □□ □□□:	2070
https://www.krdump.com/IIA.IIA-CIA-Part3-KR.v2026-02-16.q207.html	

NEW QUESTION: 1
□□ □□ □□ □□ □ □□ □□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□ □ □□□ □□ □□□ □□□□ □□ □□□ □□
B. □□□ □□□ □□ □ □□ □□ □□□ □□□ □□
C. □□ □□ □□□ □□ □□ □□□□□ □□ □□ □ □□ □□ □ □□□ □□
D. □□ □□ □□□ □□ □□□ □□ □ □□, □□ □□, □□□□ □□□ □□□ □□ □ □□ □□
Answer: C (LEAVE A REPLY)
Innovation in internal audit is reflected in how the function applies new technologies, methodologies, and thought leadership. Measuring staff application of technology in audit fieldwork and their engagement in professional organizations/publications demonstrates innovation and forward-looking practices.
Options A, B, and D measure performance, satisfaction, or compliance but do not specifically address innovation.
Reference:
IIA Practice Guide - Measuring Internal Audit Effectiveness and Efficiency.

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

According to the IIA Standards, the CAE must ensure that the internal audit activity is appropriately staffed with competent individuals to achieve the approved audit plan. While risk-based planning and collaboration with risk functions support effectiveness, the most direct way to ensure resources are adequate is by developing and maintaining the competencies of internal audit staff through training, recruitment, and professional development.
Mapping the audit risk assessment (Option B), collaboration with risk functions (Option C), or refining processes (Option D) may strengthen planning and alignment, but they do not directly address the resource requirement. Only enhancing and ensuring competencies ensures the internal audit activity has the skills necessary to execute the plan.
Reference:
IIA Standards - Standard 2030: Resource Management.

NEW QUESTION: 3
□□ □□□ □□ □ □□□ □□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□.
B. □□ □□ □□□.
C. □□ □ □□□ □□□□□.
D. □□ □□□□□.
Answer: D (LEAVE A REPLY)
Evaluating an organization's performance involves analyzing its profitability over a specific period. The budgeted income statement serves as a crucial tool in this assessment. Here's an analysis of the provided options:
A). Cash Budget:
A cash budget forecasts the organization's cash inflows and outflows over a particular period, ensuring sufficient liquidity to meet obligations. While it is vital for managing cash flow, it doesn't provide a comprehensive view of overall performance, as it excludes non-cash items like depreciation and doesn't reflect profitability.
B). Budgeted Balance Sheet:
The budgeted balance sheet projects the organization's financial position at a future date, detailing expected assets, liabilities, and equity. Although it offers insights into financial stability and structure, it doesn't directly measure operational performance or profitability.
C). Selling and Administrative Expense Budget:
This budget estimates the costs associated with selling and administrative activities. While controlling these expenses is essential, this budget focuses solely on a specific cost area and doesn't encompass the organization's overall financial performance.
D). Budgeted Income Statement:
The budgeted income statement, also known as the pro forma income statement, projects revenues, expenses, and profits for a future period. It provides a detailed forecast of expected financial performance, including:
* Revenue Projections: Estimations of sales or service income.

* Cost of Goods Sold (COGS): Direct costs attributable to the production of goods sold.
* Gross Profit: Revenue minus COGS.
* Operating Expenses: Expenses related to regular business operations, such as salaries, rent, and utilities.
* Net Income: The final profit after all expenses have been deducted from revenues.
By comparing the budgeted income statement to actual performance, organizations can assess how well they met their financial goals, identify variances, and make informed decisions to improve future performance.
This comprehensive overview makes it the most effective tool among the options provided for evaluating an organization's performance.

NEW QUESTION: 4
□□ □□ □ □□ □□ □□ □□ □□□ □□□□□ □□□ □□□ □□□□ □□□ □□ □□ □ □□□ □□□?
A. □□ □□
B. □□□□ □□□□
C. □□ □□ □□
D. □□ □□□ □□ □□ □□(SAIV)
Answer: B (LEAVE A REPLY)
The QAIP (Quality Assurance and Improvement Program) requires both ongoing monitoring and periodic assessments. Among these, ongoing monitoring is the mechanism that ensures continuous evaluation of whether engagements are being performed with quality and in conformance with the Standards.
Option A (periodic assessments) review effectiveness but are not continuous. Option C (external assessments) and Option D (SAIV) are broader and periodic, not engagement-level consistency checks.
Reference:
IIA Standards - Standard 1311: Internal Assessments.

NEW QUESTION: 5
IIA □□□ □□□ □□ □ □□□□□□ □□ □□□ □□(□□) □□ □□□□□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□ □□□□ □□□ □□ □□ □□□□ □□□□□.
B. □□□□□ □□□ □□□, □□□□ □□□ □□□.
C. □□ □□□ □□ □□□ □□□ □□□
D. □□□□□ □□□□ □□ □□ □□□□□□ □□□□ □□□
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
A management (audit) trail ensures financial transparency by tracking who initiated, approved, and processed transactions within the general ledger (GL).
Option A (Report on data outside system parameters) is a validity control, not an audit trail.

Option C (Comparison of results with input) ensures accuracy but is not a comprehensive audit trail.
Option D (Error-free processing confirmation) does not track user activity.
Since audit trails require tracking transactions by time and individual, Option B is correct.
Reference: IIA IT Controls - Audit Trails & Financial Systems

NEW QUESTION: 6
□□ □□ □□□ □□□ □, □□□□□□□(CAE)□ □□□□ □□ □□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□□□ □□□□ □□□ □□□□□□. □ □□ □ □□□□ □□ CAE□ □□ □□ □□□ □□□ □□□?
A. □□□ □□ □□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□ □□□ □□□□□.
C. □□ □□□□□ □□□ □□□□□.
D. □□□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
According to the International Standards for the Professional Practice of Internal Auditing, when significant risk exposures remain unaddressed after a follow-up engagement, the CAE must first discuss the matter with the appropriate level of management responsible for the area. The purpose is to determine whether there is a valid reason for not implementing the recommended corrective actions, to clarify management's perspective, and to encourage timely resolution.
If management still refuses to act and the risk remains high, the CAE must then escalate the issue to senior management and, if necessary, to the board. Immediate escalation to the board without first discussing with management is inappropriate, as it bypasses the chain of accountability. Reporting directly to external auditors is also not the responsibility of the CAE unless specifically mandated by regulation or law.
Therefore, the correct initial step is to discuss the issue with management responsible for the risk area (Option B).
Reference:IIA Standards - Standard 2500: Monitoring Progress; Implementation Guide 2500 - Monitoring Progress.

NEW QUESTION: 7
□□□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□□ □ □□□□ □□□□ □□□ □□ □ □□ □□□□□□ □□□□□?
A. □□□□ □□ □□.
B. □□□□ □□ □□
C. □□ □□ □□.
D. □□□□ □□ □□
Answer: (SHOW ANSWER)

In project integration management, the coordination of technical and organizational interfaces typically occurs during the Project Plan Execution phase. At this stage, project managers and teams work together to:
* Implement the project plan.
* Manage interdependencies between technical and business processes.
* Ensure all project components are aligned.
* Coordinate different stakeholders, vendors, and internal teams.
* (A) Project plan development:
* This phase involves defining objectives, scope, timelines, and resource allocation but does not focus on coordination of interfaces.
* (B) Project plan execution (Correct Answer):
* This phase involves implementing the project and actively managing its technical and organizational interfaces, making it the correct answer.
* (C) Integrated change control:
* This process ensures that project changes are properly managed, but it does not focus on initial coordination of interfaces.
* (D) Project quality planning:
* This phase focuses on setting quality standards and criteria, but not on the integration of technical and organizational interfaces.
* IIA Practice Guide: Auditing Projects - Highlights that project execution is where coordination across different teams and stakeholders is critical.
* PMBOK Guide (Project Management Body of Knowledge) - States that integration management during execution ensures that all elements of the project work together effectively.
* COSO ERM Framework - Supports the alignment of business processes and technical execution as part of risk management.
Analysis of Each Option:IIA References:Conclusion:Since technical and organizational coordination is essential during project execution, option (B) is the correct answer.

NEW QUESTION: 8
□□ □□□□ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□. □□□□ □□□ □ □ □ □□□□□□ □□□ □□□ □□ 10% □ 7%□ □□□□□. □□ □ □□ □□□□ □ □□□ □□□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)
Vertical analysis expresses each financial statement item as a percentage of a base figure (e.g., revenue).

In this case, the internal auditor calculates electricity and depreciation expenses as a percentage of revenue
, which is a clear application of vertical analysis.
* (A) Horizontal analysis:
* Compares financial data across different periods to identify trends and growth.
* The given scenario does not compare financial statements over time, making this incorrect.
* (B) Vertical analysis (Correct Answer):
* Expresses each line item as a percentage of a base figure (e.g., revenue for income statements, total assets for balance sheets).
* In this case, electricity and depreciation expenses are calculated as a percentage of revenue, confirming vertical analysis.
* (C) Ratio analysis:
* Involves calculating financial ratios (e.g., profitability, liquidity, efficiency).
* This scenario does not involve ratios but rather percentage-based comparisons, making it incorrect.
* (D) Trend analysis:
* Identifies patterns over multiple periods (e.g., revenue growth over five years).
* The question does not involve time-based comparisons, so this answer is incorrect.
* IIA Practice Guide: Internal Audit and Financial Reporting - Recommends vertical analysis for financial statement assessment.
* IIA Standard 2320 - Analysis and Evaluation - Requires auditors to apply relevant analytical techniques, including percentage-based evaluations.
* COSO Internal Control Framework - Financial Reporting Component - Supports financial data analysis techniques such as vertical and horizontal analysis.
Analysis of Each Option:IIA References:Conclusion:Since the auditor expressed financial statement items as a percentage of revenue, option (B) is the correct answer.

NEW QUESTION: 9
□□ □ □□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□ □□□□□?
A. □□□ □□□ □□ □□ □□□ □□□□□ □ □□□ □□□.
B. □□ □□□□ □□□□ □ □□□ □□□ □□□ □□□□□.
C. □□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□□ □ □□□ □□□.
D. □□ □□□□ □□□□ □□□ □□ □□□ □□□ □ □□□ □□□□.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Data analytics in internal auditing provides quantitative, evidence-based insights, enhancing audit conclusions and decision-making.
Option B (Reduces report preparation time) - While efficiency is a benefit, the main advantage is improved accuracy and factual support.

Option C (Prevents overlooking risks) - While true, data analytics primarily strengthens evidence collection.
Option D (Monitoring controls) - Auditors assess controls, but data analytics enhances findings through data- driven validation.
Thus, Option A is correct, as data analytics strengthens audit conclusions with factual evidence.
Reference: IIA Audit Analytics Guide - Data-Driven Internal Auditing

NEW QUESTION: 10
□□□□ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□□□□. □ □□□ □□ □ □□ □□□□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□ □□ □ □□□□ □□□ □□□□□□. □□ □ □ □□□ □□□ □□□□□□ □ □□ □□□ □ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□,
B. □□□ □□□ □□□□ □□ □□□ □□ □.
C. □□□ □□ □□ □□□ □□ □ □ □□□□□□ □□□.
D. □□□ □□□ □□ □ □ □□ □□□ □□ □□□□□ □□.
Answer: A (LEAVE A REPLY)
Fraud in time-tracking systems-such as "buddy punching" (where one employee clocks in/out for another)
-is a common payroll fraud scheme. The most effective method to prevent this is biometric authentication, which ensures that only the actual employee can clock in or out.
* (A) Face or finger recognition equipment. #
* Correct. Biometric authentication (such as fingerprint or facial recognition) is the most effective solution because it uniquely identifies each individual, making it impossible for an employee to clock in on behalf of a colleague.
* IIA GTAG "Managing and Auditing IT Vulnerabilities" recommends biometric authentication as a strong fraud prevention measure.
* IIA Practice Guide "Fraud Prevention and Detection in an Automated Environment" highlights the use of biometrics for enhancing security in access control systems.
* (B) Radio-frequency identification (RFID) chips to authenticate employees with cards.
* Incorrect. RFID cards can be shared between employees, allowing fraud to continue. They are useful for access control but do not verify the identity of the person using the card.
* (C) A requirement to clock in and clock out with a unique personal identification number (PIN).
* Incorrect. PINs can be shared or stolen, making them ineffective in preventing buddy punching.
* (D) A combination of a smart card and a password to clock in and clock out.
* Incorrect. Like RFID and PIN systems, smart cards and passwords can be shared, making them ineffective against fraudulent time-tracking practices.
* IIA GTAG - "Managing and Auditing IT Vulnerabilities"

* IIA Practice Guide - "Fraud Prevention and Detection in an Automated Environment"
* COSO Framework - Fraud Risk Management
Analysis of Answer Choices:IIA References:Thus, the correct answer is A, as biometric authentication directly verifies the employee's identity, preventing time-tracking fraud.

NEW QUESTION: 11
□□□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□?
A. □□ □□ □□□ □□□ □□□□ □□□□□□.
B. □□□ □□□ □□ □ □ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□.
D. □□ □□□□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)
* Understanding Data Analysis in Internal Auditing
* Data analytics enhances audit testing by identifying patterns, anomalies, and high-risk transactions within large datasets.
* Advanced analytics tools (e.g., AI, machine learning, continuous auditing) help auditors pinpoint areas of fraud, compliance violations, or operational inefficiencies.
* Why Option B is Correct?
* Data analysis improves risk assessment by allowing auditors to focus on high-risk areas, such as fraudulent transactions or control weaknesses.
* IIA Standard 1220 - Due Professional Care requires auditors to use technology to improve audit effectiveness, including identifying risks.
* IIA GTAG (Global Technology Audit Guide) 16 - Data Analytics supports using analytics to enhance risk-based auditing.
* Why Other Options Are Incorrect?
* Option A (Improves effectiveness of spot check testing techniques):
* Data analysis enables continuous and full-population testing, rather than just improving spot checks.
* Option C (Reduces the overall scope of the audit engagement):
* Analytics refines audit focus but does not necessarily reduce the scope; it may expand testing capabilities.
* Option D (Increases the auditor's objectivity):
* Objectivity is an ethical requirement rather than a direct effect of data analysis.
* Data analytics enhances internal audit testing by providing deeper insights into high-risk areas.
* IIA Standard 1220 and GTAG 16 emphasize data analytics in risk-based auditing.
Final Justification:IIA References:
* IPPF Standard 1220 - Due Professional Care
* IIA GTAG 16 - Data Analytics in Auditing
* COSO Framework - Data-Driven Risk Management

NEW QUESTION: 12

□□ □ □□□ □□□□(man-in-middle) □□□ □□□ □□ □□□□ □□ □□□ □□?

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

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

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

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

Answer: C (LEAVE A REPLY)

* Understanding a Man-in-the-Middle (MITM) Attack:

* A Man-in-the-Middle (MITM) attack occurs when a cybercriminal intercepts, alters, or steals data while it is being transmitted between two parties.

* The attacker can modify messages, inject malicious content, or eavesdrop on sensitive communications without the knowledge of the sender or receiver.

* How MITM Attacks Work:

* Attackers position themselves between two communicating parties (e.g., a user and a banking website) and intercept the data exchange.

* This allows them to steal login credentials, financial information, or confidential communications.

* Common MITM attack methods include:

* Wi-Fi eavesdropping (public network interception).

* Session hijacking (stealing active user sessions).

* HTTPS spoofing (tricking users into thinking they are on a secure website).

* Why Other Options Are Incorrect:

* A. The perpetrator is able to delete data on the network without physical access to the device

- Incorrect.

* This describes a remote cyberattack, such as malware or ransomware, rather than MITM, which focuses on data interception.

* B. The perpetrator is able to exploit network activities for unapproved purposes - Incorrect.

* This is too broad and could refer to insider threats, malware, or privilege escalation attacks, rather than specifically MITM.

* D. The perpetrator is able to disable default security controls and introduce additional vulnerabilities - Incorrect.

* This describes a system exploitation attack, such as a rootkit or backdoor installation, not an MITM attack.

* IIA's Perspective on Cybersecurity and IT Risk Management:

* IIA Standard 2110 - Governance requires organizations to implement cybersecurity controls to mitigate risks like MITM attacks.

* IIA GTAG (Global Technology Audit Guide) on Cybersecurity Risks advises organizations to use encryption (e.g., TLS, VPNs) to protect data in transit.

* NIST Cybersecurity Framework recommends multi-factor authentication (MFA) and secure protocols to prevent MITM attacks.
IIA References:
* IIA Standard 2110 - IT Security and Cyber Risk Governance
* IIA GTAG - Cybersecurity Controls and Threat Mitigation
* NIST Cybersecurity Framework - Secure Data Transmission
Thus, the correct and verified answer is C. The perpetrator is able to take over control of data communication in transit and replace traffic.

NEW QUESTION: 13
□□□ □□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□□. □□ □□ □ □ □□□ □□ □ □□□ □ □□ □□ □□□□□?
A. □□□ □□□□ □□□□ □□□□.
B. □□□ □□ □□□□□ □□□□□□.
C. □□□□ □□ □□□ □□□□ □□□□.
D. □□□ □□□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
A declining inventory turnover means that inventory is sitting longer before being sold, while an increasing gross margin rate suggests the company is making higher profits on each sale. This combination is often a sign of inventory overstatement, possibly due to accounting errors or fraud.
* Correct Answer (D - The Organization's Inventory is Overstated)
* Inventory turnover ratio = Cost of Goods Sold (COGS) / Average Inventory. A declining inventory turnover indicates higher inventory levels relative to sales.
* Gross margin rate = (Revenue - COGS) / Revenue. An increasing gross margin means either higher selling prices or lower COGS.
* Overstating inventory artificially reduces COGS, making gross margin appear higher.
* The IIA's GTAG 8: Audit of Inventory Management explains that inflated inventory levels can distort financial reporting and lead to misinterpretations of business performance.
* Why Other Options Are Incorrect:
* Option A (Operating expenses are increasing):
* An increase in operating expenses would not directly explain declining inventory turnover or increasing gross margin.
* Gross margin focuses on revenue and COGS, not operating expenses.
* Option B (Just-in-Time Inventory):
* A just-in-time (JIT) system reduces inventory levels, leading to higher inventory turnover, which contradicts the scenario.
* Option C (Inventory Theft):
* If theft were occurring, inventory levels would decrease, leading to higher turnover, not declining turnover.

* GTAG 8: Audit of Inventory Management - Discusses inventory valuation risks, including overstatement and its impact on financial ratios.
* IIA Practice Guide: Assessing Inventory Risks - Covers fraud risks related to inventory manipulation.
Step-by-Step Explanation:IIA References for Validation:Thus, the best explanation for a declining inventory turnover with an increasing gross margin rate is inventory overstatement (D).

NEW QUESTION: 14
□□ □ □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□
B. □□□ □□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□
C. □□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□
D. □□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□
Answer: D (LEAVE A REPLY)
Meaningful recommendations are those that address the root cause of the condition by comparing it to the established criteria and propose sustainable, long-term solutions. This ensures that the identified issue will not recur and strengthens the control environment. Option A relates to symptoms (condition vs. consequence), not root causes. Option B identifies the correct gap (criteria vs. condition) but offers only short-term fixes. Option C incorrectly compares criteria to consequence, which is not a valid basis for audit recommendations.
Thus, Option D is correct.
Reference:
IIA Practice Guide - Audit Findings: Condition, Criteria, Cause, Effect, and Recommendation.

NEW QUESTION: 15
□□ □ □□□ □□□ □□ □□□ □□ 40%□ □□□ □ □□□ □□□□ □□ □□ □□ □ □□□□□?
A. □□ □□
B. □□□
C. □□ □□
D. □□□□□
Answer: B (LEAVE A REPLY)
The equity method is used when an investor owns between 20% and 50% of another company's stock, indicating significant influence over the investee. Since the investor organization is purchasing 40% of the stock, it qualifies for this method.
* (A) Cost method.
* Incorrect: The cost method is used when the investor has less than 20% ownership and no significant influence.

* (B) Equity method. (Correct Answer)
* The equity method is required when the investor has significant influence over the investee (typically between 20% and 50% ownership).
* Under this method, the investor records a proportional share of the investee's profits and losses in its financial statements.
* IIA Standard 2330 - Documenting Information recommends accurate financial reporting and appropriate accounting method selection.
* (C) Consolidation method.
* Incorrect: The consolidation method is used when the investor owns more than 50% of the stock, granting control over the investee.
* (D) Fair value method.
* Incorrect: The fair value method applies when investments are traded in active markets and do not grant significant influence.
* IIA Standard 2330 - Documenting Information: Requires appropriate classification of financial investments.
* GAAP & IFRS Accounting Standards: Mandate the equity method for ownership between 20% and 50% with significant influence.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (B) Equity method, as 40% ownership implies significant influence, requiring the use of this method.

NEW QUESTION: 16
□□ □ □□□ □□□ □□ □□□□ □□ □□ □□?
A. □□□ □□□ □□ □□□□□ □□□□□ □□□.
B. □□□ □□ □□□□ □ □□□ □□□ □□□ □□□ □□□□ □□□.
C. □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□.
D. □□□□ □□ □□□□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□.
Answer: (SHOW ANSWER)
A tape rotation schedule defines how often backup tapes are overwritten or archived, directly impacting data retention periods. This is essential for compliance, disaster recovery, and internal controls over data storage.
* Correct Answer (C - The Tape Rotation Schedule Affects How Long Data is Retained)
* Organizations use backup rotation schemes such as Grandfather-Father-Son (GFS), Tower of Hanoi, or FIFO (First-In-First-Out) to determine how long backups are kept before being overwritten.
* This impacts data retention policies, regulatory compliance, and recovery capabilities.
* The IIA's GTAG 10: Business Continuity Management discusses backup strategies and retention management.
* Why Other Options Are Incorrect:
* Option A (System backups should always be performed real-time):
* Real-time backups (continuous data protection) are useful but not always required.

Many businesses use scheduled backups instead.
* Option B (Backups should be stored in a secured location onsite for easy access):
* Best practice recommends offsite or cloud storage to protect against disasters like fire or cyberattacks.
* Option D (Backup media should be restored only in case of hardware or software failure):
* Backups may also be restored for audit purposes, compliance checks, or business continuity testing.
* GTAG 10: Business Continuity Management - Covers backup strategies, data retention, and disaster recovery.
* IIA Practice Guide: IT Controls - Discusses backup policies and risks in data management.
Step-by-Step Explanation:IIA References for Validation:Thus, the tape rotation schedule (C) is correct because it determines how long data is retained.

NEW QUESTION: 17
□□□□□□ □□□□□□□ □□ □□□□□ □□□□ □ □□□ □□ □□□ □□□□□ □.

□□□ □□□ □□□ $8,500□ □□□□□□□. □□ □ □ □□ □□□□ □□ □□□ □ □□□ □□□ □□□□□?
A. □□ □□ □□
B. FIFO(□□ □□) □□
C. □□ □□ □□
D. □□ □□ □□ □□ □□
Answer: B (LEAVE A REPLY)
To determine which inventory method was used, we calculate the cost of goods sold (COGS) under different inventory valuation methods.

* Opening Inventory: 1,000 units @ $2 each = $2,000
* Purchased: 5,000 units @ $3 each = $15,000
* Total Inventory: 6,000 units
* Units Sold: 3,000 at $7 per unit
* Reported COGS: $8,500
Given Data:FIFO Calculation:FIFO (First-In, First-Out) assumes that the oldest inventory is sold first.
* 1,000 units from opening inventory @ $2 = $2,000
* 2,000 units from purchases @ $3 = $6,000
* Total COGS under FIFO: $2,000 + $6,000 = $8,000
Average Cost Calculation:Average cost per unit =
Total Cost of InventoryTotal Units=(2,000+15,000)6,000=17,0006,000=2.83 per unit
\frac{\text{Total Cost of Inventory}}{\text{Total Units}} = \frac{(2,000 + 15,000)}{6,000} = \frac{17,000}{6,000} = 2.83 \text{ per unit}Total UnitsTotal Cost of Inventory=6,000(2,000+15,000)=6,00017,000=2.83 per unit
* COGS using average cost method: 3,000×2.83=8,4903,000 \times 2.83 = 8,4903,000×2.83=8,490 This is not an exact match to the reported COGS of $8,500.
Since the closest method to the reported value is FIFO ($8,000 vs. $8,500 reported COGS, accounting for possible rounding errors or additional costs), FIFO is the most likely method used.
* (A) Average cost method. # Incorrect. The calculated COGS using the weighted average method was
$8,490, which does not match exactly with the reported COGS of $8,500.
* (B) First-in, first-out (FIFO) method. # Correct. The FIFO method yielded $8,000, which is the closest match to the reported COGS. Minor rounding adjustments or other expenses could explain the difference of $500.
* (C) Specific identification method. # Incorrect. This method applies when each inventory item is individually tracked, which is not mentioned in the question.
* (D) Activity-based costing method. # Incorrect. Activity-based costing (ABC) is used for overhead allocation and is not a primary inventory valuation method.
* IIA GTAG - "Auditing Inventory Management"
* IIA Standard 2130 - Control Activities (Inventory and Costing Methods)
* GAAP and IFRS - FIFO, Weighted Average, and Specific Identification Methods Analysis of Answer Choices:IIA References:Thus, the correct answer is B (FIFO method) because it provides the closest cost match to the reported COGS.

NEW QUESTION: 18
□□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□. □□□□ □□□□ □□□ □□□□□□. □□ □□ □□ □□□□ □□ □ □□□□ □□□ □□ □□□ □□ □□□ □□□□. □□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□ □□ □□□. □□□□ □□□ □ □□ □□□ □□□ □□□□□?

A. □□ □□ □□□ □□□□ □□ □□ □ □□ □□□□ □□□□□.
B. □□ □□ □□ □□□ □ □□ □□□□□ □□□ □□□□ □□□.
C. □□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□.
D. □□□ □□□ □□ □□□□□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
In advisory engagements, internal audit may provide consulting support that enhances processes while maintaining objectivity. In this case, the most appropriate value-adding activity is to facilitate development of a checklist for documenting asset transfers. This addresses the identified gap directly and supports management in strengthening controls. Option A identifies risks but does not resolve the gap. Option C (root cause analysis) is not as practical in this advisory setting. Option D (resource allocation) is a management responsibility, not internal audit's role.
Reference:
IIA Implementation Guidance - Advisory Services; Standard 2120: Risk Management.

NEW QUESTION: 19
□□ □ □□□ □□□ □□ □□□ □□□□ □□□?
A. □□□ □□□□□.
B. □□□ □□□□.
C. □□□□ □□□□.
D. □□□ □□□□□.
Answer: C (LEAVE A REPLY)
When a company invests in common stock, it can earn income in two primary ways:
* Dividend income: When the company receives dividends, it recognizes the income.
* Capital gains: When the stock is sold for a higher price than its purchase price, it results in a gain.
* Why Option C (Receives dividends) is Correct:
* Dividends represent income from an investment in common stock when declared and paid by the issuing company.
* Under GAAP and IFRS, dividend income is recognized when received, not when declared.
* Companies record dividends as investment income in their income statement.
* Why Other Options Are Incorrect:
* Option A (Purchases bonds):
* Incorrect because purchasing bonds is an investment transaction, not income recognition.
* Option B (Receives interest):
* Incorrect because interest income applies to bond investments, loans, or deposits, not common stock investments.
* Option D (Sells bonds):
* Incorrect because selling bonds results in capital gains or losses, not regular investment income from common stock.

* IIA Practice Guide - "Auditing Investment & Treasury Activities": Discusses the recognition of investment income.
* IFRS 9 (Financial Instruments) & GAAP Standards: Provide guidance on recording dividends as investment income.
* COSO Internal Control - Integrated Framework: Emphasizes proper financial reporting and income recognition.
IIA References:

NEW QUESTION: 20
□□ □ □□□ □□□ □□ □□□□□?
A. □□ □□ □ □□ □□ □□
B. □□□ □□ □□□ □□□□ □□ □□□ □□
C. □□□ □□ □□ □ □□ □□ □□ □□
D. □□□ □□ □□□□ □□ □□ □□□ □□ □□
Answer: (SHOW ANSWER)
A physical control is a security measure designed to protect assets, facilities, and personnel from physical threats such as fire, theft, or unauthorized access. Fire detection and suppression equipment (e.g., fire alarms, sprinklers, extinguishers) directly protects physical assets, making it a clear example of a physical control.
* (A) Providing fire detection and suppression equipment. #
* Correct. This is a direct physical security control that helps mitigate fire risks by detecting and suppressing fires.
* IIA GTAG "Physical Security and IT Asset Protection" identifies fire detection as an essential physical security measure.
* (B) Establishing a physical security policy and promoting it throughout the organization. #
* Incorrect. A policy is an administrative control, not a physical control. While important, it does not provide direct physical protection.
* (C) Performing business continuity and disaster recovery planning. #
* Incorrect. This is a procedural control, not a physical one. Planning for disasters does not physically secure assets but instead prepares an organization for recovery.
* (D) Keeping an offsite backup of the organization's critical data. #
* Incorrect. This is an IT security control, ensuring data availability rather than physically protecting assets.
* IIA GTAG - "Physical Security and IT Asset Protection"
* IIA Standard 2110 - Governance (Risk Management Controls)
* COBIT Framework - Physical and Environmental Security Controls
Analysis of Answer Choices:IIA References:Thus, the correct answer is A, as fire detection and suppression equipment provides direct physical protection against fire-related risks.

NEW QUESTION: 21
□□ □□□ □□ □ □□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□?

A. □□□, □□, □□□.
B. □□□, □□□ □ □□□.
C. □□□, □□□ □ □□□.
D. □□ □□, □□□ □□, □□□ □□.
Answer: B (LEAVE A REPLY)
Cybersecurity controls are primarily designed to protect the Confidentiality, Integrity, and Availability (CIA) of data. These are the three fundamental principles of cybersecurity and are essential for protecting organizational information assets. Let's analyze each option:
* Option A: Veracity, velocity, and variety.
* Incorrect. These attributes are commonly associated with big data and data analytics rather than cybersecurity. Cybersecurity controls focus on ensuring that data is secure, rather than on its volume, speed, or diversity.
* IIA Reference: Cybersecurity risk management frameworks emphasize the CIA triad over big data attributes. (IIA GTAG: Auditing Cybersecurity Risk)
* Option B: Integrity, availability, and confidentiality.
* Correct. These three principles are at the core of cybersecurity:
* Confidentiality: Ensures that sensitive information is only accessible to authorized individuals.
* Integrity: Protects data from unauthorized modifications or corruption.
* Availability: Ensures that data and systems are accessible when needed.
* IIA Reference: The IIA's guidance on IT governance highlights the CIA triad as the foundation of cybersecurity. (IIA GTAG: Information Security Governance)
* Option C: Accessibility, accuracy, and effectiveness.
* Incorrect. While these attributes are important in data management and usability, they do not directly define cybersecurity controls.
* Option D: Authorization, logical access, and physical access.
* Incorrect. While these are essential security components, they fall under broader IT security measures rather than forming the fundamental principles of cybersecurity.

NEW QUESTION: 22
□□□ □□ □□ □□□(CAE)□ □□ □□□ □□□□□ □□ □ □□ □□ □ □□ □□ □□□□□?
A. CAE□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
B. CAE□ □□ □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
C. CAE□ □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
D. CAE□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
When prioritizing the audit universe, the CAE typically uses a risk-factor approach. This includes a combination of likelihood, impact, control effectiveness, and other relevant criteria. Solely relying on impact (Option C) or likelihood (Option B) is insufficient. Heat

maps (Option D) may be tools used within the process, but they are not the actual method of prioritization.
Thus, the correct description is the risk-factor approach (Option A).
Reference:
IIA Practice Guide - Developing a Risk-based Internal Audit Plan.

NEW QUESTION: 23
□□□□ □□ □□ □□□ □□□ □□□ □ □□□□ □□ □□ □□ □□□ □□□ □□ □□ □□ □□□□□?
A. □□□ □□ □□□ □□□
B. □□ □□ □□□ □□□ □□
C. □□ □□ □□ □□□
D. □□ □□ □□ □ □□□
Answer: C (LEAVE A REPLY)
The IIA requires internal audit functions to have an external quality assessment at least once every five years.
External quality assurance feedback provides the most independent, objective, and reliable assurance to the board regarding whether the internal audit function conforms with standards and is positioned to achieve its objectives.
Option A measures productivity but not quality. Option B provides useful insights but is subjective. Option D indicates staffing health but does not directly assess ability to meet objectives.
Reference:
IIA Standards - Standard 1312: External Assessments.

NEW QUESTION: 24
□□ □ □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□□□?
A. □□□ □□□ □□□□□ □□ □□□□ □□□□□.
B. □□ □□□□ □□□ □□□□ □□□ □□□□□.
C. □□□ □□□ □□ □□□□ □□ □□□□ □□□□□.
D. □□ □□□□ □□□□□ □□□□ □□□ □□□□□.A
Answer: A (LEAVE A REPLY)
Transfer pricing regulations aim to prevent tax evasion and ensure that intercompany transactions reflect fair market value, preventing profit shifting to low-tax jurisdictions.
Selling inventory at fair value (arm's length price) aligns with regulatory requirements, reducing the risk of non-compliance.
* (A) Correct - The organization sells inventory to an overseas subsidiary at fair value.
* Ensuring that transactions reflect fair market value prevents regulatory violations.
* Adhering to the arm's length principle minimizes transfer pricing risks and potential tax penalties.
* (B) Incorrect - The local subsidiary purchases inventory at a discounted price.

* A discounted price could be seen as an attempt to shift profits between entities, increasing regulatory scrutiny.
* (C) Incorrect - The organization sells inventory to an overseas subsidiary at the original cost.
* Selling at the original cost does not account for market conditions, potential markup, and fair valuation.
* Regulators may view this as non-compliance with the arm's length principle.
* (D) Incorrect - The local subsidiary purchases inventory at the depreciated cost.
* Depreciated cost may not represent fair market value and could be interpreted as a tax avoidance mechanism.
* IIA's Global Internal Audit Standards - Compliance with Tax and Transfer Pricing Regulations
* Emphasizes fair pricing in intercompany transactions to prevent regulatory violations.
* OECD Transfer Pricing Guidelines
* Reinforces the arm's length principle as the standard for pricing related-party transactions.
* COSO's ERM Framework - Compliance Risk Management
* Highlights the need for adherence to tax laws and fair-value pricing in financial transactions.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 25
□□□□□ □□□ □□ □□ □□ □ □□ □□?
A. □□□□□ □□□□□□ □□□□ □□□ □□□□□.
B. □□□□□□ □□□□ □□□□ □□ □□□ □□□ □□□□.
C. □□□□□ □□□□ □□□ □ □□□□□□ □□□□□.
D. □□1 □□, □□ □□□ □□□□ □□ □□□ □□□□ □ □□ □□ □□□ □□□ □ □□□.
Answer: (SHOW ANSWER)
Cost-Volume-Profit (CVP) analysis is used to determine how changes in costs and volume affect a company's operating profit.
* Correct Answer (C - Breakeven Occurs When the Contribution Margin Covers Fixed Costs)
* Contribution Margin (CM) = Sales Revenue - Variable Costs.
* The breakeven point is where total contribution margin equals total fixed costs, meaning the company has no profit or loss.
* The IIA's Practice Guide: Auditing Financial Performance supports this as the key breakeven definition.
* Why Other Options Are Incorrect:
* Option A (Contribution margin is the amount remaining after fixed expenses are deducted):
* Incorrect because CM is calculated before fixed expenses are subtracted.

* Option B (Breakeven point is the amount of units sold to cover variable costs):
* Incorrect because breakeven covers fixed costs as well, not just variable costs.
* Option D (Following breakeven, operating income increases by the excess of fixed costs less variable costs per unit sold):
* Incorrect because operating income increases by the contribution margin per unit, not by the difference between fixed and variable costs.
* IIA Practice Guide: Auditing Financial Performance - Defines breakeven analysis as when contribution margin covers fixed costs.
* IIA GTAG 13: Business Performance - Discusses cost-volume-profit analysis for financial decision- making.
IIA References for Validation:Thus, C is the correct answer because breakeven occurs when the contribution margin equals fixed costs.

NEW QUESTION: 26
□□ □□ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□ □ □□□ □□□ □□□ □□?
A. □□□□□ □□ □□□ □□□□□.
B. □□ □□ □□□ □□□□□
C. □□□□□ □□□□ □□ □□□□ □ □□□ □□□ □□□□□.
D. □□□□□ □□ 0□□ □□□□□.
Answer: C (LEAVE A REPLY)
The discounted payback period (DPP) is a capital budgeting technique that determines how long it takes for a project's discounted cash flows to recover its initial investment. Unlike the regular payback period, the DPP accounts for the time value of money by discounting future cash flows.
* (A) It calculates the overall value of a project.
* Incorrect. The discounted payback period only measures how long it takes to recover the initial investment-it does not determine the overall value of a project. Net Present Value (NPV) and Internal Rate of Return (IRR) are used to evaluate a project's overall value.
* (B) It ignores the time value of money.
* Incorrect. Unlike the regular payback period, the discounted payback period accounts for the time value of money by discounting future cash flows using a required rate of return.
* (C) It calculates the time a project takes to break even. #
* Correct. The discounted payback period determines how long it takes for the present value of cash inflows to recover the initial investment. It helps assess the risk and liquidity of a project.
* IIA GTAG "Auditing Capital Budgeting and Investment Decisions" states that discounted payback is useful for assessing the risk of projects by considering cash flow recovery time.
* (D) It begins at time zero for the project.
* Incorrect. The calculation starts at time zero (when the investment is made), but the method itself focuses on future discounted cash flows to determine the break-even point.

* IIA GTAG - "Auditing Capital Budgeting and Investment Decisions"
* COSO ERM Framework - Capital Investment Risk Management
* GAAP/IFRS - Discounted Cash Flow Methods
Analysis of Answer Choices:IIA References:Thus, the correct answer is C, as the discounted payback period measures the time needed to break even after adjusting for the time value of money.

NEW QUESTION: 27
□□□ □□□□ □□ □□□□, □□ □□□□□ □□ □ □□ □□□ □□□ □□□. □□ □□ □ □□□□ □□□ □□ □ □□□□ □□□ □□□□□?
A. □□□□ □□□□□ □ □□□ □□□□ □□□ □□.
B. □□□ □□□□ □□□ □□.
C. □□□ □□□□ □□ □□.
D. □□□ □□□□ □□ □□□ □□□□ □.
Answer: C (LEAVE A REPLY)
* Understanding Competitive Business Strategies:
* The board of directors' focus is on industry leadership and outperforming competitors.
* A strong research and development (R&D) strategy drives innovation, allowing the organization to introduce new and differentiated products that enhance competitive advantage
.
* Why Option C (Investment in R&D) Is Correct?
* R&D drives product innovation, helping the organization stay ahead of competitors.
* Investing in new technologies and unique product features differentiates the company and strengthens market leadership.
* IIA Standard 2120 - Risk Management supports evaluating strategic investments that enhance business growth and competitive positioning.
* Why Other Options Are Incorrect?
* Option A (Divesting unprofitable product lines):
* While divestment improves financial health, it does not directly contribute to market leadership.
* Option B (Increasing diversity of business units):
* Expanding into new business areas spreads risk but may not provide a focused competitive advantage in the primary industry.
* Option D (Relocating manufacturing to another country):
* Lowering costs improves efficiency, but it does not directly position the company as an industry leader.
* Investing in R&D aligns best with the board's goal of industry leadership and competitive advantage.
* IIA Standard 2120 supports strategic risk management and innovation investment.
Final Justification:IIA References:

* IPPF Standard 2120 - Risk Management (Strategic Investment & Competitive Advantage)
* COSO ERM - Business Growth & Innovation Risk Management
* Porter's Competitive Strategy Model - R&D as a Market Differentiator

NEW QUESTION: 28
□□ □□□□ □□ □□□ □□ □ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□□. □□ □□□□ □□ □□ □□□□ □□□ □□□ □□ □□ □ □□□ □□□ □□□□□. □□ □ □□ □□□ □□□ □□, □□□ □□□ □□□ □□□ □ □□□□. □□ □□ □□□(CEO)□ □□ □□□ □□□ □□ □□□?
A. CEO □ □□ □□ □□□□ □ □□□ □□□□□.
B. □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□□□.
C. □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□.
D. □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
The CAE must communicate significant risk exposures and control issues to the board. A regulatory noncompliance issue that could result in significant fines qualifies as a high residual risk. Internal audit should not implement corrective actions (management's responsibility) or recommend disciplinary action. While discussions with management (Option A) are appropriate, the ultimate duty is to escalate the matter to the board (Option C).
Reference:
IIA Standards - Standard 2060: Reporting to Senior Management and the Board.

NEW QUESTION: 29
□□ □□□□ □□□□□ □□ □□ □□□□ □□□ □□□□ □□□□. □□ □□□□ □ □□ □□□□□?
A. □□□□□□□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
B. □□ □□□ □□□□□ □□ □□□ □□□□□ □□□□□.
C. □□□□□□□ □□□ □□□ □□ □□ □□□□ □□□□□ □□□□□.
D. □□ □□□□□ □ □□□□ □□ □□□ □□□ □□ □□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
Integration testing is a phase in the software development lifecycle (SDLC) where individual components or systems are combined and tested as a group to ensure they work together correctly.
* Ensures Component Compatibility - Confirms that different software modules and hardware components function correctly when integrated.
* Identifies Data Flow Issues - Ensures seamless communication between software systems, databases, and external applications.
* Detects System-Wide Errors - Finds defects that unit testing (individual module testing) may miss.

* Prepares for System Testing - Integration testing is conducted before full system testing to ensure subsystems work together as expected.
* A. To verify that the application meets stated user requirements.
* This refers to User Acceptance Testing (UAT), not integration testing.
* B. To verify that standalone programs match code specifications.
* This describes unit testing, where individual components are tested separately.
* C. To verify that the application would work appropriately for the intended number of users.
* This describes performance or load testing, which measures system behavior under high user load.
* IIA's GTAG on IT Risks and Controls - Emphasizes the role of integration testing in ensuring secure and functional IT environments.
* COBIT 2019 (Governance and Management of IT) - Recommends integration testing to reduce IT system failures.
* ISO/IEC 25010 (Software Quality Model) - Lists integration testing as a key quality assurance step.
Why Option D is Correct?Why Not the Other Options?IIA References:

NEW QUESTION: 30
□□□□□ □□ □□ □□□ □□ □□ □□ □ □□ □□?
A. □ □□□□ □□ □□□ □□□□ □□□□□ □□□.
B. □□□□□ □□□□□□ □□□□ □□□ □□□ □□□□□.
C. □□□□ □□□ □□□□□ □□ □□□□ □□□□ □□□□□.
D. □□□ □□□ □□□□ □□□ □□□□□ □□.
Answer: (SHOW ANSWER)
A partnership is a business structure where two or more individuals share ownership, responsibilities, and profits or losses. The accounting treatment of a partnership follows GAAP (Generally Accepted Accounting Principles) and IFRS (International Financial Reporting Standards).
Let's analyze each option:
* A. The initial investment of each partner should be recorded at book value.
* Incorrect. The initial investment is recorded at fair market value (FMV) at the time of contribution, not at book value. This ensures that all assets contributed by partners reflect their current worth.
* B. The ownership ratio identifies the basis for dividing net income and net loss. # (Correct Answer)
* Correct. A partnership agreement typically specifies profit and loss-sharing ratios based on ownership percentages. If no agreement exists, profits and losses are divided equally among partners.
* Example: If Partner A owns 60% and Partner B owns 40%, they will split net income or loss in this ratio.

* C. A partner's capital only changes due to net income or net loss.
* Incorrect. A partner's capital account changes due to additional investments, withdrawals, revaluations of assets, and profit/loss allocations.
* D. The basis for sharing net income or net losses must be fixed.
* Incorrect. Partners can change the allocation method over time through a revised partnership agreement. It is not required to remain fixed.
* IIA Practice Guide - Assessing Financial Statement Risk - Covers partnership accounting risks.
* GAAP & IFRS - Partnership Accounting Standards - Explain the treatment of capital accounts and income distribution.
* COSO Internal Control Framework - Financial Reporting Risk - Discusses financial treatment of equity structures.
* IIA Standard 2120 - Risk Management - Highlights financial statement risks, including partnerships.
IIA References:

NEW QUESTION: 31
□□ □ □□□ □□ □□□□□□(UDA) □ □□ IT □□□□□□□ □□ □□□□ □□ □ □ □□?
A. UDA □ □□ JT □□□□□□□ □□□□□ □□□ □□ □□ □□□ □□□□.
B. UDA□ □□□□□ □□□ □□□□ □□ □□□ □□□ □□□□ IT □□ □□□□□□ □ □□□□□ □□□ □□□ □□□□ □□□□.
C. □□ IT □□□□□□□ □□□□. UDA□ □□□□□ □□□□ □□ □□□□ □□ □□ □□□.
D. IT □□□ □□□□ □□□□□ □ □□ □□□ □□□□□□□ □□□ □□□□□□ □ □□ □□□□□.
Answer: C (LEAVE A REPLY)
User-Developed Applications (UDAs) are software tools, typically spreadsheets or small databases, created by business users rather than IT professionals. These applications often lack formal security, documentation, and control measures, increasing the risk of data errors, unauthorized access, and compliance failures.
* UDAs are often created quickly to meet immediate business needs, without following IT governance, security controls, or development standards.
* Unlike traditional IT applications, UDAs lack structured testing, change management, and formal documentation.
* The IIA's GTAG 14 - Auditing User-Developed Applications states that UDAs present higher risks because they are not subject to the same controls as IT-managed applications.
* A. UDAs and traditional IT applications typically follow a similar development life cycle # Incorrect. Traditional IT applications follow a formal Software Development Life Cycle (SDLC), whereas UDAs are developed informally by end-users.

* B. A UDA usually includes system documentation to illustrate its functions, and IT-developed applications typically do not require such documentation. # Incorrect. IT applications require extensive documentation, whereas UDAs often lack documentation entirely.
* D. IT testing personnel usually review both types of applications thoroughly to ensure they were developed properly. # Incorrect. IT applications undergo rigorous testing and quality assurance, while UDAs often bypass IT reviews altogether.
* IIA GTAG 14 - Auditing User-Developed Applications highlights the risks of UDAs and emphasizes the need for internal controls.
* COBIT Framework (Control Objectives for Information and Related Technologies) recommends IT governance measures for all business-critical applications.
* ISO 27001 (Information Security Management System) warns against uncontrolled user-developed applications due to security risks.
Why Option C is Correct?Explanation of the Other Options:IIA References & Best Practices:Thus, the correct answer is C. Unlike traditional IT applications, UDAs typically are developed with little consideration of controls.

NEW QUESTION: 32
Maslow□ □□ □□ □□□ □□□, □□ □□□ □□□ □□ □□□ □□ □□ □ □□ □□ □ □□ □ □□□ □□□ □□ □□□□□?
A. □□□ □□.
B. □□.
C. □□ □□.
D. □□
Answer: D (LEAVE A REPLY)
According to Maslow's hierarchy of needs, once an individual's lower-level needs (physiological, safety, and social needs) are met, they seek higher-level motivators such as esteem and self-actualization.
Recognition falls under esteem needs, which include respect, status, and appreciation. Employees who feel valued and recognized are more likely to stay with an organization.
* A. Social benefits - These are lower-level needs (belongingness/social needs), which have already been met in this scenario.

* B. Compensation - While salary is important, it primarily addresses physiological and security needs, which are lower on Maslow's hierarchy. Once these are met, higher-level motivators like recognition become more influential.
* C. Job safety - Safety and security are lower-level needs, and in this scenario, they are already met.
* D. Recognition (Correct Answer) - Falls under esteem needs, which are crucial for employee retention once basic needs are satisfied.
* IIA IPPF Standard 2120 - Risk Management includes talent management as part of organizational sustainability.
* COSO ERM Framework - Human Capital Risk highlights employee motivation as a key factor in risk management.
* IIA GTAG 7 - Managing IT Security Risks discusses employee satisfaction and its impact on organizational security and retention.
Explanation of Each Option:IIA References:

NEW QUESTION: 33
□□□ □□□□ □□□□□ □□□□ □□□□□ □□ 58□□ □□□□. □□□□ □□□ □□ □□□ 42□□ □□□□□. □□□ □□□ □□□ □□□□ □ □□ 10□□ □□□□ □ □□ □□ □□□ □□□□□?
A. 26□.
B. 90□.
C. 100□.
D. 110□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
The cash conversion cycle (CCC) is calculated as:
CCC=Days Inventory Outstanding+Days Sales Outstanding#Days Payables Outstanding \text{CCC} = \text
{Days Inventory Outstanding} + \text{Days Sales Outstanding} - \text{Days Payables Outstanding} CCC=Days Inventory Outstanding+Days Sales Outstanding#Days Payables Outstanding CCC=58+42#10=90 daysCCC = 58 + 42 - 10 = 90
\text{ days}CCC=58+42#10=90 days Option A (26 days) - Incorrect, as it does not account for total cycle components.
Option C (100 days) & Option D (110 days) - Overestimate the cycle by not correctly adjusting for payables.
Thus, Option B (90 days) is the correct answer.
Reference: IIA Financial Management - Working Capital & Cash Flow Analysis

NEW QUESTION: 34
□□ □□□□ □ □□ □□ □□□□□□□ □□ □□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□?

A. □□□□□□ □□ □□□ □□□ □□□□ □□□ □□□□□□□.
B. □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□□ □□ □ □□□.
C. □□ □□□□□ □□□□ □□□□ □□ □□□ □□ □□□ □□□□□□.
D. □□ □□ □□□□□□□ □□ □□□ □□ □□ □□ □□ □□□□ □□□□ □□□ □□□□.
Answer: (SHOW ANSWER)
The most recent backup is primarily used to restore lost data in the event of a system failure, data corruption, or cyberattack. If a data center failure occurs, the latest backup is the best source to recover the human resources database and resume operations.
* (A) Incorrect - An incorrect program fix was implemented just prior to the database backup.
* If an incorrect fix was applied before the backup, restoring the latest backup would still contain the error.
* The organization would need to restore an earlier version before the faulty update.
* (B) Incorrect - The organization is preparing to train all employees on the new self-service benefits system.
* The latest backup is not needed for training; the live system or historical data would be used instead.
* (C) Correct - There was a data center failure that requires restoring the system at the backup site.
* In the event of a system failure, restoring from the most recent backup minimizes data loss and downtime.
* This is the primary reason for maintaining regular backups.
* (D) Incorrect - There is a need to access prior year-end training reports for all employees in the human resources database.
* Historical records would likely be stored in archived backups or reports, not the latest backup.
* The most recent backup contains current data, not old reports.
* IIA's GTAG (Global Technology Audit Guide) - IT Disaster Recovery and Backup Strategies
* Covers the importance of backups in system restoration.
* NIST Cybersecurity Framework - Data Recovery and Business Continuity
* Recommends frequent backups to protect against system failures.
* ISO 22301 - Business Continuity Management
* Defines recovery procedures and best practices for backup site restoration.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 35
□□□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□?
A. □□ □□ □□□ □□□ □□□□ □□□□□□.

B. □□□ □□□ □□ □ □ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□.
D. □□ □□□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
Reference: IIA Business Knowledge for Internal Auditing, Data Analytics in Auditing section.

NEW QUESTION: 36
□□□□ □□ □□□□□ □□□ □□□□□ □□ □□ □ □□ □□□□ □□□ □□□□ □□□?
A. □□□□□.
B. □□□ □□□(LAN).
C. □□□□.
D. □□□.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
An intranet is a private network used by an organization for internal communication and information sharing among employees. It is accessible only to authorized personnel within the company.
Option A (Extranet) - Allows external parties (e.g., suppliers, partners) to access limited information.
Option B (LAN) - Refers to a network infrastructure rather than controlled access.
Option D (Internet) - Is public and not restricted to internal personnel.
Thus, Option C (Intranet) is the correct answer as it ensures access only to organizational personnel.
Reference: IIA IT Security - Network Access Controls

NEW QUESTION: 37
□□ □ □□ □□□ □□□□ □ □□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□ □□□ □□□□□.
B. □□□ □□□ □□.
C. □□□□ □□ □□□□ □□□ □□□□□.
D. □□□ □□ □□□ □ □□ □□□ □□ □□□□ □□□ □□
Answer: D (LEAVE A REPLY)
Earnings management occurs when companies manipulate financial reporting to meet targets, often leading to unethical practices or financial misstatements. The best way to disincentivize earnings management is to link performance to nonfinancial measures such as customer satisfaction and employee training, which cannot be directly manipulated through financial reporting.
* Avoiding Short-Term Financial Manipulation:

* When performance is tied to financial metrics (e.g., return on investment, stock price, or production quotas), there is a higher risk of earnings manipulation, such as shifting revenues, deferring expenses, or aggressive accounting practices.
* Nonfinancial measures, however, emphasize long-term value creation and are harder to manipulate.
* Sustainable Business Growth:
* Customer satisfaction and employee training foster long-term profitability by improving product quality, brand reputation, and workforce capabilities.
* Companies focusing on these measures build sustainable competitive advantages without distorting financial results.
* Regulatory and Ethical Considerations:
* Internal auditors, following IIA Standard 2120 (Risk Management), must evaluate risks related to unethical financial reporting.
* Regulatory bodies (e.g., SEC, PCAOB, and COSO) emphasize reducing the risk of fraudulent financial reporting by incorporating broader performance measures beyond financial results.
* A. Linking performance to profitability measures such as return on investment:
* ROI and similar metrics can pressure executives to inflate earnings or cut necessary expenses to meet short-term targets.
* B. Linking performance to the stock price:
* Stock-based incentives can lead to earnings manipulation (e.g., stock buybacks, revenue recognition adjustments) to inflate stock prices artificially.
* C. Linking performance to quotas such as units produced:
* Production-based targets can result in overproduction or quality compromises, leading to inefficient resource allocation and long-term financial issues.
* IIA Standard 2120 (Risk Management): Internal auditors must assess risks related to financial reporting integrity.
* COSO's Internal Control Framework: Emphasizes performance measures beyond financial results to ensure ethical management practices.
* IIA Practice Guide: Assessing Organizational Governance: Encourages balanced scorecards, including nonfinancial KPIs, to reduce financial misstatement risks.
Step-by-Step Justification:Why Not the Other Options?IIA References:Thus, the correct answer is D. Linking performance to nonfinancial measures such as customer satisfaction and employee training. #

NEW QUESTION: 38
□□□ □□□□□□ □□□ □□□ □ □□□ □□□ □□□ □□□□ □□□□ □ □□ □ □□□□□□ □□ □□ □□ □□□ □□ □□□□□.
□□ □ □□□□ □□□ □□□□ □□ □ □□ □□□ □□□□□?
A. □□□ □□□□
B. □□□□□ □□

C. □□□□ □□□ □□.
D. □□□ □□□ □□
Answer: D (LEAVE A REPLY)
The situation describes a scenario where a customer's personal information was shared with third parties without explicit consent, leading to unsolicited offers. This indicates a control weakness in data privacy and confidentiality, specifically the undue disclosure of information to external parties.
* (A) Incorrect - Excessive collecting of information.
* While collecting too much personal data can be a privacy concern, the issue here is not about data collection but how the data was shared.
* (B) Incorrect - Application of social engineering.
* Social engineering refers to deceptive tactics used to manipulate individuals into disclosing confidential information, which is not the case here.
* (C) Incorrect - Retention of incomplete information.
* The issue is not about missing or incomplete data but rather unauthorized sharing of data.
* (D) Correct - Undue disclosure of information.
* The retailer improperly shared the customer's personal data with other businesses, leading to unsolicited offers.
* This represents a failure to comply with data privacy regulations (e.g., GDPR, CCPA).
* IIA's GTAG (Global Technology Audit Guide) - Data Privacy Risks and Controls
* Highlights the risks associated with unauthorized data sharing.
* NIST Cybersecurity Framework - Data Protection and Privacy
* Emphasizes the importance of controlling access to customer information.
* COSO's ERM Framework - Information Governance and Compliance
* Discusses the importance of data protection policies to prevent undue disclosure Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 39
IIA □□□ □□□ □□ □ □□□□ □□ □ □□□ □□□□ □ □□□□ □□ □□, □□ □ □□□ □□□□ □□□ □□□□□?
A. □□□□ □□□□□.
B. □□□□ □□
C. □□□□ □□□□.
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
Project governance refers to a broad collection of integrated policies, standards, and procedures that provide a framework for planning and executing projects. It establishes decision-making processes, accountability, and risk management controls to ensure that projects align with organizational objectives.
* (A) Project portfolio. #

* Incorrect. A project portfolio refers to a collection of projects managed together to achieve strategic objectives. It does not specifically define the policies, standards, and procedures for project execution.
* (B) Project development. #
* Incorrect. Project development focuses on designing, building, and testing a project, but it does not encompass governance structures like policies, standards, and oversight.
* (C) Project governance. #
* Correct. Project governance includes integrated policies, standards, and procedures that guide project planning, execution, and oversight.
* IIA GTAG "Auditing IT Projects" emphasizes project governance as the primary control framework for managing project risks and ensuring alignment with organizational goals.
* (D) Project management methodologies. #
* Incorrect. Project management methodologies (e.g., Agile, Waterfall, PRINCE2) provide structured approaches for executing projects but do not encompass the full governance framework.
* IIA GTAG - "Auditing IT Projects"
* IIA Standard 2110 - Governance (Project Risk Management)
* COSO ERM Framework - Project Oversight and Risk Governance
Analysis of Answer Choices:IIA References:Thus, the correct answer is C (Project governance), as it provides the integrated policies, standards, and procedures needed for effective project oversight.

NEW QUESTION: 40
□□ □□ □ □□ □□□ □□□ □□ □ □□□ □□?
A. □□□□, □□□□, □□.
B. □□□, □□□□, □□□□.
C. □□ □□, □□ □□, □□ □□□ □□ □□□□.
D. □□□, □□□□□ □□, □□□□□.
Answer: B (LEAVE A REPLY)
Manufacturing costs are classified into three main categories: direct materials, direct labor, and manufacturing overhead. These categories help organizations determine product costs, pricing strategies, and financial reporting.
* Why Option B (Overhead costs, direct labor, direct materials) is Correct:
* Direct materials: Raw materials used directly in production (e.g., wood for furniture).
* Direct labor: Labor costs directly tied to production (e.g., factory workers assembling a product).
* Manufacturing overhead: Indirect costs related to production (e.g., depreciation, factory utilities, maintenance).
* These categories align with GAAP, IFRS, and cost accounting standards.
* Why Other Options Are Incorrect:
* Option A (Direct materials, indirect materials, raw materials):

* "Indirect materials" and "raw materials" are part of manufacturing overhead and direct materials, respectively, but do not form a primary cost classification.
* Option C (Direct materials, direct labor, depreciation on factory buildings):
* Depreciation on factory buildings is an overhead cost, not a separate category.
* Option D (Raw materials, factory employees' wages, production selling expenses):
* Selling expenses are not part of manufacturing costs; they are part of operating expenses.
* IIA Practice Guide - Auditing Cost Management: Defines manufacturing cost classifications.
* IFRS & GAAP Cost Accounting Standards: Outline manufacturing cost components.
* COSO Framework - Cost Control Guidelines: Emphasizes accurate cost allocation in financial reporting.
IIA References:

NEW QUESTION: 41
□□ □ □□□ □□□ □□□ □□ □□□ □□ □□ □□□□□ □□ □□□ □□ □□□ □□ □□□□□?
A. BYOD(Bring Your Own Device) □□□ □□ □□ □□□ □□□□□.
B. □□□ □□□ □□□ □□ □□ □□
C. □□ □□ □□ □□□ □□ □□ □□□□
D. □□ □□□ □□□ □□□ □□□
Answer: C (LEAVE A REPLY)
In an assurance engagement involving smart devices, the first step is to obtain a comprehensive inventory of all devices in use. This ensures that the audit covers all relevant assets and allows the internal auditor to assess risks, controls, and policies effectively.
* (A) Incorrect - Train all employees on bring-your-own-device (BYOD) policies.
* While employee training is important, it is a control measure rather than the first step in an assurance engagement.
* Without an inventory of devices, training effectiveness cannot be assessed.
* (B) Incorrect - Understand what procedures are in place for locking lost devices.
* This is a specific control measure but not the starting point for an engagement.
* The first step should be to identify what devices exist before evaluating security measures.
* (C) Correct - Obtain a list of all smart devices in use.
* The foundation of an assurance engagement is identifying the scope, which includes listing all smart devices in use.
* This allows the auditor to evaluate security risks, compliance, and control measures effectively.
* (D) Incorrect - Test encryption of all smart devices.
* Testing encryption is an audit procedure that should be performed after understanding the inventory and existing controls.

* Without knowing which devices exist, encryption testing would not be effective.
* IIA's Global Internal Audit Standards - Technology Assurance and Cybersecurity Audits
* Outlines steps for conducting technology-related assurance engagements.
* IIA's GTAG (Global Technology Audit Guide) on Auditing Smart Devices
* Recommends obtaining an inventory of devices as the first step in an audit.
* COBIT Framework - IT Asset Management and Control
* Emphasizes identifying assets as the foundation of IT governance and risk management.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 42
□□ □□ □□ □ □□□□□ □□□ □□□□ □□□ □□□□ □□ □□□□□?
A. □□□.
B. □□.
C. □□□□□.
D. □□
Answer: B (LEAVE A REPLY)
Consideration is a fundamental element of a legally binding contract, referring to something of value exchanged between parties. It ensures that each party receives a benefit or suffers a legal detriment in return for the promise made.
* Essential for Contract Enforceability - A contract must involve an exchange of value (e.g., money, services, goods, or a promise to act or refrain from acting).
* Legal Reciprocity - Both parties must give and receive something of value to make the contract valid.
* Distinguishes Contracts from Gifts - A gift is voluntary and does not require consideration, whereas a contract does.
* A. Lawfulness - A contract must be lawful, but lawfulness is a requirement, not something exchanged.
* C. Agreement - An agreement is part of a contract, but without consideration, an agreement is not legally binding.
* D. Discharge - Discharge refers to ending a contract, not forming one.
* IIA's GTAG on Contract Management Risks - Highlights consideration as a key contract principle.
* COSO's Internal Control Framework - Covers contract law fundamentals in risk management.
* Common Law and Uniform Commercial Code (UCC) - Define consideration as an essential element of a contract.
Why Consideration is the Correct Answer?Why Not the Other Options?IIA References:

NEW QUESTION: 43

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

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

B. □□ □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□.

C. □□ □□□ □□□ □□ □□ □□□ □□□□ □□□□.

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

Answer: C (LEAVE A REPLY)

According to the IIA Standards, follow-up is mandatory only for assurance engagements, where corrective action plans are agreed and tracked. Advisory services are intended to add value and offer recommendations but do not require formal follow-up by internal audit. Responsibility for implementing recommendations lies with management.

Options A and B improperly delegate follow-up responsibilities, and Option D incorrectly suggests mandatory follow-up for advisory engagements.

Reference:

IIA Standards - Standard 2500: Monitoring Progress (applies to assurance, not advisory services).

NEW QUESTION: 44

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

A. □□ □□ □ □□ □□□ □□ □□ □□ □□.

B. □□ □□ □ □□ □□□ □□ □□□ □□.

C. □□ □□□ □□□ □□ □□ □□

D. □□ □□ □ □□□ □□□□ □□ □□

Answer: B (LEAVE A REPLY)

* Recovery Point Objective (RPO) Defined:

* RPO is the maximum amount of data loss an organization can tolerate before it significantly impacts business operations.

* It determines how frequently backups should be performed to minimize data loss in the event of a system failure, cyberattack, or disaster.

* For example: If an organization has an RPO of 4 hours, backups must be performed at least every 4 hours to ensure minimal data loss.

* IIA GTAG on Business Continuity Management states that RPO should align with business risk tolerance and data criticality.

* A. The maximum tolerable downtime after the occurrence of an incident. (Incorrect)

* This defines the Recovery Time Objective (RTO), which refers to the time needed to restore operations.

* RPO relates to data loss, not downtime.

* C. The maximum tolerable risk related to the occurrence of an incident. (Incorrect)

* Risk tolerance is a separate concept related to risk management strategies, not data recovery.
* D. The minimum recovery resources needed after the occurrence of an incident. (Incorrect)
* This refers to disaster recovery planning and resource allocation, not the specific metric of data loss tolerance.
Explanation of Incorrect Answers:Conclusion:The Recovery Point Objective (RPO) measures the maximum allowable data loss (Option B) before it significantly affects business continuity.
IIA References:
* IIA GTAG - Business Continuity Management
* IIA Standard 2120 - Risk Management

NEW QUESTION: 45
□□□□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□□□ □□ □□□□ □□□□ □□□ □ □□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□ □□ □□ □□.
B. □□□ □□□□ □□□ □□□ □□□ □□□□□.
C. □□□□□□ □□ □□ □ □□□ □□□□□ □□ □□□ □□□□.
D. □□□ □□ □□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
To ensure security when employees use their own smart devices to access organizational applications, the best approach is to allow only pre-approved devices that meet the organization's security standards.
* Device Security & Compliance: Approved devices are verified for security measures like encryption, mobile device management (MDM), and antivirus protection.
* Risk Management: Restricting access to pre-approved devices reduces the risk of malware, unauthorized access, and vulnerabilities.
* IT Control & Monitoring: IT can enforce security updates, compliance policies, and access control mechanisms on pre-approved devices.
* Option A (Using a jailbroken or rooted smart device feature): Jailbroken or rooted devices remove security protections and create severe security vulnerabilities.
* Option C (Obtaining written assurance from the employee that security policies and procedures are followed): Written assurances alone are not a security measure; technical controls must be enforced.
* Option D (Introducing a security question known only by the employee): Security questions are weak authentication measures and do not verify the legitimacy of a device.
* IIA's GTAG on Information Security Management stresses the importance of device security and requiring IT-approved devices.

* NIST Special Publication 800-124 (referenced in IIA's IT Audit Guidance) highlights best practices for securing mobile devices in an enterprise setting, recommending pre-approved devices.
Why Option B is Correct:Why Other Options Are Incorrect:IIA References:Thus, the most appropriate answer is B. Using only smart devices previously approved by the organization.

NEW QUESTION: 46
□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□, □ □□□ □□□□□ □□ □□□□□ □□□ □□□□□ □□ □□ □□□ □□□□□ □□ □□□ □□□ □ □□ □
B. □□□□ □□□ □□□ POS □□□□ □□□□□ □□□ □□ □□ □□□ □□ □ □ □□ □□ □□□ □□□ □□□ □□□□ □□□□□□.
C. □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□ □ □□ □□□ □ □□ □□□□□□. □□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□□.
D. □□□ □□□ □□□ □□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □ □□□□ □□ □□□ □□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Cybersecurity and IT Risks section.

NEW QUESTION: 47
□□□□□□□(CAE)□ □□ □□ □□ □□□ □□□□□ □□ □□ □□ □□ □□□ □ □□□ □□□□. CAE□ □□□ □□□ □ □□ □ □□□ □□□□ □□□. □□ □□□□ □□□ □ □□ □□□ □□□□□ □□ □ □□ □□□ □□□□ □□□?
A. □□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□
B. □□□ □□ □□ □□□ □□□ □□
C. □□□ □□ □□ □□ □□□□ □□□ □□
D. □□ □□ □□□ □□□ □□
Answer: A (LEAVE A REPLY)
When calculating available audit hours, the CAE must exclude non-engagement activities such as administration, meetings, professional development, and staff coaching. These are essential but not directly part of engagement execution.

Preliminary risk assessment (Option B), documentation (Option C), and reporting (Option D) are all integral steps of an engagement and should be included in engagement hours. Thus, only coaching time (Option A) should be deducted.
Reference:
IIA Practice Guide - Engagement Planning: Considerations for Resource Planning.

NEW QUESTION: 48
□□ □ 2 □ □□□□□ □□ □□□□□ □□□□ IT □□ □□□ □□□□□?
A. □□ □□□□ □□□□□.
B. □□□ □□□.
C. □□ □□ □□□ □□□ □□□□□.
D. IT □□□ □□ □□□ □ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
* Understanding the Three Lines of Defense Model:
* First Line of Defense (Operational Management): Performs daily IT security tasks, such as blocking unauthorized traffic and encrypting data.
* Second Line of Defense (Risk Management & Compliance): Monitors and reviews security controls, including disaster recovery testing and risk management activities.
* Third Line of Defense (Internal Audit): Provides an independent assessment of IT security controls.
* Why Option C (Review Disaster Recovery Test Results) Is Correct?
* The second line of defense is responsible for monitoring and evaluating IT risk management processes, including disaster recovery and business continuity planning.
* Reviewing disaster recovery test results ensures that the organization is prepared for IT disruptions and meets compliance requirements.
* IIA Standard 2110 - Governance requires auditors to evaluate whether IT risk management activities (such as disaster recovery) are being effectively monitored.
* Why Other Options Are Incorrect?
* Option A (Block unauthorized traffic):
* This is a first-line defense task, typically handled by IT security teams (e.g., firewall and intrusion detection system monitoring).
* Option B (Encrypt data):
* Encryption is part of daily IT security operations and is handled by the first line of defense.
* Option D (Provide an independent assessment of IT security):
* Independent assessments are the responsibility of internal audit (third line of defense), not the second line.
* The second line of defense focuses on monitoring IT risk, making disaster recovery test review a key responsibility.
* IIA Standard 2110 and the Three Lines of Defense Model confirm this role.
Final Justification:IIA References:
* IPPF Standard 2110 - Governance (IT Risk Management)

* IIA Three Lines of Defense Model
* COBIT Framework - IT Governance & Risk Management

NEW QUESTION: 49
□□ □ □□ □□□ □□□□ □□ □□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□□□□ □□ □□□ □□□□ □□□□ □□□□□ □□□, □□□ □□ □□□□ □□□□.
B. □□□□ □□□□□□□□ □□□□□ □□□ □□□□□□ □□□ □□□ □□□□.
C. □□□ □□□□□ □□□ □□□□ □□□, □□□□□ □□□ □□□□□ □□□□ □ □ □□□ □□□□□.
D. □□□□ □□ □□□ □ □□□□□ □□□ □□□ □□□ □□□□ □□□ □□□□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Data Privacy and Regulation section.

NEW QUESTION: 50
□□ □ □□□□ □□□ □□ □ □□□ □□?
A. □ □□ □□□ □□ □□ □□ □□□ □□□□ □□ □□
B. □□ □□□ □□□□ □□ □□ □□ □□ □□ □□.
C. □□ □□□ □□□□ □□ □□ □□□ □□ □□ -ng
D. □□ □□□ □□□□ □□□□ □□ □□ □□ □□□ □□□□ □□
Answer: B (LEAVE A REPLY)
* Understanding Outsourcing:
* Outsourcing refers to contracting business processes, functions, or expertise to an external service provider.
* Companies use outsourcing to reduce costs, access specialized skills, and improve efficiency.
* Why Option B (Contracting Functions or Knowledge-Related Work with an External Provider) Is Correct?
* Outsourcing involves delegating specific business functions (e.g., IT support, payroll, customer service) to external specialists.
* IIA Standard 2110 - Governance supports evaluating outsourcing risks and effectiveness.
* ISO 37500 - Outsourcing Management Framework emphasizes knowledge-based work outsourcing for expertise gains.
* Why Other Options Are Incorrect?
* Option A (Foreign service providers for cost savings):
* While some outsourcing involves foreign providers, outsourcing is not limited to offshoring.
* Option C (Internal service provider):

* Internal service providers do not involve outsourcing, as the work remains within the company.
* Option D (External + internal provider collaboration):
* This describes co-sourcing, not pure outsourcing.
* Outsourcing involves contracting business functions to an external provider, making option B correct.
* IIA Standard 2110 supports governance over outsourcing decisions and risk management.
Final Justification:IIA References:
* IPPF Standard 2110 - Governance (Outsourcing & Vendor Risk Management)
* ISO 37500 - Outsourcing Management Framework
* COSO ERM - Third-Party Risk Management in Outsourcing

NEW QUESTION: 51
□□□ □□ X□ Y□ □□□□□.
□ □□□ □□□ □□□□ □□□ 500kg□□ □□□□□.

	Product X	Product Y
Selling price per unit	$10	$13
Materials per unit (at $1/kg)	2 kg	6 kg
Monthly demand	70 units	120 units

(kg) □. □□ □□ □□□ □□□□□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□ □□□□. □□□ □□□□□ □□ □□□□ □□ □□□□ □□ □□ Y□ □□□□□?
$10 $13
2 kg
70 units
6 kg
120 units
A. 50 units
B. 60 units
C. 70 units
D. 1:20 units
Answer: B (LEAVE A REPLY)
To maximize profit with a limited material supply of 500 kg per month, the company should prioritize producing the product that generates the highest contribution margin per kg of material used.
Step 1: Calculate Contribution Margin Per Unit for Each ProductSince fixed costs are not relevant in this decision, we focus on the contribution margin per unit of raw material:
* Selling price per unit = $10
* Material cost per unit = 2 kg × $1/kg = $2

* Contribution margin per unit = $10 - $2 = $8
* Contribution margin per kg = $8 ÷ 2 kg = $4 per kg
* Selling price per unit = $13
* Material cost per unit = 6 kg × $1/kg = $6
* Contribution margin per unit = $13 - $6 = $7
* Contribution margin per kg = $7 ÷ 6 kg = $1.17 per kg
* Product X ($4 per kg) is more profitable per kg than Product Y ($1.17 per kg).
* To maximize profit, produce as many units of Product X as possible first, then allocate the remaining material to Product Y.
* First, maximize production of Product X
* Each unit of Product X requires 2 kg.
* Maximum units of Product X = 500 kg ÷ 2 kg per unit = 250 units.
* However, demand is only 70 units, so produce 70 units of Product X.
* Material used for 70 units of X = 70 × 2 kg = 140 kg.
* Material remaining = 500 kg - 140 kg = 360 kg.
* Use remaining material for Product Y
* Each unit of Product Y requires 6 kg.
* Maximum units of Product Y = 360 kg ÷ 6 kg per unit = 60 units.
* Produce 70 units of Product X (to meet demand).
* Produce 60 units of Product Y (using the remaining material).
* IIA GTAG 13: Business Performance Management - Discusses maximizing profit by prioritizing high contribution margin products.
* IIA Practice Guide: Cost Analysis for Decision-Making - Covers constraints and resource allocation for maximizing profitability.
Product XProduct YStep 2: Prioritize Product with Higher Contribution Margin Per KgStep 3: Allocate Limited Material (500 kg)Final Decision:IIA References for Validation:Thus, B (60 units) is the correct answer because it optimally allocates the 500 kg of material to maximize profit.

NEW QUESTION: 52
□□ □□ □□□□ □□□□ □□ □□ □ □□ □□ □□□□□?
A. □□ □□ □□□□ □□ □□ □ □□□ □□ □□□□□□ □□ □□□ □□□ □ □□ □ □□ □□□□.
B. IIA □□□□□ □□□ □□□□□□ □□ □□ □□□□ □□□ □ □□□ □□ □□□ □□□□ □□□□.
C. □□ □□ □□□□ □□ □□ □ □□□ □□ □□ □ □□ □□□ □□□ □□□□ □□ □□.
D. □□ □□ □□□□ □□□ □□ □□ □□□□ □□ □□□□□ □□ □□ □ □□ □□ □□ □□□□ □□□□ □□□.
Answer: (SHOW ANSWER)

Internal audit methodologies are determined by the CAE and should be aligned with the IIA's principles of confidentiality, integrity, objectivity, and competency. This ensures methodology design is consistent with professional standards.
Option A misstates the objective-methodologies are not for client validation. Option B is incorrect because methodologies are not required to be publicly posted. Option C mischaracterizes the objective: methodology ensures audit consistency, not execution of organizational strategy directly.
Reference:
IIA Standards - Standard 2040: Policies and Procedures.

NEW QUESTION: 53
□□□ □□□ □□□□ □□ □□□ □□□□□ □□ □□ □□□□ □□□□□□□. □□ □□ □□ □ □□□□ □□ □□□□ □□□□□□. □□□□ □□□□□□ □□□ □□□ □ □□□□ □□□ □□□ □□□□□ □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □□□□□□. □□□ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□. □□ □ □□□□ □□□□ □□□□ □□ □ □□□ □□ □□□ □□□□□?
A. □□□ □□.
B. □□□ □□.
C. □□□ □□.
D. □□□ □□□.
Answer: D (LEAVE A REPLY)
The auditor likely omitted the data normalization step, which is crucial when integrating multiple datasets from different sources (e.g., human resources (HR) and payroll). Without normalization, inconsistencies in formatting, naming conventions, or unique identifiers (e.g., employee ID vs. full name) can result in incorrect mismatches.
* Standardization of Data Formats:
* Employee names or IDs may be stored differently across systems (e.g., "John A. Doe" in HR vs.
"Doe, John" in payroll).
* Normalization ensures uniform formatting to enable accurate comparisons.
* Removal of Duplicates & Inconsistencies:
* Employee records could have multiple variations due to typos, abbreviations, or missing fields.
* Proper cleaning and transformation of data ensures better accuracy.
* Use of Unique Identifiers:
* Instead of matching by name, the auditor should have used a unique identifier (e.g., Employee ID), which remains constant across systems.
* A. Data analysis (Incorrect)
* Reason: The auditor did attempt data analysis (matching employee records) but without proper preparation (normalization), the results were flawed.

* B. Data diagnostics (Incorrect)
* Reason: Data diagnostics refers to evaluating data quality issues, but it does not involve transforming data to a common format, which was the missing step.
* C. Data velocity (Incorrect)
* Reason: Data velocity relates to the speed at which data is processed, which is not relevant to the issue of incorrect matching.
* IIA Global Technology Audit Guide (GTAG) 16: Data Analysis Technologies - Covers data quality, normalization, and audit data preparation.
* IIA GTAG 3: Continuous Auditing - Discusses the importance of accurate data extraction and transformation.
* IIA Standard 2320 - Analysis and Evaluation - Ensures appropriate data validation before concluding audit findings.
Why is Data Normalization Important?Analysis of Incorrect Answers:IIA References:Thus, the correct answer is D. Data normalization.

NEW QUESTION: 54
□□□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □ □□□□?
A. □□ □ □□ □□□ □□
B. □□ □□ □□□ □□ □□ □□
C. □□□ □□□ □□ □□ □□ □□□ □□ □□
D. □□□□□ □□□□ □□□ □□ □□□□□ □□□ □ □□ □□ □□
Answer: (SHOW ANSWER)
Reference: IIA Business Knowledge for Internal Auditing, Job Design section.

NEW QUESTION: 55
□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□ □□□ □□ □□□□ □□. □□□□ □□□ □□ □□□□ □□ □□□ □□□?
A. □□□□□ □□□□□□ □□□□ □□□□□□□.
B. □□□□□ □□□□□□ □□□□ □□□□□□□.
C. □□ □□□ □□ □□□□ Wi-Fi□ □□□□ □□□ □□□ □□□□.
D. □□□□□ □□□ □□ □□□□ □□□□□□□.
Answer: A (LEAVE A REPLY)
A periodic inventory system calculates cost of goods sold (COGS) using the formula: COGS=Beginning Inventory+Purchases#Ending InventoryCOGS = \text{Beginning Inventory} + \text
{Purchases} - \text{Ending Inventory}COGS=Beginning Inventory+Purchases#Ending Inventory If beginning inventory is understated, it causes COGS to be understated, which in turn overstates net income because expenses are lower than they should be.
* Understated Beginning Inventory # Understated COGS
* Since COGS is too low, fewer expenses are deducted from revenue.
* Understated COGS # Overstated Net Income

* If COGS is too low, the company's profit (net income) is artificially inflated.
* (A) COGS will be understated and net income will be overstated (Correct Answer):
* Since the beginning inventory was understated, COGS is lower than it should be, making net income higher than it should be.
* (B) COGS will be overstated and net income will be understated:
* This would be true if beginning inventory was overstated, but in this case, it was understated, making this incorrect.
* (C) COGS will be understated and there will be no impact on net income:
* Since COGS affects net income, this statement is incorrect. Understated COGS overstates net income.
* (D) There will be no impact on COGS and net income will be overstated:
* This is incorrect because COGS is directly affected by an inventory misstatement.
* IIA GTAG 3: Continuous Auditing - Discusses the importance of accurate financial reporting in preventing misstatements.
* COSO Internal Control Framework - Financial Reporting Component - Highlights the impact of inventory errors on financial accuracy.
* IIA Standard 2330 - Documenting Information - Requires auditors to evaluate financial calculations for accuracy and completeness.
Step-by-Step Impact on Financial Statements:Analysis of Each Option:IIA References:Conclusion:Since COGS is understated and net income is overstated, option (A) is the correct answer.

NEW QUESTION: 56
□□ □ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□ □□□□□?
A. □□□ □□ □□□ □□□□ IT □□□□ □□□□ □□, □□□ □□ □□□ IT □□□ □□□ □□□□□□ □□□□ □□□□□.
B. □□□ □□ □□□ IT □□□ □□□ □□□□□□ □□□□ □□□□ □□, □□□ □□ □□□ □□□□ IT □□□□ □□□□□.
C. □□□ □□ □□□□ □□□, □□□ ID, □□□□□ □□□□, □□□ □□ □□□□ □ □□□□ □□□□ □□□□□.
D. □□□ □□ □□□□ □□ □□ □ □□ □□□ □□□□ □□, □□□ □□ □□□□ □ □ □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Physical access controls are security measures designed to prevent unauthorized physical access to tangible IT resources, such as computer hardware, servers, and networking equipment. Examples include locks, security guards, and biometric access systems. In contrast, logical access controls protect access to software and data within the IT system, ensuring that only authorized users can interact with digital resources. These controls include mechanisms like user IDs, passwords, firewalls, and encryption. Option A

accurately captures this distinction, whereas the other options either reverse the definitions or misclassify examples of physical and logical controls.

NEW QUESTION: 57
□□ □□ □ □□ □□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□ □□ □□ □□ □□□□□?
A. □□ □□
B. □□□ □□
C. □□ □□□ □□
D. □□ □□□ □□□
Answer: C (LEAVE A REPLY)
If the internal audit activity lacks the necessary skills to perform certain audits, this represents a limitation that could impair internal audit's ability to meet its responsibilities. The CAE must report such resource or competency limitations to the board.
Options A, B, and D (procedures, forms, or methods) may be adjusted internally, but they do not rise to the level of a significant limitation requiring board reporting. Skills gaps, however, directly impact audit coverage and effectiveness.
Reference:
IIA Standards - Standard 2030: Resource Management; Standard 2060: Reporting to Senior Management and the Board.

NEW QUESTION: 58
□□□ □□□ □□□□ IT □□□□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □ □□ □□□ □□□ □□ □□□□ □□□□□□□. □□ □□□ □□ □ □□ □□ □□□ □ □ □□□ □□□ □ □□□□ □□□□?
A. □□□ □□ □□□□ □□□□□ □□□□□□ □□□ □□□□ □□□□□.
B. □□□□□ □□□□□□ □□□ □□ □□□□ □ □□□ □□□□ □□□□.
C. □□ □□□□ □□ □□□□ □□ □□□□□□□.
D. □□ □□□ □□ □□□□ □□□ □□□ □ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, IT Risk and Controls section, Disaster Recovery and Business Continuity principles.

NEW QUESTION: 59
□□ □ □□ □□□□□ □□□□□ □□□□ □□□ □□□□□?
A. □□□□ □□□□
B. □□ □□
C. □□□ □□
D. □□□, □□ □□ □□□□ □□ □□
Answer: (SHOW ANSWER)
Reference: IIA Business Knowledge for Internal Auditing, Help Desk Functions section.

NEW QUESTION: 60
IT□ □□ I1A □□□ □□□. □□ □□□ □□ □□ □□ □ □□□, □□ □□□ □□ □□ □□ □□ □□ □□□ □□□ □□ □ □ □□ □□ □□□□□?
A. □□ □□□ □□□□ □□□□□□□.
B. □□□ □□ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
* Understanding Information Security Responsibilities:
* Executive management sets the overall strategy and ensures resources are allocated for information security.
* Internal auditors provide independent assurance on security effectiveness.
* The board provides oversight and ensures that security risks are managed appropriately.
* Line management is responsible for day-to-day operations, including the review and monitoring of security controls to ensure compliance with security policies.
* Why Reviewing and Monitoring Security Controls is a Line Management Function:
* Line management directly oversees operational security measures, ensuring that established controls are functioning effectively.
* They address security gaps, enforce security policies, and report issues to senior management when necessary.
* This aligns with IIA Standard 2120 - Risk Management, which requires management to implement and monitor risk mitigation controls.
* Why Other Options Are Incorrect:
* B. Dedicate sufficient security resources: This is the responsibility of executive management, as they control resource allocation.
* C. Provide oversight to the security function: The board and executive management provide oversight, not line management.
* D. Assess information control environments: Internal auditors assess control environments, ensuring compliance and effectiveness.
* IIA Standards and References:
* IIA Standard 2110 - Governance: Emphasizes the board's role in overseeing security.
* IIA Standard 2120 - Risk Management: States that management must monitor security risks.
* IIA GTAG (Global Technology Audit Guide) on Information Security (2016): Outlines that line management is responsible for monitoring security controls on a daily basis.
Thus, the correct answer is A: Review and monitor security controls.

NEW QUESTION: 61
□□ □□□□ □□□ □□ □□ □□□□ □ □□ □□□ □□□ □□ □□□□ □□□ □ □□ □□□□□□. □□ □ □ □□ □□/□□□□ □□□□ □ □ □□ □□ □□□□□?

A. □□□□ □□□□□ □□□□□□.
B. □□ □□□ 1□□ □□□ □□□
C. □□□ □□□ □ □□□ □□□□ □□□.
D. □□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
A cold site is a disaster recovery option that provides only basic infrastructure (such as power, space, and network connectivity) but does not have pre-installed IT equipment such as servers and storage.
Organizations must procure and install servers and restore data before resuming operations, leading to longer recovery times.
Let's analyze each option:
* Option A: Data is synchronized in real-time
* Incorrect.
* Real-time data synchronization is a feature of hot sites, which have fully operational infrastructure and data replication.
* Cold sites do not support real-time synchronization because they lack servers and storage.
* Option B: Recovery time is expected to be less than one week
* Incorrect.
* Cold sites require significant setup time since servers and infrastructure must be procured, configured, and installed.
* Recovery time can often exceed one week, depending on the complexity of IT systems.
* Option C: Servers are not available and need to be procured
* Correct.
* A cold site lacks computing hardware (e.g., servers, storage, network devices), meaning the organization must purchase or transport servers to the site before recovery can begin.
* IIA Reference: Internal auditors assess disaster recovery strategies, including the limitations of cold sites and their impact on business continuity. (IIA GTAG: Auditing Business Continuity and Disaster Recovery)
* Option D: Recovery resources and data restore processes have not been defined.
* Incorrect.
* Even though a cold site lacks IT infrastructure, the organization still has a disaster recovery plan, which includes predefined recovery steps, resource planning, and data restoration procedures.
Thus, the verified answer is C. Servers are not available and need to be procured.

NEW QUESTION: 62
□□ □ □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □ □□□□ □□ □ □□□□?
A. □□□ □□□□ □□ □□ □□□ □□□□□
B. □□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□ □□ □□□□ □□□□□.
D. □□ □□□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The CAE's role is to provide assurance that risks are identified and managed appropriately. When residual risk appears to exceed the organization's tolerance, the CAE should first communicate the matter with senior management to discuss the issue and understand management's acceptance of risk. Only if the risk remains unresolved should it be escalated to the board.
Option A is management's responsibility, not internal audit's. Option B is incomplete as evidence alone does not fulfill the communication requirement. Option C is premature because immediate escalation to the board skips management dialogue.
Reference:
IIA Standards - Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 63
□□ □□ □□ □ □□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. □□ □□ □□ □□
B. □□□ □□.
C. □□ □□ □□ □□□□
D. □□ □□ □□
Answer: (SHOW ANSWER)
Preventing security breaches requires proactive security controls, and the approval of identity requests ensures that only authorized individuals gain access to systems and data.
* Types of Security Controls:
* Preventive Controls (Stop security incidents before they happen)
* Detective Controls (Identify security breaches after they occur)
* Corrective Controls (Address security issues after detection)
* Why Identity Request Approval is the Most Effective Preventive Control?
* User access approval ensures that only verified personnel receive credentials.
* According to IIA GTAG on Identity and Access Management, user provisioning must follow strict approval workflows to prevent unauthorized access.

* By restricting access before a breach occurs, organizations reduce risks related to insider threats, phishing attacks, and credential misuse.
* Why Not Other Options?
* B. Access Logging:
* Access logs record activity but do not prevent security breaches.
* C. Monitoring Privileged Accounts:
* Monitoring privileged accounts helps detect suspicious activity but does not stop unauthorized access beforehand.
* D. Audit of Access Rights:
* Regular audits ensure compliance but do not actively prevent unauthorized access in real-time.
* IIA GTAG - Identity and Access Management
* IIA Standard 2120 - Risk Management and IT Controls
* COBIT 2019 - Access Control and Security Management
Step-by-Step Justification:IIA References:Thus, the correct and verified answer is A. Approval of identity request.

NEW QUESTION: 64
□□ □□□□ □□ □□ □□ □ □□□□ □□□ □□ □□□ □□□ □□ □□□□ □□ □□□□. □□□□ 3□□ □ □□ □□□ □□ □□ □□□ □□ □□ □□□□ □, □□□ □ □□ □□ □□□□ □□□ □□□□□ □□□□ □□□ □□□ □□□ □□□□ □□□ □ □□□□□. □□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□□ □□□ □□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□□.
B. □□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□ □□□ □□□ □ □□□ □□ □□□ □□□ □□□.
C. □□ □□□□ □ □□□ □□ □□ □□□□□ □□□□ □□, □□ □□ □□□□ □□ □□ □□□ □□□ □□□□ □□ □□□□ □□□.
D. □□ □□□□ □ □□□ □□ □□ □□□□□ □□□□ □□, □□ □□ □□□□ □ □ □□ □□ □□□□ □□□□ □□□.
Answer: D (LEAVE A REPLY)
When management has not implemented agreed action plans, the internal audit team must escalate the matter to the CAE. The CAE is responsible for discussing such cases with senior management to understand the reasons and determine next steps.
Option A is inappropriate because it is management's responsibility-not internal audit's-to propose action plans. Option B disregards the initial high-risk issue. Option C (escalation to the board) is premature unless senior management fails to act.
Thus, the correct response is Option D: report to the CAE, who should discuss with senior management.
Reference:
IIA Standards - Standard 2500: Monitoring Progress; Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 65
□□□ □□□ □□□□□ □□□□ □□□ □□□□ □□□□. □□ □ □ □□□ □□□ □□□ □□□□□?
A. □□ □□ □□, □□ □□ □ □□ □□ □□.
B. □□ □□, □□ □□ □□ □ □□ □□ □□.
C. □□ □□, □□ □□ □ □□ □□ □□.
D. □□ □□ □□, □□ □□ □ □□ □□
Answer: A (LEAVE A REPLY)
When deciding whether to sell a product as-is or process it further, a manufacturer should consider only relevant costs-those that will change based on the decision.
* Why Option A (Incremental processing costs, incremental revenue, and variable manufacturing expenses) is Correct:
* Incremental processing costs: These are additional costs required to process the material further, making them directly relevant.
* Incremental revenue: The additional revenue that would be generated if the product is processed further is a key factor in decision-making.
* Variable manufacturing expenses: These costs change with production levels, making them important in the decision-making process.
* Why Other Options Are Incorrect:
* Option B (Joint costs, incremental processing costs, and variable manufacturing expenses):
* Incorrect because joint costs (costs incurred before the split-off point) are sunk costs and are not relevant in the decision.
* Option C (Incremental revenue, joint costs, and incremental processing costs):
* Incorrect because, again, joint costs are not relevant to the decision.
* Option D (Variable manufacturing expenses, incremental revenue, and joint costs):
* Incorrect because joint costs should be ignored in a sell-or-process-further decision.
* IIA GTAG - "Auditing Cost Accounting Decisions": Discusses relevant costs in decision-making.
* IFRS & GAAP Cost Accounting Standards: Explain cost classification and decision-making.
* COSO Internal Control - Integrated Framework: Recommends proper cost allocation methods for financial decisions.
IIA References:

NEW QUESTION: 66
IT□ □□ IIA □□□ □□□. □□ □ □□□ □□ □□□ □□□□ □□ □□□□□□□ □ □ □□ □□□ □□□□ □□ □□□□□?
A. □□ □ □□ □□□□ □□ □□□ □□□□ □□□□.
B. □□□□□□□ □□ □□□□ □□□□ □□□ □□□□□.

C. □□□□□□□ □□□ □□□ □□□□□ □□□□.
D. □□□ □ □□□□ □□□□□□ □□□ □□□□ □ □□□□□.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Primary controls in spreadsheet management focus on ensuring data accuracy, integrity, and security.
Option A (Locking formulas and static data) prevents unauthorized changes, ensuring data integrity. This is a direct control over spreadsheet accuracy, making it the correct answer.
Option B (Backup storage) is an IT operational control, not a primary financial reporting control.
Option C (Documentation of spreadsheet use) is important for governance but does not directly prevent errors.
Option D (Version control software) helps manage changes but does not directly ensure financial reporting accuracy.
Thus, locking and protecting spreadsheet formulas is the most critical primary control for accurate financial reporting.
Reference: IIA IT Controls & Data Governance

NEW QUESTION: 67
□□ □□□□ □□ □□ □□□□□ □□ □□□□ □□ □□ □□□□ □□□ □□□ □□ □ □□□□ □□ □□□ □□□□□□. □□□□ □□□□ □□ □□□ □□□ □□ □□□ □ □□□□, □ □□□□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□□□. □□ □□ □□ □ □□□ □□□□ □□ □□□□□ □□ □ □□□ □□ □□□ □□□□ □□ □□□□□?
A. □□ □□□ □□□□ □□□□□ □□ □□□□ □□□□□□□.
B. □□ □□□□□ □□ □□ □□□ □□ □□ □□
C. □□□□ □□ □□ □□□□ □□□□ □□□□□.
D. □□ □□ □□□ □□□ □□ □□□□□ □□□□□□.
Answer: (SHOW ANSWER)
The root cause of the missing significant risks lies in the methodology used for risk identification. If the process relies too rigidly on a standard set of questions, it may overlook critical risks. By revising the risk identification methodology, the organization ensures that future projects capture relevant risks comprehensively and consistently, adding long-term value.
Option A addresses only the current project, not the underlying issue. Option B may improve knowledge but does not fix the flawed process. Option D merely shifts responsibility but does not address the methodology weakness.
Reference:
IIA Standards - Standard 2120: Risk Management.

NEW QUESTION: 68

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

A. □□□ □□ □□□□ □□□□ □□□□□.

B. □□□□ □□□ □□ □□□ □□ □□□ □□□□□.

C. □□ □□ □□ □ □□□□ □□□ □□□□□.

D. □□□□ □□□□□□.

Answer: C (LEAVE A REPLY)

When performing follow-up work, the first step for an auditor-especially one not previously involved in the engagement-is to review the prior audit report, findings, and management's agreed response/action plan.

This provides context on what needs to be validated before collecting new evidence. Interviewing management (Option A), requesting documentation (Option B), or performing walkthroughs (Option D) are important steps, but they come only after the auditor has reviewed the original findings and corrective commitments.

Reference:

IIA Standards - Standard 2500: Monitoring Progress.

NEW QUESTION: 69

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

A. □□ □□ □□

B. □□ □□

C. □□□ □□ □□□□ □ □□□□.

D. □ □□ □□ □□ □□

Answer: C (LEAVE A REPLY)

When a company finances through bonds (debt) instead of issuing common stock (equity), it increases earnings per share (EPS) because bond financing does not dilute ownership, whereas issuing new stock does.

* Impact on Earnings Per Share (EPS):

* EPS formula: EPS=Net Income#Preferred DividendsNumber of Outstanding Shares \text{EPS}

= \frac{\text{Net Income} - \text{Preferred Dividends}}{\text{Number of Outstanding Shares}} EPS=Number of Outstanding SharesNet Income#Preferred Dividends

* Since bond financing does not increase the number of shares outstanding, net income is distributed among fewer shareholders, increasing EPS.

* If the company issues more stock instead of bonds, EPS decreases because the same earnings are divided among more shares.

* Why Bond Financing Affects EPS Favorably:

* Interest on bonds is tax-deductible, reducing taxable income and increasing net profits.

* Unlike dividends, which are paid on common stock and reduce retained earnings, bondholders receive fixed interest payments that do not dilute equity ownership.
* A. Lower shareholder control: #
* Bondholders do not get voting rights, whereas issuing more stock reduces existing shareholders' control.
* This statement would be true for stock financing, not bond financing.
* B. Lower indebtedness: #
* Bonds increase a company's debt obligations, not reduce them.
* If a company uses stock financing instead of bonds, it avoids taking on debt.
* D. Higher overall company earnings: #
* While bonds increase EPS, they do not necessarily increase total earnings.
* The company must pay interest on bonds, which could reduce net income if not managed properly.
* IIA Standard 2110 (Governance): Ensures management selects financing strategies that align with financial stability.
* COSO ERM Framework - Financial Risk Management: Evaluates how financing choices impact shareholder value and risk exposure.
* IFRS & GAAP Accounting Standards on Debt vs. Equity Financing: Explain how bond financing increases EPS compared to issuing new shares.
Step-by-Step Justification:Why Not the Other Options?IIA References:

NEW QUESTION: 70
□□□ IT □□□ □□□ □□□ □ □□ □ □□□□□□ □□□ □□□ □□□□□ □□ □ □□ □□□□□?
A. □□ □□□
B. □□□ □□
C. □□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)
* Understanding IT Infrastructure Risks and Workstation Security:
* Reviewing an organization's IT infrastructure risks includes assessing the security of workstations (desktops, laptops, and terminals) that connect to the organization's network.
* Workstations are vulnerable to physical theft, unauthorized access, and malware attacks, making physical controls a critical security measure.
* Why Physical Controls Are the Most Relevant for Workstations:
* Physical controls prevent unauthorized physical access, theft, tampering, and damage to workstations.
* Examples include:
* Locked office spaces or workstation enclosures to restrict access.
* Security badges or biometric authentication to prevent unauthorized use.
* Cable locks for laptops and desktop computers to deter theft.

* Surveillance cameras and security guards to monitor access.
* Why Other Options Are Incorrect:
* A. Input controls - Incorrect.
* Input controls ensure accuracy and completeness of data entry, which applies more to application security, not workstation security.
* B. Segregation of duties - Incorrect.
* Segregation of duties prevents fraud and conflicts of interest, but it does not directly address workstation security risks.
* D. Integrity controls - Incorrect.
* Integrity controls ensure data consistency and accuracy in databases and transactions , not workstation security.
* IIA's Perspective on IT Risk and Physical Security Controls:
* IIA Standard 2110 - Governance requires organizations to implement physical security measures for IT assets, including workstations.
* IIA GTAG (Global Technology Audit Guide) on IT Risks highlights the importance of restricting physical access to IT devices to prevent unauthorized use or data breaches.
* ISO 27001 Information Security Standard recommends physical controls to secure IT infrastructure and prevent workstation-related risks.
IIA References:
* IIA Standard 2110 - IT Security & Physical Access Control
* IIA GTAG - Physical Security of IT Assets
* ISO 27001 - Physical Security and IT Risk Management
Thus, the correct and verified answer is C. Physical controls.

NEW QUESTION: 71
□□ □ □□ □□ □□□ □□□ □□ □ □□□ □□?
A. □□ □□□ □□□□ □□□□ □□.
B. □□□ □□□ □□ □□□ □□□ □□.
C. □□□□□□ □□□□ □□□□ □□□ □□□□□ □□.
D. □□ □□□□□□ □ □□□ □□□□
Answer: A (LEAVE A REPLY)
Fixed manufacturing costs refer to costs that do not vary with the level of production activity within a relevant range. These costs include expenses such as depreciation, rent, property taxes, and salaries of permanent employees in the production facility. Their primary purpose is to ensure the availability and operational readiness of production facilities, regardless of fluctuations in production levels.
* (A) Correct - To ensure availability of production facilitiesFixed manufacturing costs are incurred to maintain and operate production facilities, ensuring that they remain functional and available for production when needed. These costs exist even if no units are produced, emphasizing their role in sustaining the production infrastructure.

* (B) Incorrect - To decrease direct expenses related to productionFixed manufacturing costs are unrelated to direct expenses, such as raw materials and labor, which vary with production volume.
Instead, they remain constant regardless of output levels.
* (C) Incorrect - To incur stable costs despite operating capacityWhile fixed costs remain stable within a relevant range, their primary purpose is not just cost stability but ensuring production facilities' availability and functionality.
* (D) Incorrect - To increase the total unit cost under absorption costingUnder absorption costing, fixed manufacturing costs are allocated to units produced, affecting per-unit cost calculations. However, this is an accounting treatment rather than the core purpose of fixed manufacturing costs.
* IIA's Global Internal Audit Standards - Managing Resources Effectively
* Fixed manufacturing costs ensure operational resources are available and managed efficiently.
* IIA's Guide on Cost Management and Internal Control
* Highlights the role of cost structures, including fixed costs, in ensuring business continuity.
* IIA's Practice Advisory on Cost Accounting Controls
* Discusses the importance of maintaining production facilities to ensure operational readiness.
Breakdown of Answer Choices:IIA References and Internal Auditing Standards:Would you like further clarification on any point?

NEW QUESTION: 72
□ □□□□□□□ □□□ □□ □□□□ □□ □□ □□ □□□ □□ □□□ □□□ □□□ □□ □□□. □□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□□ □□□ □ □□□□ □□ □□□□ □□□ □□ □□□ □□ □ □ □□□ □□□ □ □□□□.
B. □□ □□ □ □ □□ □□□□ □□ □□ □□□ □□□□□ □□□□□.
C. □□□ □□ □□□□□ □□ □□□ □□□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□ □□ □□□□ □□□□□□.
Answer: D (LEAVE A REPLY)
The Global Internal Audit Standards require that workpapers be properly supervised and reviewed to ensure quality and compliance. A sole auditor cannot perform a meaningful self-review (Option A). Having clients review workpapers (Option B) compromises independence. Having management or the board sign off (Option C) is also inappropriate as it undermines audit objectivity.
The most suitable solution is to arrange for peer reviews from external auditors or other organizations, with confidentiality and legal safeguards in place. This provides independent oversight while maintaining audit quality.
Reference:

IIA Standards - Standard 1312: External Assessments; Practice Guide - Quality Assurance and Improvement Program.

NEW QUESTION: 73
IIA□ 3□ □□ □□□ □□□ □□ IT □□ □□ □ 3□ □□ □□□□ □□□□□ □□□□ □□ □□□□□?
A. □3□ □ □□□□□ □□ □□.
B. □□ IT □□□ □□ □ □□.
C. □□□ □□ □ □□ □□ □□.
D. □□ □□□□ □ □□ □□□ □□ □ □□.
Answer: A (LEAVE A REPLY)
* Understanding The IIA's Three Lines Model:
* The Three Lines Model defines responsibilities for risk management and control across different organizational functions:
* First Line: Operational management (owns and manages risks).
* Second Line: Risk and compliance functions (monitors and facilitates risk management).
* Third Line: Internal audit (provides independent assurance).
* Why Third-Party and Supplier Assessments Are Shared Across All Three Lines:
* First Line (Operational Teams & IT Security): Ensures that vendors comply with security standards.
* Second Line (Risk & Compliance Teams): Conducts due diligence and ensures compliance with cybersecurity regulations.
* Third Line (Internal Audit): Independently evaluates supplier risk management processes.
* Why Other Options Are Less Relevant:
* B. Recruitment and retention of certified IT talent - Primarily a first-line management responsibility (HR and IT departments).
* C. Classification of data and design of access privileges - Typically a first-line IT security function, with oversight from the second line.
* D. Creation and maintenance of secure network configurations - Falls under first-line IT operations with oversight but not shared by all three lines.
* IIA's Three Lines Model (2020 Update): Emphasizes shared responsibilities in areas like third-party risk.
* IIA Practice Guide on Third-Party Risk Management: Internal audit must assess supplier security and compliance.
* COSO ERM Framework: Highlights vendor risk management as a cross-functional responsibility.
Relevant IIA References:# Final Answer: Assessments of third parties and suppliers (Option A).

NEW QUESTION: 74
□□ □ □□□□□ □□□□ □□ □□ □□□ □□ □□ □ □□ □□ □□□□□?

A. □□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□.
B. □□ □□□ □□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□□□.
C. □□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □ □□□.
D. □□□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □□ □ □□ □□□ □□□ □ □□ □□□ □□ □□□ □ □□□□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
In a hierarchical audit structure, work is reviewed across multiple levels of management, resulting in higher costs because highly skilled and experienced auditors are required for supervisory roles. This increases the cost base compared to a flat structure.
Option A exaggerates benefits of a flat structure. Option B is incorrect because hierarchical structures require more-not less-supervision. Option C is misleading because flat structures typically limit growth opportunities due to fewer layers of promotion.
Reference:
IIA Practice Guide - Organizational Governance in Internal Audit.

NEW QUESTION: 75
□□□□ □□ □□ □□□ □□□□ □□ □□ □□□□ IT □□□□□ □□ □□ □□□□ □□ □□□ □□ □□ □□□ □□ □ □□□□ □□ □□□ □□□ □□□ □ □□□ □□ □□□□. □□□□ □□□□ □□□ □□□ □□ □□ □□□□ □□□ □□□ □ □□□ □□□ □□□□□□. □□ □ □□ □□□ □□ □□ □□ □□□ □□□□□?
A. □ □□□ □□ □□□□□ □ □□ □□□□, □□□□□□□ □□□ □□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□.
B. □□□□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□ □□□□□□ □□□ □ □□ □□ □□□ □□□□□ □□□□ □□□.
C. □□□□ IT □□□□□ □□□ □□□ □□□ □ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□□ □□□.
D. □□□ □□□ □ □□□ □□□□ □□□ □ □□□ □□ □□ □□□□□ □□□□□ □□ □□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
A tolerance threshold is a recognized control that allows for efficiency while preventing abuse. By setting a monetary limit, the process permits legitimate small variances (e.g., transport costs) while ensuring significant discrepancies are flagged and cannot be bypassed.
Option A is overly rigid and impractical. Option B is administratively burdensome. Option D lacks control and exposes the process to risk.
Reference:
IIA Standards - Standard 2130: Control.

NEW QUESTION: 76

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

A. □□ □□□ □□ □□

B. □□ □□□ □□ □□ □□

C. □□ □□ □□ □□

D. □□□□ □□□ □□□ □□ □□□□ □□

Answer: C (LEAVE A REPLY)

Reference: IIA Business Knowledge for Internal Auditing, Business Continuity Planning section.

NEW QUESTION: 77

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

A. □□ □□□ □□ □□□□ □□ □ □□ □□□ □□□□.

B. □□□ □□□ □□□□□ □□ □□□□ □□□ □□□□.

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

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

Answer: A (LEAVE A REPLY)

* Understanding Organizational Structures in Internal Audit:
* A flat organizational structure has fewer levels of management, leading to faster decision-making, less bureaucracy, and lower administrative costs.
* A hierarchical structure has multiple levels of management, which may improve control and oversight but increases complexity and costs.
* Why a Flat Structure Reduces Operating and Support Costs:
* Fewer management layers mean fewer salaries and reduced administrative expenses.
* Streamlined decision-making reduces inefficiencies in reporting and communication.
* Leaner support functions lead to cost savings in internal audit activity.
* Why Other Options Are Less Relevant:
* B. Stable and collaborative environment: Collaboration depends on culture, not just structure.
Hierarchical models can also be collaborative.

* C. Enables field auditors to report to senior auditors: This is more common in hierarchical structures where clear reporting lines exist.
* D. More dynamic with advancement opportunities: Hierarchical structures often provide clearer career progression due to well-defined promotion paths.
* IIA Standard 2030 - Resource Management: Encourages optimizing resources, which a flat structure can support.
* IIA Practice Guide on Effective Internal Audit Governance: Discusses structural efficiency and cost control in internal audit.
* COSO's Internal Control Framework: Emphasizes efficient resource allocation in governance structures.
Relevant IIA References:# Final Answer: A flat structure results in lower operating and support costs than a hierarchical structure (Option A).

NEW QUESTION: 78
□□ □ □□ □□□ □□□ □ □□ □□?
A. □□□ □□□□ □□ □□
B. □□ □□.
C. □□ □□□□□□ □□,
D. □□ □□□ □□
Answer: B (LEAVE A REPLY)
Debt investments refer to financial instruments where an investor lends money to an entity (corporation, government, or institution) in exchange for periodic interest payments and the repayment of the principal amount at maturity. These include:
* Government bonds (such as U.S. Treasury bonds, municipal bonds, and sovereign bonds)
* Corporate bonds
* Certificates of deposit (CDs)
* Commercial paper
* A. Investments in the capital stock of a corporation # Incorrect. Capital stock represents ownership (equity investments), not debt investments.
* C. Contents of an investment portfolio # Incorrect. A portfolio may contain both equity and debt investments, making this too broad to classify specifically as debt.
* D. Acquisition of common stock of a corporation # Incorrect. Common stock is an equity investment, not a debt investment.
* The IIA's Global Internal Audit Standards on Investment Management and Risk Assessment highlight debt instruments as fixed-income securities.
* International Financial Reporting Standards (IFRS 9 - Financial Instruments) classify bonds and loans as debt investments, distinct from equity instruments.
* The Generally Accepted Accounting Principles (GAAP) - FASB ASC 320 specifies how to account for debt securities.

Explanation of the Other Options:IIA References & Best Practices:Thus, the correct answer is B. Acquisition of government bonds.

NEW QUESTION: 79
IIA □□□ □□□, □3□□ □□□ □□□□□ □□□□ □□□□ □□ □□□ □□□□ □ □ □ □□ □□□ □□ □□ □□ □□□□□?
A. □□□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□□□ □□ □□□□ □□ □ □□ □□
B. □□□□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□□ □□ □□ □□
C. □□□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□
D. □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□□ □□
Answer: B (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Third-Party Risk Management section.

NEW QUESTION: 80
□□ □□□ □□□ □□□□□ □□□ □□□□ □□□□, □□□ □□□ □□□ □□ □□ □ □□□□ □□□□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□□□□□
C. □□□□□
D. □□ □□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Zero-coupon bonds are issued at a discount to their face (par) value and do not pay periodic interest. Instead, the bond's value increases over time as it accrues interest, reaching its full face value at maturity. Investors receive the total payoff (the face value) upon maturity, which includes the initial investment plus the interest earned over the bond's term. High-yield bonds (also known as junk bonds) offer higher interest rates due to higher risk but pay periodic interest. Commodity-backed bonds are tied to commodity prices and may pay periodic interest. Therefore, zero-coupon bonds fit the described characteristics.

NEW QUESTION: 81
1□ □□ □□□□ □□□ □□□□ S250,000□□ □□□ $30,000□□□. □□□ □□□□ □ 5265,000□□□ □□ □ □□□□□□?
A. 12% □□□□□.
B. 12□□□.
C. 12.01%□□ 12.50% □□.
D. 12 50% □□.
Answer: (SHOW ANSWER)
The market interest rate (yield to maturity, YTM) is calculated using the following formula:

YTM=Coupon Payment+(Face Value#Market PriceYears to Maturity)Face Value+Market Price2YTM = \frac
{\text{Coupon Payment} + \left(\frac{\text{Face Value} - \text{Market Price}}{\text{Years to Maturity}}
\right)}{\frac{\text{Face Value} + \text{Market Price}}{2}}
YTM=2Face Value+Market PriceCoupon Payment+(Years to MaturityFace Value#Market Price) Given:
* Face Value (F) = $250,000
* Coupon Payment (C) = $30,000
* Market Price (P) = $265,000
* Time to Maturity = 1 year
* Calculate the Yield to Maturity (YTM) using the Approximation Formula:
Step-by-Step Calculation:YTM=30,000+(250,000#265,0001)250,000+265,0002YTM = \frac{30,000 + \left(
\frac{250,000 - 265,000}{1} \right)}{\frac{250,000 + 265,000}
{2}}YTM=2250,000+265,00030,000+ (1250,000#265,000)
YTM=30,000+(#15,000)250,000+265,0002YTM = \frac{30,000 + (-15,000)}{\frac
{250,000 + 265,000}{2}}YTM=2250,000+265,00030,000+(#15,000)
YTM=15,000257,500YTM = \frac
{15,000}{257,500}YTM=257,50015,000 YTM=0.0583 or 5.83% (Current Yield)YTM = 0.0583 \text{ or }
5.83\% \text{ (Current Yield)}YTM=0.0583 or 5.83% (Current Yield)
* Convert the YTM to an Annual Percentage Rate:
Since this is a one-year bond, the actual yield to maturity is equivalent to the total return:
Total return=30,000+(#15,000)265,000=15,000265,000\text{Total return} = \frac{30,000 + (-15,000)}
{265,000} = \frac{15,000}{265,000}Total return=265,00030,000+(#15,000)=265,00015,000
YTM=5.66%
+250,000#265,000265,000=12.26%YTM = 5.66\% + \frac{250,000 - 265,000}{265,000} = 12.26\%YTM=5.
66%+265,000250,000#265,000=12.26%
Final Answer:Since 12.26% falls between 12.01% and 12.50%, option (C) is correct.
* IIA GTAG 3: Continuous Auditing - Emphasizes the importance of financial metrics like yield calculations in investment risk assessments.
* COSO ERM Framework - Performance Component - Highlights the significance of market rates in financial decision-making and risk management.
* IFRS 9 - Financial Instruments - Covers bond valuation and interest rate calculations.
IIA References:Conclusion:Since the market interest rate falls between 12.01% and 12.50%, option (C) is the correct answer.

NEW QUESTION: 82

□□ □ □□□□□□□□ □□□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □□□□ □□.
B. □□□□□□ □□□.
C. □□ □□.
D. □□□□.
Answer: B (LEAVE A REPLY)
Data extraction involves retrieving data from various sources for processing or storage. Among the options provided, the database system is the component that facilitates data extraction from an application. Here's why:
A). Application Program Code:
While the application program code defines the logic and functionality of an application, it doesn't inherently provide mechanisms for data extraction. Instead, it interacts with databases to perform operations like data retrieval, insertion, or modification.
B). Database System:
A database system is designed to store, manage, and retrieve data efficiently. It offers structured methods, such as querying with SQL, to extract specific data as needed. Applications rely on the database system to access and extract the required data for various operations. For instance, in a relational database, data extraction is performed using SQL queries that retrieve data based on specified criteria. This process is fundamental to operations like reporting, analytics, and data migration.
teradata.com
C). Operating System:
The operating system manages hardware resources and provides services for application execution but doesn't directly handle data extraction from applications. It ensures that applications have the necessary environment to run but delegates data management tasks to the database systems.
D). Networks:
Networks facilitate data transmission between systems but don't directly extract data from applications. They provide the pathways for data to travel between clients and servers or between different systems but aren't responsible for the extraction process within an application.
In summary, the database system is the component that provides the necessary tools and methods for data extraction within an application, making option B the correct answer.

NEW QUESTION: 83
IT□ □□ IIA □□□ □□□ □□ □ □□□ □□□□ □□□ □□ □□□ □□□ □ □□□ □□□ □□ □□□ □□□□□ □□ □ □□ □□□□□ □□□□ □□ □□□ □□ □ □ □□□ □□ □□□□□?
A. □□ □□ □□
B. □ □□□□ □□
C. □□ □□□□ □□

D. □□ □□□ □□

Answer: D (LEAVE A REPLY)

A disaster recovery plan (DRP) ensures that critical systems and data can be restored after an incident. If backup plans exist but no recovery and restore processes are defined, then the organization lacks a functional recovery plan altogether.

* (A) Hot recovery plan.
* Incorrect. A hot recovery plan includes real-time data replication and immediate failover systems, allowing for almost instant recovery in case of an outage. Since the scenario mentions that no restore process is defined, this cannot be a hot recovery plan.
* (B) Warm recovery plan.
* Incorrect. A warm recovery plan involves regular backups and a standby system that can be activated within hours or days. However, without defined restore procedures, the organization does not even have a warm recovery plan.
* (C) Cold recovery plan.
* Incorrect. A cold recovery plan means that backups exist but recovery takes significant time because systems and infrastructure need to be rebuilt. However, a cold plan still includes a recovery process, which the scenario lacks.
* (D) Absence of recovery plan. #
* Correct. If data backup plans exist but no restore processes are defined, then there is no functional recovery plan. Without a structured approach to data recovery, backups alone are useless in an actual disaster scenario.
* IIA GTAG "Business Continuity and Disaster Recovery" highlights the need for detailed recovery processes as part of an overall disaster recovery plan.
* IIA GTAG - "Business Continuity and Disaster Recovery"
* IIA Standard 2120 - Risk Management
* COBIT Framework - IT Disaster Recovery Controls

Analysis of Answer Choices:IIA References:Thus, the correct answer is D, as data backups without recovery procedures indicate the absence of a recovery plan.

NEW QUESTION: 84

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

A. □□

B. □□

C. □□

D. □□ □□

Answer: B (LEAVE A REPLY)

Reference: IIA Business Knowledge for Internal Auditing, Cybersecurity Risks section.

NEW QUESTION: 85

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

A. □□□□□ □□□□□ □□□□□ □□□□.
B. □□ □□□ □□□□□ □□□□ □□ □□□ □□□□□.
C. □□□□□ □□□ □□□ □□□ □□□ □□□ □□□□□ □□□□□.
D. □□□□□ □□ □□□ □□□ □□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
Managerial accounting differs from financial accounting in that it focuses on internal decision-making, cost control, and performance evaluation based on predetermined standards. Unlike financial accounting, which follows GAAP (Generally Accepted Accounting Principles) for external reporting, managerial accounting sets internal benchmarks to guide operational efficiency and strategic planning.
* Use of Predetermined Standards:
* Managerial accounting often uses standard costing, budgets, and variance analysis to compare actual performance against pre-set benchmarks.
* This helps management make data-driven decisions and improve efficiency.
* Internal Decision-Making:
* Managerial accounting reports are used by internal stakeholders (e.g., managers, executives) rather than external entities.
* Control and Performance Measurement:
* It focuses on variance analysis (actual vs. expected performance) to highlight areas requiring corrective action.
* Not Governed by GAAP:
* Unlike financial accounting, managerial accounting does not require compliance with GAAP or IFRS since it is meant for internal use only.
* A. Managerial accounting uses double-entry accounting and cost data:
* While cost data is relevant to managerial accounting, double-entry accounting is a fundamental principle of all accounting systems, including financial accounting.
* B. Managerial accounting uses generally accepted accounting principles (GAAP):
* GAAP is required for financial accounting (external reporting), but managerial accounting does not follow GAAP since it focuses on internal decision-making.
* C. Managerial accounting involves decision making based on quantifiable economic events:
* While managerial accounting analyzes economic data, its distinguishing feature is using predetermined standards to evaluate and improve performance, which makes Option D the best choice.
* IIA Standard 2110 - Governance: Internal auditors should assess decision-making processes, including managerial accounting techniques.
* IIA Standard 2120 - Risk Management: Cost control and budget variance analysis are key components of risk management.
* COSO Framework - Performance Monitoring: Emphasizes variance analysis, which aligns with predetermined standards in managerial accounting.

Key Reasons Why Option D is Correct:Why Other Options Are Incorrect:IIA References:Thus, the correct answer is D. Managerial accounting involves decision making based on predetermined standards.

NEW QUESTION: 86
□□ □ □□□ □□□ □□ □□□□ □□□□□?
A. □□.
B. □□□ □□□ □□□□(PRINCE2).
C. □□ □□ □□□ □□□□□(ITIL).
D. □□
Answer: A (LEAVE A REPLY)
A systems development methodology refers to a structured approach used in software development and systems engineering to guide the design, development, and implementation of software applications.
* Why Option A (Waterfall) is Correct:
* Waterfall methodology is a linear and sequential systems development methodology where each phase (e.g., requirements, design, implementation, testing, deployment) must be completed before moving to the next.
* It is widely established and historically one of the first software development methodologies.
* Used in large-scale enterprise projects where detailed planning and structured execution are required.
* Why Other Options Are Incorrect:
* Option B (PRINCE2 - Projects in Controlled Environments):
* Incorrect because PRINCE2 is a project management framework, not a systems development methodology.
* Option C (ITIL - Information Technology Infrastructure Library):
* Incorrect because ITIL is a set of IT service management (ITSM) best practices, not a software development methodology.
* Option D (COBIT - Control Objectives for Information and Related Technologies):
* Incorrect because COBIT is a governance framework for IT management and controls, not a development methodology.
* IIA GTAG - "Auditing IT Projects and Systems Development": Highlights Waterfall as a traditional systems development methodology.
* IIA's Global Technology Audit Guide on IT Risks: Discusses software development lifecycle risks, including Waterfall methodology.
* COBIT Framework - BAI03 (Manage Solutions Identification and Build): References structured methodologies like Waterfall in IT governance.
IIA References:

NEW QUESTION: 87

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

1. □□□ □□ □□□ □□.
2. □□□ □□□ □□.
3. □□□ □□ □□□ □□.
4. □□□ □□□ □□.

A. 1 □ 2

B. 1 □ 4

C. 3 □ A

D. 2 □ 3

Answer: A (LEAVE A REPLY)

* Understanding Labor Variances in Cost Accounting:
* Labor efficiency variance measures the difference between the actual hours worked and the standard hours allowed for actual production.
* Labor rate variance measures the difference between the actual labor cost per hour and the standard rate set for labor.
* Why Options 1 (Favorable Labor Efficiency Variance) and 2 (Adverse Labor Rate Variance) Are Correct?
* Favorable Labor Efficiency Variance (1):
* Hiring more experienced researchers should lead to higher productivity, meaning that the team completes tasks faster, reducing the total labor hours required.
* This results in a favorable labor efficiency variance because less time is spent on the project than initially expected.
* Adverse Labor Rate Variance (2):
* More experienced employees command higher salaries, leading to an increase in labor costs per hour compared to the budgeted rate.
* This results in an adverse labor rate variance because the actual wage rate exceeds the standard rate.
* Why Other Options Are Incorrect?
* Option 3 (Adverse Labor Efficiency Variance):
* This would occur if the new hires were less productive, which contradicts the scenario.
* Option 4 (Favorable Labor Rate Variance):
* A favorable variance in labor rate occurs when labor costs are lower than expected, which is unlikely when hiring more experienced (higher-paid) employees.
* Hiring more experienced employees improves efficiency (favorable efficiency variance) but increases wages (adverse rate variance).
* IIA Standard 1220 - Due Professional Care requires auditors to consider operational efficiency in decision-making evaluations.

Final Justification:IIA References:

* IPPF Standard 1220 - Due Professional Care

* IIA Practice Guide - Assessing Business Performance Metrics

NEW QUESTION: 88
□□ □□□ □□□□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□ □ □ □□□ □□□ □□□□□□. □□ □□□□ □□□□□ □□ □□ □□□□□ □□ □□ □□ □□□ □□□□ □□□ □□□□ □ □□□□. □□ □ □□□ □□ □□□ □□ □ □ □□ □□?
A. □□.
B. □□.
C. □□□.
D. □□.
Answer: C (LEAVE A REPLY)
* Descriptive Analytics - Answers "What happened?" by summarizing past data.
* Diagnostic Analytics - Answers "Why did it happen?" by identifying causes of trends or issues.
* Prescriptive Analytics - Answers "What should we do?" by providing data-driven recommendations and optimal solutions for decision-making.
* Prolific Analytics - This is not a recognized category in standard analytics models.
* The model makes specific recommendations for store operations (extended hours, staffing adjustments).
* It optimizes resource allocation based on demand patterns.
* It goes beyond identifying past trends (descriptive) or diagnosing causes (diagnostic) and provides actionable solutions.
* A. Descriptive - Would only summarize sales data but not suggest changes.
* B. Diagnostic - Would explain why luxury stores see higher traffic on weekends but would not recommend actions.
* D. Prolific - Not a standard analytics category.
* IIA's GTAG on Data Analytics - Describes prescriptive analytics as the highest level of business intelligence, driving decision-making.
* COSO's Enterprise Risk Management (ERM) Framework - Encourages data-driven decision- making using prescriptive models.
* COBIT 2019 on IT Governance - Recommends leveraging prescriptive analytics for operational efficiency.
Types of Analytical Models in Business Intelligence:Why Prescriptive Analytics is the Best Choice?Why Not the Other Options?IIA References:# Final Answer: C. Prescriptive.

NEW QUESTION: 89
□□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□
B. □□ □□□□ □□□ □□□□□ □.
C. □□□ □□□ □□ □.

D. □□ □□□ □□□ □□.

Answer: (SHOW ANSWER)

A contract is closed out when all the contractual terms have been fully satisfied, including the completion of deliverables, final payments, and any post-contract evaluations or obligations.

* Correct Answer (B - When all contractual obligations have been discharged)
* According to contract management principles and IIA standards, a contract is officially closed out once:
* All agreed-upon deliverables have been completed.
* All payments and financial obligations are settled.
* Final performance evaluations or audits are completed.
* The contract is formally reviewed and documented for closure.
* The IIA's GTAG 3: Contract Management Framework supports that contract closure occurs after full performance and obligations are met.
* Why Other Options Are Incorrect:
* Option A (When there's a dispute between contracting parties):
* Disputes do not necessarily close out a contract; instead, they may lead to mediation, renegotiation, or legal action. The contract remains active until resolved.
* The IIA's Practice Guide: Auditing Contracts recommends dispute resolution mechanisms but does not define them as a reason for contract closure.
* Option C (When there is a force majeure event):
* A force majeure (unforeseen event like natural disasters or war) may suspend or modify contractual obligations but does not always lead to closure.
* The contract may be renegotiated or resumed once conditions allow.
* Option D (When the termination clause is enacted):
* Termination and closure are not the same. Termination means ending the contract before full obligations are met, whereas closure means fulfilling all obligations.
* IIA GTAG 3: Contract Management Framework explains that contract termination can occur under specific clauses, but closure happens only after all duties are fulfilled.
* IIA GTAG 3: Contract Management Framework - Covers contract lifecycle, including closeout procedures.
* IIA Practice Guide: Auditing Contracts - Details contract auditing, dispute resolution, and obligations fulfillment.

Step-by-Step Explanation:IIA References for Validation:

NEW QUESTION: 90

□□□ □□□ □□□ □□ □□□ □□ 8□□□ □□□□ □□ □□□□. □□□ □□ □□ □ □□□ □□□□□, □□ □□ □ □□ □□ □□□□□?

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

B. □□□□ □□□□ □□, □□, □□□ □□□□□.

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

D. □□□ □□□ □□ □□□ □□□ □□□□

Answer: B (LEAVE A REPLY)

Reference: IIA Business Knowledge for Internal Auditing, Organizational Structure and Culture section.

NEW QUESTION: 91

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

A. □□ □□

B. □□,

C. □□.

D. □□ □□.

Answer: D (LEAVE A REPLY)

Social engineering is a psychological manipulation technique used by attackers to trick individuals into divulging sensitive information. Instead of exploiting technical vulnerabilities, it targets human weaknesses such as trust, fear, or urgency.

* Manipulates Human Behavior - The attacker impersonates a trusted entity (a bank representative) to deceive the employee.
* Leads to Unauthorized Information Disclosure - The employee unknowingly provides sensitive financial data.
* Results in Fraud - The stolen information is misused, causing financial loss.
* A. Shoulder Surfing - This occurs when an attacker physically observes someone entering sensitive data (e.g., watching a person type a password).
* B. Pharming - This involves redirecting users to a fraudulent website to steal their credentials, not direct impersonation.
* C. Phishing - This is a broad category of social engineering that typically involves emails or fake websites, whereas this scenario describes a direct impersonation attack.
* IIA's GTAG on Cybersecurity - Discusses social engineering as a key risk for organizations.
* NIST SP 800-61 (Incident Handling Guide) - Identifies social engineering as a common attack vector.
* COBIT 2019 (IT Governance Framework) - Highlights human-related cybersecurity risks.

Why Social Engineering is the Correct Answer?Why Not the Other Options?IIA References:

NEW QUESTION: 92
□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□. □□ □ □□□ □□ □□□ □□□ □□□□ □□□□ □□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□ □ □□ □□□□ □□□□□.
B. □□ □□ □□□□ □□□□□ □□ □□□ □□□□□ □□□□ □□
C. □□□ □□□□□ □□ □□□ □□□□ □□□ □□ □□.
D. □□□ □□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
When conducting a cybersecurity risk assessment, an internal auditor must evaluate the most significant threats based on their potential impact on the organization. In the pharmaceutical industry, intellectual property (IP), such as research and development (R&D) data, is one of the most valuable and sensitive assets.
* (A) Cybercriminals hacking into the organization's time and expense system to collect employee personal data:While the loss of employee personal data is a serious concern due to privacy and regulatory implications (e.g., GDPR, CCPA), it does not pose as critical a threat as the loss of proprietary pharmaceutical research.
* (B) Hackers breaching the organization's network to access research and development reports (Correct Answer):R&D reports contain proprietary drug formulas, clinical trial results, and patent- pending innovations, making them highly valuable to competitors and cybercriminals. A breach could lead to intellectual property theft, financial losses, loss of competitive advantage, and regulatory non- compliance (e.g., FDA, EMA requirements). This is considered the most significant threat because:
* It could result in billions of dollars in lost revenue.
* Competitors or state-sponsored hackers could exploit stolen research.
* It could disrupt drug development and approval processes.
* (C) A denial-of-service (DoS) attack that prevents access to the organization's website:While DoS attacks can damage an organization's reputation and disrupt operations, they generally do not cause the same level of financial or strategic harm as the loss of critical R&D data. Most organizations have cybersecurity measures (e.g., load balancers, CDNs) to mitigate DoS risks.
* (D) A hacker accessing the financial information of the company:Unauthorized access to financial data can be serious, leading to fraud or reputational damage. However, publicly traded companies already disclose much of their financial data, and financial breaches typically have a lower long-term impact compared to intellectual property theft.
* IIA Global Technology Audit Guide (GTAG) 15: Information Security Governance: Recommends that internal auditors prioritize risks that impact strategic assets, such as intellectual property.

* IIA Standard 2120 - Risk Management: Requires internal auditors to evaluate the organization's risk management processes, emphasizing risks with significant financial and operational consequences.
* IIA Practice Advisory 2110-2: Assessing the Adequacy of Risk Management Processes: Highlights that internal auditors must identify risks that could threaten the organization's long-term objectives, such as IP theft.
* COSO ERM Framework: Encourages prioritization of risks that have high impact on an organization' s value and strategic objectives, such as cyber threats to proprietary research.
Analysis of Each Option:IIA References:Conclusion:Given the pharmaceutical industry's reliance on proprietary R&D, a breach compromising research reports represents the most significant cyber threat.
Therefore, option (B) is the correct answer.

NEW QUESTION: 93
□□ □ □□□□ □□ □□ □□□ □□□ □□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□□□.
B. □□□ □□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□.
C. □□ □□ □□ □□□ □□ □□□ □□ □ □□□ □□ □□□□□.
D. □□□□ □ □□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Preventive security controls proactively stop unauthorized access before it occurs. The most effective method is strict access management, where new or additional access rights require formal validation before being granted.
* Prevents Unauthorized Entry - Ensures that only approved personnel have access to the power plant.
* Implements Segregation of Duties (SoD) - Supervisors validate access requests, reducing insider threats.
* Aligns with Least Privilege Principle - Employees get only the minimum access necessary for their role.
* Prevents Security Risks Before They Happen - Unlike detective or corrective controls, this method stops unauthorized access before it occurs.
* A. Offboarding procedure (monthly review) - This is a detective control, identifying issues after access is granted, not preventing them.
* B. Smart lock anomaly scanning - Also detective, as it identifies suspicious behavior after access has been used.
* D. Automatic notifications for after-hours entry - A corrective control, responding to potential violations instead of preventing them.
* IIA's GTAG on Identity and Access Management - Recommends pre-approval processes for sensitive locations.
* ISO 27001 Annex A.9 (Access Control) - Requires role-based access management for critical infrastructures.

* NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems) - Defines supervisor approval as a key preventive measure.
Why Approval-Based Access Control is the Best Preventive Measure?Why Not the Other Options?IIA References:

NEW QUESTION: 94
IT□ □□ IIA □□□ □□□ □□ □□ □ □□□ □□□□ □□□□ □□□ □□ □□ □□ □ □□□□ □□□ □□□□□?
A. □□□□ □□□ □□ □□.
B. □□□□ □□□ □□ □□ □□.
C. □□□□ □□□ □□ □□
D. □□ □□□ □□□ □□ □□ □□
Answer: C (LEAVE A REPLY)
The Business Impact Analysis (BIA) plan is a key component of business continuity planning that identifies critical business processes and determines their Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
* Correct Answer (C - Business Impact Analysis Plan)
* The BIA is a systematic process that identifies essential functions, assesses potential disruptions, and determines the recovery time requirements to ensure business continuity.
* The Recovery Time Objective (RTO) defines the maximum acceptable downtime for critical business functions.
* The Recovery Point Objective (RPO) identifies how much data loss is tolerable.
* According to the IIA Global Technology Audit Guide (GTAG) 10: Business Continuity Management, a BIA is essential for assessing the financial, operational, and reputational impact of disruptions.
* Why Other Options Are Incorrect:
* Option A (Business Continuity Management Charter):
* A charter defines the governance, responsibilities, and overall framework of business continuity but does not focus on RTOs or critical business processes.
* Option B (Business Continuity Risk Assessment Plan):
* A risk assessment identifies threats and vulnerabilities but does not define recovery time objectives.
* While risk assessments inform the BIA, they do not replace it.
* Option D (Business Case for Business Continuity Planning):
* A business case justifies investment in continuity planning but does not map business processes to RTOs.
* GTAG 10: Business Continuity Management - Defines BIA as the process for identifying critical business functions and their RTOs.
* IIA Practice Guide: Auditing Business Continuity - Emphasizes the role of BIA in business resilience.

Step-by-Step Explanation:IIA References for Validation:Thus, the Business Impact Analysis (BIA) Plan (C) is the correct answer because it pairs critical business processes with recovery time objectives.

NEW QUESTION: 95
□□ □□□ □□□□ □□□□ □□□ 24□□ □□□ □□□□ □□□□ □□ □□□□□ □□ □□□□□. □□ □□□□ □ □□□ □□ □□□□□ □□□ □□□ □□□ □□□□ □□□ □□□?
A. □3□ □□ □□ □□□.
B. □□□ □□ □□□□□.
C. □□□ □□□ □□ □□.
D. □□□□ □□ □□□ □□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
□□ □□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□ □□ □□□□□ □ □□□ □□□□□?
A. □□□□ □□
B. □□ □□□ □□
C. □□□□□
D. □□ □□
Answer: C (LEAVE A REPLY)
A zero-coupon bond is a type of bond that sells at a discount from its face value and gradually increases in value over time until maturity when the bondholder receives the full face value. Unlike regular bonds, zero-coupon bonds do not pay periodic interest (coupons) but instead accumulate interest over the bond's life.
Let's analyze each option:
* Option A: High-yield bonds
* Incorrect.
* High-yield bonds (junk bonds) offer higher interest rates due to higher risk but pay periodic interest rather than being sold at a discount and growing in value over time.
* Option B: Commodity-backed bonds
* Incorrect.
* Commodity-backed bonds are linked to the price of a commodity (e.g., gold, oil) rather than increasing in value over time from an initial discount.
* Option C: Zero coupon bonds
* Correct.
* These bonds are issued at a discount and increase in value each year as interest accrues.
* The investor receives the full face value at maturity, which includes the principal and accumulated interest.

* IIA Reference: Internal auditors evaluate investment risks, including bond valuation and discount amortization. (IIA Practice Guide: Auditing Investment and Treasury Functions)
* Option D: Junk bonds
* Incorrect.
* Junk bonds are simply high-risk, high-yield bonds that pay interest periodically and do not necessarily sell at a deep discount.
Thus, the verified answer is C. Zero coupon bonds.

NEW QUESTION: 97
□ □□ □□□ □□□ □□ □□□ $10,000□ □□□ □□□ □□□□□□. □□□ □□ □ □□ □□ □□□ □□□□□?
A. □□□□□ □□□□□□ □□□□□.
B. □□□□□ □□□□□□ □□□□□□□□□.
C. □□□□□ □□□□□□ □□□ □□□□□□ □□□.
D. □□□□□ □□□□□□ □□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
When inventory is understated (not included in the physical count) at year-end, the financial impact affects both cost of sales (COGS) and net income as follows:
* Correct Answer (C - Cost of Sales is Understated and Net Income is Overstated)
* The ending inventory is part of the formula used to calculate the cost of goods sold (COGS):
COGS=BeginningInventory+Purchases#EndingInventoryCOGS = Beginning Inventory + Purchases - Ending InventoryCOGS=BeginningInventory+Purchases#EndingInventory
* If ending inventory is understated, then:
* COGS will be understated (because inventory that should have been counted as sold was omitted).
* Net income will be overstated because COGS is lower than it should be, making profits appear higher.
* This error causes financial misstatements, violating IIA auditing standards for financial accuracy.
* Why Other Options Are Incorrect:
* Option A (Cost of sales and net income are understated):
* Net income would not be understated-it would be overstated because the cost of goods sold is too low.
* Option B (Cost of sales and net income are overstated):
* COGS would be understated, not overstated. If COGS were overstated, net income would be understated.
* Option D (Cost of sales is overstated and net income is understated):
* The opposite happens-COGS is understated and net income is overstated.
* IIA GTAG 8: Audit of Inventory Management - Covers financial impact of inventory misstatements.

* IIA Practice Guide: Auditing Financial Statements - Addresses common inventory errors and financial reporting impacts.
Step-by-Step Explanation:IIA References for Validation:Thus, C is the correct answer because an understated inventory reduces COGS and inflates net income.

NEW QUESTION: 98
□□□□□□□(CAE)□ □□□ □ □□ □□□ □□□□□, □□ □□□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□□□. □ □□□□ CAE□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□□□ □□□□□.
B. □□ □□ □□□□□ □□□ □□□ □□ □□ □□□ □□□□□□.
C. □□ □□□ □□□□ □□□□□.
D. □□ □□ □□□□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)
When internal audit identifies a risk that appears unacceptable, the CAE should first discuss the matter with the responsible management. This ensures management has an opportunity to explain their rationale or adjust actions before escalation.
Option A (direct escalation to senior management) or Option C (to the board) are appropriate only if management refuses to act. Option B (sending a letter with a deadline) is not aligned with IIA guidance.
Reference:
IIA Standards - Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 99
□□ □ □□ □□ □□ □□□□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□ □□
B. □□□□ □□ □□□ □□□ □□□ □ □□□ □□ □□
C. □ □□□ □□□ □□□□ □□ □□
D. □□□□ □□□□□□□ □□□□ □□□ □ □□ □□□ □□
Answer: B (LEAVE A REPLY)
The internal audit procedures manual documents policies and procedures for conducting audit engagements, including steps to follow when issues arise, such as disputes with management regarding findings. It ensures consistency and standardization of audit practice.
Option A (strategic plan) and Option C (resources) are not part of audit procedures but rather part of planning or organizational documents. Option D (authority to collect data) belongs in the internal audit charter, not in the procedures manual.
Therefore, the correct answer is appropriate response options for disputes with management (Option B).
Reference:
IIA Practice Guide - Developing the Internal Audit Manual.

NEW QUESTION: 100
IT□ □□ 11A □□□ □□□ □□ □□□□□□ □ □□□ □□□ □□ □□ □□□□□□ □□□ □□□□ □□ □□ □□□□□□□ □□□□□?
A. □□ □□□ □□ □ □□ □□□□ □□ □□□□ □□ □□ □□□□□□□□□.
B. □□ □□□ □□□□ □□□ □□ □□ □□ □□□□□□.
C. □□□ □□ □□□ □□□□□ □□□□ □□ □□ □□ □□□□□□.
D. □□ □□□□ □□□ □□□□ □ □□□□ □□□ □□ □□□□□□
Answer: B (LEAVE A REPLY)
A high-risk user-developed application (UDA) refers to spreadsheets or other tools created and maintained by end-users (not IT) that are critical to financial reporting, decision-making, or regulatory compliance. The IIA guidance on IT risk management emphasizes evaluating the complexity, significance, and control environment of such applications.
* (A) Revenue Calculation Spreadsheet
* Uses price and volume reports from production, meaning it relies on structured, external sources, reducing the risk of significant undetected errors.
* Less complexity and external verification reduce its risk level.
* (B) Asset Retirement Calculation Spreadsheet (Correct Answer)
* Contains multiple formulas and assumptions, making it complex and prone to errors.
* Assumptions introduce subjectivity and risk of incorrect calculations, affecting financial statements and compliance.
* No automated controls or independent validations, making it a high-risk UDA.
* IIA Standard 2110 - Governance and GTAG 14 (Auditing User-Developed Applications) emphasize assessing high-risk spreadsheets that impact financial decision-making.
* (C) Ad-Hoc Inventory Listing Spreadsheet
* Used for written-off inventory, which is historical data and not a key financial driver.
* Limited impact on financial reporting, making it a low-risk UDA.
* (D) Accounts Receivable Reconciliation Spreadsheet
* Used by the accounting manager to verify balances, likely cross-checked with ERP or other financial systems.
* Since external reconciliation exists, the spreadsheet does not pose a high inherent risk.
* GTAG 14 (Auditing User-Developed Applications) - Identifies UDAs with complex formulas, financial impact, and lack of controls as high-risk.
* IIA Standard 2110 (Governance) - Internal auditors must assess governance around financial and operational risk management, including IT risks.
* IIA Standard 2120 (Risk Management) - Emphasizes identifying and mitigating risks from user- developed applications.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (B) Asset Retirement Calculation Spreadsheet, as it aligns with IIA guidance on high-risk spreadsheets due to complex formulas, assumptions, and potential financial misstatements.

NEW QUESTION: 101
□□ □□ □□ □ □□ □□ □□□ □□ □□ □□□ □□□□□□ □□ □ □□□□□?
A. □□□ □□□□
B. □□
C. □□ □□
D. □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Gain sharing is a compensation program where employees receive bonuses tied directly to the company's cost- saving measures and productivity improvements. This approach aligns employees' interests with organizational goals by rewarding them for identifying and implementing efficiencies that reduce costs.
Unlike profit sharing, which is based on overall profitability, gain sharing focuses specifically on performance improvements that lead to cost savings. Commissions are typically related to sales performance, and pensions are long-term retirement benefits not directly linked to immediate cost-saving efforts. Therefore, gain sharing is the most indicative of targeting cost-saving objectives.

NEW QUESTION: 102
□□□□□□□(CAE)□ □□□□ □□□ □ □□□ □□□□□□. □□ □□ □□ □□ □ □□ □□□□ □□□ □□ □□ □□ □□□□. □□□ □□ □□□□□□□□ □□ □, CAE□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□ □□□. CAE□ □□□ □□□□ □□□?
A. □□□□□ □□ □□□□□□ □□ □□ □□ □□□ □□□□□ □□□□□.
B. □□ □□□ □□□ □□□□ □□ □□□ □□□□, □□ □ □□□ □□ □□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□ □□ □□ □□□ □□□□□ □□□□.
D. □□□ □□□ □□□ □□□□ □□□□□ □□ □□ □□ □□□ □□□□□ □□ □□ □□ □□□□□.
Answer: B (LEAVE A REPLY)
The IIA Standards emphasize that the internal audit plan must remain dynamic and responsive to changes in risks and priorities. If significant risks are identified after the plan has been approved, the CAE must revise the plan and communicate the interim changes to senior management and the board for review and approval.
Option A ignores emerging risks. Option C delays addressing significant risks. Option D bypasses governance approval and does not respect the board's oversight role.
Reference:
IIA Standards - Standard 2020: Communication and Approval.

NEW QUESTION: 103

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

A. □□□□ □□ □□□ □□□□□□.

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

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

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

Answer: (SHOW ANSWER)

Data cleaning and normalization are essential steps in the data analytics process to ensure that data is accurate, complete, and useful for analysis. The primary purpose of these steps is to identify and correct anomalies, inconsistencies, and errors, making the data usable for decision-making.

* (A) The auditor eliminated duplicate information. #
* Incorrect. Removing duplicates is one part of data cleaning, but it does not encompass the full process of making data usable.
* (B) The auditor organized data to minimize useless information. #
* Incorrect. While organizing data helps improve efficiency, it does not necessarily involve error detection and correction, which is key to data cleaning.
* (C) The auditor made data usable for a specific purpose by ensuring that anomalies were identified and corrected. #
* Correct. The primary goal of cleaning and normalizing data is to detect and fix anomalies (e.
g., missing values, inconsistencies, formatting errors), ensuring that data is reliable for analysis.
* IIA GTAG "Data Analytics: Elevating Internal Audit Performance" highlights that correcting data anomalies is a critical step in preparing data for effective use.
* (D) The auditor ensured data fields were consistent and that data could be used for a specific purpose. #
* Incorrect. While consistency in data fields is part of normalization, it does not fully address the broader purpose of identifying and fixing errors.
* IIA GTAG - "Data Analytics: Elevating Internal Audit Performance"
* IIA Standard 2320 - Analysis and Evaluation
* NIST Data Quality Framework - Data Cleaning and Normalization

Analysis of Answer Choices:IIA References:Thus, the correct answer is C, as data cleaning and normalization ensure that anomalies are detected and corrected, making the data usable for a specific purpose

NEW QUESTION: 104

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

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

B. □□□ □□ □□□ □□□□ □□ □□ □□□□.

C. □□□ □□□□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□ □□□□ □□□
Answer: C (LEAVE A REPLY)
A transformational leader focuses on inspiring and motivating employees to exceed expectations, emphasizing vision, innovation, and long-term goals rather than just rule enforcement or performance monitoring.
* (A) The leader searches for deviations from the rules and standards and intervenes when deviations exist.
* Incorrect: This describes a transactional leader, who focuses on correcting errors and enforcing rules rather than inspiring employees.
* (B) The leader intervenes only when performance standards are not met.
* Incorrect: This describes a passive transactional leader, who waits for issues before taking action.
* (C) The leader intervenes to communicate high expectations. (Correct Answer)
* Transformational leaders set high expectations, inspire employees to achieve them, and foster a culture of continuous improvement.
* IIA Standard 2110 - Governance highlights the importance of leadership in driving organizational performance.
* Transformational leadership aligns with COSO's principles of strong governance and strategic vision.
* (D) The leader does not intervene to promote problem-solving.
* Incorrect: A transformational leader actively promotes problem-solving by encouraging innovation and continuous improvement.
* IIA Standard 2110 - Governance: Recognizes leadership's role in fostering a strong ethical and performance-driven culture.
* COSO ERM - Governance and Culture: Highlights leadership's role in shaping strategic direction.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (C) because a transformational leader inspires employees by setting high expectations and motivating them to achieve organizational goals.

NEW QUESTION: 105
□□ □ □□□ □□ □□ □□□ □□□□ □□□ □□ □ □□□ □□?
A. □□□□□□ □□ □□□ □□ □ □□ □□□ □□□ □□
B. □□□□ □□□ □□ □□ □□□ □□□ □□
C. □□□□ □□□ □□ □□ □□□ □□□□ □□
D. □□□□ □□□□□ □□□ □□□□□□□□ □□ □□□□ □□□□ □
Answer: D (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Leasing and Financial Management section.

NEW QUESTION: 106

□□ □ □□ □□□ □□□ □□ □ □□□ □□?

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

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

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

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

Answer: B (LEAVE A REPLY)

* Understanding Predictive Analytics:
* Predictive analytics involves using historical data, statistical algorithms, and machine learning techniques to forecast future trends and behaviors.
* It applies assumptions and models patterns to predict outcomes, helping businesses make proactive decisions.
* Why Option B is Correct:
* Predictive analytics is forward-looking and uses assumptions (e.g., weather conditions) to predict where stock levels would decrease more quickly.
* This aligns with the goal of predictive analytics: forecasting potential events before they occur.
* Why Other Options Are Incorrect:
* A. Analyzed instances where parts were out of stock before scheduled deliveries: This is descriptive analytics, as it looks at past data without making future predictions.
* C. Analyzed past stockouts and found a correlation with stormy weather: This is diagnostic analytics, as it identifies past correlations but does not predict future trends.
* D. Modeled different scenarios for stock reordering and delivery decisions: This is prescriptive analytics, which focuses on decision-making rather than predictions.
* IIA Standards and References:
* IIA GTAG on Data Analytics (2017): Highlights predictive analytics as a tool for forecasting risks and operational inefficiencies.
* IIA Standard 1220 - Due Professional Care: Encourages auditors to use analytical techniques to anticipate potential issues.
* COSO ERM Framework: Supports the use of predictive models to improve risk management and strategic planning.

Thus, the correct answer is B: A supplier of electrical parts analyzed sales, applied assumptions related to weather conditions, and identified locations where stock levels would decrease more quickly.

NEW QUESTION: 107
□□ □□□□ □□□□□ □□ □□□□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□□□? □□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□ □□□ □□□□ □ □□ □□ □□□□□?
A. □□ □□□.
B. □□ □□
C. □□□□ □□.
D. □□□ □□
Answer: C (LEAVE A REPLY)
Earned Value Analysis (EVA) is a project management technique that integrates scope, time, and cost data to measure project performance and progress objectively. EVA allows internal auditors to assess whether a software development project is on track by comparing planned work with completed work and actual costs.
Here's why EVA is the most appropriate choice:
* Evaluates Project Progress and Performance - EVA measures how much work has been completed against the planned schedule and budget, helping auditors analyze project efficiency.
* Identifies Deviations - It highlights cost overruns or delays in task completion, which is critical for software development projects.
* Uses Key Metrics - EVA includes essential indicators like:
* Planned Value (PV) - The budgeted cost of work scheduled.
* Earned Value (EV) - The value of actual work performed.
* Actual Cost (AC) - The real cost incurred for work completed.
* Schedule Variance (SV) and Cost Variance (CV) - Indicators of deviations from planned performance.
* Supports Risk-Based Internal Audit Approach - The IIA emphasizes risk-based auditing, and EVA helps auditors assess risks related to project cost overruns, schedule slippage, and performance gaps.
* A. A Balanced Scorecard - This measures overall organizational performance across perspectives (financial, customer, internal processes, and learning & growth), but it is not specifically designed for evaluating project task completion.
* B. A Quality Audit - This focuses on compliance with quality standards and does not measure project task completion efficiency.

* D. Trend Analysis - This evaluates patterns over time but does not provide a structured measurement of project progress in terms of cost, time, and completion percentage.
* The IIA's GTAG (Global Technology Audit Guide) on IT Project Management - Recommends using earned value analysis for project auditing.
* IIA's International Professional Practices Framework (IPPF) - Performance Standard 2120 (Risk Management) - Emphasizes the need for internal auditors to evaluate the effectiveness of project risk management, which EVA supports.
* COSO's Enterprise Risk Management (ERM) Framework - Encourages structured performance measurement techniques like EVA to monitor projects.
Why Not the Other Options?IIA References:Thus, Earned Value Analysis (EVA) is the correct answer because it provides a precise, quantitative way to measure project performance. #

NEW QUESTION: 108
□□ □ □□□□□ □□□□ □□ □□ □□?
A. □□□□□ □□□□□ □□ □□□ □□□□.
B. □□□□ □□ □□□ □□□□□ □□ □□□ □□□□.
C. □□□□□ □□ □□□ □□□ □□□□ □ □□□ □□□□.
D. □ □□□□ □□□ □□□□□□ □□□ □□ □□□□ □□□□.
Answer: (SHOW ANSWER)
Big data refers to extremely large and complex datasets that require advanced analytics to extract insights.
Effective visualization is a crucial step in making big data analytics actionable.
Let's analyze the options:
* A. Big data is often structured.
* Incorrect. Big data can be structured, semi-structured, or unstructured. Many sources of big data (e.g., social media, sensor data, emails) are unstructured, making analysis more challenging.
* B. Big data analytic results often need to be visualized. # (Correct Answer)
* Correct. Due to its complexity, big data analytics results must often be visualized using dashboards, charts, or graphs to communicate insights effectively.
* Examples of visualization tools include Tableau, Power BI, and Google Data Studio.
* C. Big data is often generated slowly and is highly variable.
* Incorrect. Big data is typically generated rapidly and continuously (e.g., social media posts, IoT sensors, financial transactions). This relates to the "velocity" characteristic of big data.
* D. Big data comes from internal sources kept in data warehouses.
* Incorrect. Big data comes from both internal and external sources, including social media, cloud applications, and sensors. Additionally, data warehouses store structured data, whereas big data is often unstructured and stored in data lakes.

* IIA GTAG - Auditing Big Data Analytics - Explores best practices for analyzing and visualizing big data.
* COSO ERM Framework - Technology & Data Risk - Discusses the need for big data governance and visualization.
* ISO/IEC 27032 - Cybersecurity and Data Analytics - Covers big data security and interpretation.
* IIA Standard 2120 - Risk Management in Big Data Analytics - Focuses on internal auditors' role in overseeing data-driven decision-making.
IIA References:

NEW QUESTION: 109
□□□□ □□□ □ □□ □□□□ □□ □ □□ □□ □□□□□?
A. □□□□□□(EVM).
B. □□ □□.
C. □□ □□.
D. □□□□ □□ □□ □□□(PMIS).
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
A Project Management Information System (PMIS) is a centralized tool used throughout a project's planning, execution, and monitoring phases. It helps track schedules, costs, and risks.
Option A (EVM) - Used primarily in monitoring and control phases, not all three.
Option B (Organizational procedures) - Provides guidance but is not actively used in all project phases.
Option C (Performance measurement) - Important in monitoring, but not central to planning or execution.
Since PMIS is used throughout the project lifecycle, Option D is correct.
Reference: IIA Project Management - Tools & Techniques

NEW QUESTION: 110
□□ □□□□ □□□ 1,000□□ □□□ □□□□. □□□ □□ □□□ 10□□□□ □□ □ □□
$4; □□□ □□ □□ □□□ $5□□□. □□□ □□□ □□ □□(□□ □□)□ □□□□□?
A. $0
B. $4,000
C. $5,000
D. $10,000
Answer: C (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Inventory Valuation section.

NEW QUESTION: 111

□□ □□□□□□□(CAE)□ □□□□ □□□ □□ □□ □□□ □□□□ □□□□. □ □ □ □□□ □□ □□□□□ □□□□□ □□□□□□ □□ □□□□ □□□□□. □□ □□ □ □□□□ □□□□ □□ □□□ □ □□□□. □ □□□□ □□ □ □□ □□□ □□□ □ □□□□?

A. CAE□ □□□ □□

B. □□□ □□ □□

C. □□□ □□ □□ □□

D. □□□ □□ □□ □□

Answer: (SHOW ANSWER)

The CAE should use the organization's risk acceptance policy to determine when unimplemented audit recommendations represent risks that exceed acceptable tolerance. This ensures consistency with governance frameworks and prevents reliance solely on personal judgment.

Option A lacks formal criteria and would not ensure consistency. The code of conduct (Option B) addresses ethical behavior, not risk acceptance. The audit charter (Option D) defines internal audit's authority and responsibility but does not guide which issues must be escalated.

Reference:

IIA Standards - Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 112

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

A. □□ □□□ □□□□□.

B. □□ □□□□ □□□ □□.

C. □□□ □□□ □□□□□.

D. □□□ □□□ □□.

Answer: B (LEAVE A REPLY)

When multiple organizations co-own shopping malls, their primary strategy is to increase market synergy, meaning they combine resources and expertise to enhance market presence, attract more customers, and improve competitive positioning.

* (A) To exploit core competence.
* Incorrect: Core competencies refer to unique internal capabilities, whereas co-owning shopping malls is a collaborative market strategy.
* (B) To increase market synergy. (Correct Answer)
* Market synergy occurs when businesses collaborate to create greater market impact than they could individually.
* Shared ownership enhances customer traffic, brand reach, and business opportunities.
* IIA Standard 2110 - Governance highlights the importance of strategic partnerships in achieving synergy.
* (C) To deliver enhanced value.

* Incorrect: While value is a benefit, the main goal of co-ownership is strategic market advantage and synergy.
* (D) To reduce costs.
* Incorrect: Cost reduction may be a secondary benefit, but the primary goal is market synergy through shared resources and customer base expansion.
* IIA Standard 2110 - Governance: Encourages strategic collaborations for business growth.
* COSO ERM - Strategy and Objective-Setting: Highlights market synergy as a key factor in strategic partnerships.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (B) because co- ownership of shopping malls primarily aims to increase market synergy, allowing organizations to leverage shared resources and customer networks for greater market impact.

NEW QUESTION: 113
□□ □□ □□ □ □□□ □□□ □□ □□□ □□□□□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
During the initiation phase of contracting, the organization assesses whether the market conditions, supplier capabilities, and contract objectives align with the strategic goals and operational needs of the organization.
This phase is critical because it sets the foundation for the entire contracting process, ensuring that the business environment, risks, and potential opportunities are well understood before proceeding.
* Market Analysis & Alignment with Organizational Objectives:
* The organization conducts market research to evaluate supplier capabilities, industry trends, pricing structures, and risk factors.
* This helps determine whether external providers can meet the organization's needs and objectives.
* Aligning market opportunities with organizational strategy is crucial to ensure a contract is viable and beneficial.
* Risk Identification & Assessment:
* Potential risks such as supply chain disruptions, vendor reliability, and compliance issues are analyzed.
* Internal auditors may assess historical performance and external market conditions.
* Stakeholder Involvement & Approval:
* Internal stakeholders (finance, legal, procurement, and operational teams) collaborate to define the contracting requirements.

* The organization sets high-level objectives, including cost-effectiveness, quality standards, and compliance expectations.
* Preliminary Budgeting & Feasibility Analysis:
* The organization estimates the financial impact of potential contracts and ensures alignment with budgetary constraints.
* Initial cost-benefit analysis is conducted to determine contract viability.
* Bidding Phase (B): This occurs later in the process when vendors submit proposals, and the organization evaluates them against predefined criteria. It does not focus on market alignment but rather vendor selection.
* Development Phase (C): This phase involves drafting the contract terms, service level agreements (SLAs), and detailed responsibilities. Market alignment has already been considered in the initiation phase.
* Negotiation Phase (D): Here, the organization finalizes terms and conditions with the selected vendor, focusing on cost, deliverables, and legal requirements rather than market alignment.
* IIA's International Professional Practices Framework (IPPF) - Standard 2120 (Risk Management): This standard emphasizes that organizations must assess external risks (including market conditions) to align with strategic objectives.
* IIA's Global Technology Audit Guide (GTAG) on Contract Management: This guide highlights the importance of market analysis in the initiation phase to ensure contracts support organizational objectives.
* IIA's Practice Guide: Auditing Contract Management: It states that an effective contract management process starts with a thorough market assessment and strategic alignment in the initiation phase.
Step-by-Step Breakdown:Why Not the Other Phases?IIA References:

NEW QUESTION: 114
□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□□. □□□□ □□□□□□□ □ □□□ □□ □□ □□□ □□□ □□□□□?
A. A star
B. A cash cow
C. A question mark
D. A dog
Answer: B (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, BCG Matrix section.

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

B. □□ □□
C. □□ □□ □□.
D. □□ □□.
Answer: D (LEAVE A REPLY)
Understanding the Metric:
* The Budgeted Cost of Work Performed (BCWP), also known as Earned Value (EV), represents the value of work actually performed up to a specific date, based on the budgeted cost.
* This metric is part of Earned Value Management (EVM) and is used to track project performance by comparing planned and actual progress.
Why Cost Control?
* Cost control involves monitoring expenses, comparing actual performance with the budget, and taking corrective actions when needed.
* BCWP is a core metric in cost control as it helps in determining whether a project is staying within budget.
Why Other Options Are Incorrect:
* A. Resource planning: Focuses on allocating personnel, equipment, and materials but does not deal with financial performance.
* B. Cost estimating: Involves predicting project costs before execution, but BCWP is used during the project, not during estimation.
* C. Cost budgeting: Refers to setting a budget, whereas BCWP measures how much work has been performed relative to that budget.
IIA Standards and References:
* IIA Standard 2120 - Risk Management: Internal auditors should assess cost control mechanisms to manage financial risks.
* IIA Practice Guide: Auditing Capital Projects (2016): Emphasizes earned value management as a key cost control measure.
* PMBOK Guide - Cost Management Knowledge Area: Highlights BCWP as a crucial tool for monitoring and controlling project costs.

NEW QUESTION: 116
□□□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□ □□□□ □□ □□□ □□ □□□ □□□□□□. □□ □ □□ □□□ □□ □□□□ □□□ □□□ □□□□□?
A. □□ □□□□ □□ □□□□ □□□ □□□ □□ □□□□□□ □□□□.
B. □□ □□□ □□□□□ □□□ □□□ □□ □□□□ □□□□□.
C. □□ □□□ □□ □□□□ □□□ □□□ □□ □□□□.
D. □□□ □□ □□□□ □□ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
A highly centralized organization is one where decision-making authority is concentrated at the top management level, with lower levels having minimal autonomy. This change means

that most critical decisions are made at the corporate level, and lower-level managers have limited decision-making power.
* (A) Incorrect - Top management does little monitoring of the decisions made at lower levels.
* In a centralized organization, top management monitors and controls most decisions.
* This statement applies more to decentralized structures where decision-making is distributed.
* (B) Incorrect - The decisions made at the lower levels of management are considered very important.
* In a centralized structure, decisions made at lower levels hold less significance since authority is concentrated at the top.
* (C) Correct - Decisions made at lower levels in the organizational structure are few.
* Centralized structures limit decision-making power at lower levels, keeping control with top executives.
* Lower-level managers mostly follow directives from upper management rather than making independent decisions.
* (D) Incorrect - Reliance is placed on top management decision-making by few of the organization' s departments.
* In a centralized system, most (not just a few) departments rely on top management for decision- making.
* IIA's Global Internal Audit Standards - Organizational Governance and Decision-Making
* Explains centralized vs. decentralized structures and their impact on risk management.
* COSO's ERM Framework - Governance and Decision Authority
* Discusses the implications of centralization on strategic decision-making.
* IIA's Guide on Corporate Governance and Internal Control Frameworks
* Highlights the effect of centralization on accountability, oversight, and risk management.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 117
□□ □□ □□□□ □□ □□ □□□□□□□ □□□ □□ □□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□□ □□ □□□
C. □□□ □□□
D. □□□□ □□□ □□ □□□
Answer: (SHOW ANSWER)
The executive summary of the final audit report is intended for senior management and the board, who require a high-level overview of critical matters. Therefore, it should focus on significant observations that represent key risks, issues, or deficiencies.
Option A (all observations) makes the summary cluttered. Option B is incomplete since some significant issues may not yet have action plans. Option D would suppress important issues that management disagreed with.

Reference:
IIA Standards - Standard 2410: Criteria for Communicating.

NEW QUESTION: 118
□□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□□ □□□□□ □□ □□□ □□□□□.
B. □□□ □□ □□ □□□ □□□ □□ □□□□ □□ □□ □□ □□□ □□ □□□□□ □.
C. □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □.
D. □□□□□□ □□ □□□ □□□□□□ □□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
A sound network configuration practice should focus on enhancing security, preventing unauthorized access, and ensuring data integrity. The validation of intrusion prevention controls ensures that the network security measures function as intended and effectively protect data from threats.
* (A) Change management practices to ensure operating system patch documentation is retained.
* Incorrect: While maintaining patch documentation is important, change management alone does not directly enhance network security.
* (B) User role requirements are documented in accordance with appropriate application-level control needs.
* Incorrect: This practice improves access control and governance, but it is not a direct network security configuration practice.
* (C) Validation of intrusion prevention controls is performed to ensure intended functionality and data integrity. (Correct Answer)
* Intrusion Prevention Systems (IPS) help detect and prevent malicious activities in real time.
* Ensuring proper validation enhances security and prevents data corruption.
* IIA GTAG 15 - Information Security Governance recommends continuous monitoring and validation of security controls.
* (D) Interfaces reinforce segregation of duties between operations administration and database development.
* Incorrect: Segregation of duties is a good governance practice, but it does not directly relate to network security configuration.
* IIA GTAG 15 - Information Security Governance: Recommends validating security controls, including intrusion prevention systems.
* IIA Standard 2120 - Risk Management: Encourages proactive security controls to prevent cyber threats.

Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (C) Validation of intrusion prevention controls, as it directly enhances information security by ensuring real-time threat detection and data integrity.

NEW QUESTION: 119

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

A. □□ □□ □□□ □□□□ □ □□□□.

B. □□□ □□□ □□□□ □□ □□□ □□□ □□ □ □□□□.

C. □□□ □□ □□□ □□□□□□□.

D. □□□ □□□ □□□□ □□□ □□□□ □ □□□□□□.

Answer: B (LEAVE A REPLY)

Working capital = Current Assets - Current Liabilities

A high amount of working capital compared to industry averages suggests that the organization may not be efficiently using its resources. This could mean that:

* Excess cash is invested in inventory or accounts receivable, instead of being used for growth, investment, or shareholder returns.
* The company may be holding too much inventory, which could lead to obsolescence or additional storage costs.
* The business may have slow turnover in receivables, meaning cash is not being collected efficiently.
* A. Settlement of short-term obligations may become difficult. (Incorrect)
* A high working capital means the organization has sufficient assets to cover short-term obligations, so liquidity issues are unlikely.
* B. Cash may be tied up in items not generating financial value. (Correct)
* High working capital may indicate inefficient use of assets, such as excess inventory, high accounts receivable, or idle cash.
* This can negatively impact return on assets (ROA) and overall financial performance.
* C. Collection policies of the organization are ineffective. (Incorrect)
* While high receivables can be a factor, working capital includes all current assets and liabilities
, not just accounts receivable.
* The issue could be inventory mismanagement or excess liquidity, not just collection policies.
* D. The organization is efficient in using assets to generate revenue. (Incorrect)
* A high working capital does not necessarily mean efficiency. In fact, it may indicate underutilized resources rather than optimized performance.
* IIA GTAG 3 - Continuous Auditing: Implications for Internal Auditors highlights the importance of monitoring key financial metrics such as working capital.
* IIA Practice Advisory 2130-1 - Assessing Organizational Performance emphasizes that internal auditors should assess whether financial resources are being used efficiently.

* Financial Management Principles (IIA Guidance) discuss the impact of excessive working capital on liquidity and return on investment.
Explanation of Answer Choices:IIA References:Thus, the correct answer is B. Cash may be tied up in items not generating financial value.

NEW QUESTION: 120
□□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □ □ □□□□?
A. □□□ □□□ □□ □□ □□□ □□ □□□□□ □□□ □□□□□.
B. □□□ □□ □□ □□ □ □□□ □ □□ □□ □□ □□ □□□ □ □□□□.
C. □□ □□□□□ □□ □□□ □□□□ □□□□□ □□□ □□ □□□ □□□ □□□ □ □□□ □□□ □ □□□□.
D. □□□ □□ □□□□ □□□ □□□ □□□□□ □□□□ □□□□ □□□ □□ □ □□ □□.
Answer: D (LEAVE A REPLY)
Relevant cost refers to costs that will change depending on a specific business decision. It is crucial for decision-making as it helps management assess the financial impact of alternatives.
* Relevant costs focus on future costs that differ between decision alternatives.
* They help management analyze how different choices impact profitability.
* This supports decision-making in areas such as pricing, outsourcing, and product discontinuation.
* A. It explains the assumption that both costs and revenues are linear through the relevant range # Incorrect. While linear cost behavior is often assumed, it is not the primary purpose of relevant cost analysis.
* B. It enables management to calculate a minimum number of units to produce and sell without having to incur a loss # Incorrect. This describes break-even analysis, not relevant cost analysis.
* C. It enables management to predict how costs such as the depreciation of equipment will be affected by a change in business decisions # Incorrect. Depreciation is a sunk cost and is not considered relevant for decision-making.
* The IIA's Practice Guide: Financial Decision-Making and Internal Audit's Role outlines how relevant cost analysis aids business strategy.
* International Professional Practices Framework (IPPF) Standard 2120 states that internal auditors should assess management's cost-analysis techniques.
* Managerial Accounting Concepts (by IMA and COSO) emphasize relevant costs in strategic decision-making.
Why Option D is Correct?Explanation of the Other Options:IIA References & Best Practices:Thus, the correct answer is D. It enables management to make business decisions, as it explains the cost that will be incurred for a given course of action.

NEW QUESTION: 121

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

A. □□ □□ lo □□ □□

B. IT □□□□ □□ □ □□□□ □□ □□□□□□.

C. □□ □ □□.

D. □□□□□ □□□ □ □□

Answer: D (LEAVE A REPLY)

After upgrading to a new accounting software, it is critical to ensure that the system is functioning correctly and meets the organization's operational, compliance, and security requirements. The immediate priority should be software testing and validation to confirm that:

* The upgrade was successfully implemented.
* The system is free from major bugs or functionality errors.
* Financial data integrity is maintained.
* Compliance with accounting and regulatory standards is ensured.
* (A) Market analysis to identify trends:
* This is unrelated to post-upgrade activities. Market analysis is a strategic function typically handled by business intelligence or marketing teams, not IT software vendors.
* (B) Services to manage and maintain the IT infrastructure:
* While IT infrastructure maintenance is important, it is typically an ongoing operational task rather than an immediate post-upgrade activity.
* (C) Backup and restoration:
* While data backup should be completed before the software upgrade, restoration would only be necessary if the upgrade fails. However, this is a contingency plan, not a standard immediate post- upgrade activity.
* (D) Software testing and validation (Correct Answer):
* Immediately after an upgrade, software testing is critical to ensure that financial transactions, reporting, and other accounting functions operate correctly.
* This includes user acceptance testing (UAT), integration testing, and validation against financial reporting requirements.
* IIA Global Technology Audit Guide (GTAG) 8: Auditing Application Controls - Emphasizes the importance of testing and validating application functionality after implementation or upgrades.
* IIA Standard 2110 - Governance - Requires internal auditors to assess whether IT governance supports the organization's strategic objectives, including testing new software for operational effectiveness.
* COBIT (Control Objectives for Information and Related Technologies) Framework - Highlights the importance of post-implementation review to confirm that IT systems perform as expected.

Analysis of Each Option:IIA References:Conclusion:To ensure that the accounting software upgrade is successful and operationally sound, software testing and validation must be performed immediately.
Therefore, option (D) is the correct answer.

NEW QUESTION: 122
IIA □□□ □□□ □□□□□ □□□ □□ □□□ □□□□□ □□□□□□ □□□□ □□ □□ □□ □ □□ □□?
A. □□ □□□□□□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.
B. □□□□ □□□ □□□□□□ □□ □□□ □□ □□□□ □ □□□ □□□ □□□□ □ □□.
C. □□□ □□ □□□ □□□□□□ □□□□ □□□ □ □□ □□□□□□ □□□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□□ □□□ □□ □□□ □□□□ □□ □□□□□ □□□□ □ □ □□□.
Answer: B (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Workstation Security section.

NEW QUESTION: 123
4□□ □□□ □□□□ □□□□□□ □□□ □□□ □ □□ □□□□ □ □□□□ □□□ □ □□□ 4□□□ □□□ □□□□□ □□□□□?
A. □□
B. □□ □□□□
C. □□ □□
D. □□ □□□□
Answer: D (LEAVE A REPLY)
The four-level model for reviewing application controls follows a hierarchy:
* Level 1 - Activity: Smallest unit of work within a process.
* Level 2 - Subprocess: A collection of related activities that accomplish a part of the process.
* Level 3 - Major Process: A significant business function consisting of multiple subprocesses.

* Level 4 - Mega Process: The highest level, representing an end-to-end business process, often spanning multiple departments or systems.
* Mega processes encompass entire business functions (e.g., order-to-cash or procure-to-pay cycles).
* They involve multiple major processes and provide a high-level perspective on business operations.
* At level 4, the focus is on strategic alignment of IT application controls with enterprise-wide objectives.
* A. Activity - Too detailed and only represents individual tasks.
* B. Subprocess - A subset of a major process, not a high-level business function.
* C. Major Process - A significant function but not the highest-level view.
* IIA's GTAG on Business Process Controls - Recommends a hierarchical review model to assess IT application controls.
* COBIT 2019 (Governance and Management of IT) - Defines mega processes as enterprise-wide workflows.
* ISO 27001 Annex A.12 (Operational Security) - Highlights process-based security in IT controls.
Why "Mega Process" is the Correct Answer?Why Not the Other Options?IIA References:#
Final Answer: D.
Mega process.

NEW QUESTION: 124
□□□ □□□ □□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□□□ □□□□□□ □□□□□.
B. □□ □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□ □□□.
C. □□ □□□□ □□□ □□□□□□ □□
D. □□□ □□□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Data Integrity Controls section.

NEW QUESTION: 125
□ □□□ □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□ □ □□ □□□□□. □□ □ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□.
B. □□ □□□□□.
C. □□ □□.
D. □□ □□.
Answer: C (LEAVE A REPLY)
When an organization faces unexpected disruptions, such as the inability to receive raw materials due to a military conflict, it should have contingency plans in place to manage such risks.

* Contingency Planning for Unforeseen Events (Correct Answer: C)
* Contingency plans are designed to prepare for and respond to unexpected disruptions, such as supply chain failures, political instability, or natural disasters.
* IIA Standard 2120 - Risk Management requires organizations to have business continuity and disaster recovery plans, which include contingencies for supply chain disruptions.
* A well-prepared contingency plan could involve alternative suppliers, stockpiling critical materials, or adjusting production schedules.
* Why the Other Options Are Incorrect:
* A. Just-in-time (JIT) delivery plans (Incorrect)
* JIT is a supply chain management strategy that minimizes inventory and relies on timely delivery.
* While JIT increases efficiency, it is not a backup plan for unexpected disruptions.
* In fact, JIT makes companies more vulnerable to supply chain interruptions.
* B. Backup plans (Incorrect)
* A backup plan generally refers to IT/data backup or system recovery strategies, not a comprehensive risk management approach for supply chain issues.
* Contingency plans encompass broader business continuity strategies beyond simple backup plans.
* D. Standing plans (Incorrect)
* Standing plans are routine, long-term procedures for normal operations, such as HR policies or standard operating procedures.
* They do not specifically address unexpected crises like supply chain failures due to war.
* IIA Standard 2120 - Risk Management (Ensuring business continuity planning)
* IIA Standard 2110 - Governance (Assessing organizational resilience strategies)
* IIA Standard 2130 - Compliance (Evaluating regulatory and risk mitigation plans) Step-by-Step Justification:IIA References for This Answer:Thus, the correct answer is C. Contingency plans, as they are specifically designed to address unexpected disruptions like supply chain failures due to military conflict.

NEW QUESTION: 126
□□ □□ □□ □ □□ □□□□ □□□ □□ □ □□□ □□ □□ □□□ □□ □□□□ □ □□□ □ □□□□ □□ □□□□□?
A. □ □□□□ □□□□□.
B. □□ □□□ □□□ □□□□□.
C. □□ □□□□ □□□□□.
D. □□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
Duplicate testing is an analytical technique used to detect fraudulent payments, errors, or inefficiencies by identifying repeated transactions within financial records. In this case, an internal auditor would use duplicate testing to ensure that employees are not receiving fraudulent invoice payments by verifying that no invoice has been paid multiple times.

* Detecting Duplicate Payments: Fraudulent employees may submit the same invoice multiple times with slight modifications to avoid detection. Duplicate testing helps find identical or similar transactions.
* Identifying Unusual Patterns: By analyzing payment records, auditors can detect repeat payments to the same vendor, same invoice number, or similar amounts within a short time frame.
* Aligns with Fraud Prevention Practices: As per IIA Standard 2120 - Risk Management, internal auditors must identify and assess fraud risks, including duplicate invoice payments.
* Supports Data Analytics in Auditing: IIA GTAG (Global Technology Audit Guide) 16 - Data Analysis Techniques recommends using duplicate testing to identify fraud, control weaknesses, and errors in financial transactions.
* A. Perform gap testing: Gap testing is used to identify missing data or transactions in a sequence (e.
g., missing invoice numbers), but it does not specifically target duplicate or fraudulent payments.
* B. Join different data sources: This method is useful for cross-checking information across multiple databases, but it is not directly related to identifying duplicate invoice payments.
* D. Calculate statistical parameters: Statistical analysis provides summary insights about data (e.g., mean, median), but it does not specifically detect duplicate payments.
* IIA Standard 2120 - Risk Management: Internal auditors must evaluate fraud risks, including duplicate payments.
* IIA Standard 1220 - Due Professional Care: Requires auditors to apply appropriate data analytics techniques.
* IIA GTAG 16 - Data Analysis Techniques: Recommends duplicate testing as an effective fraud detection method.
Key Reasons Why Option C is Correct:Why Other Options Are Incorrect:IIA References:Thus, the correct answer is C. Perform duplicate testing.

NEW QUESTION: 127
□ □□□□ □3□ □□ □□ □□□□ □□□□ □□ □□ □□□□ □□□□□ □□□ □ □□□□ □□□□□□. □□ □ □□□□ □□□ □□ □ □□□ □□?
A. □□□
B. □□ □□
C. □□ □□
D. □□
Answer: B (LEAVE A REPLY)
Vertical integration occurs when a company expands its operations into a different stage of its supply chain. In this case, the restaurant is moving from relying on third-party delivery services to handling its own delivery operations, which is an example of backward vertical integration (taking control of a process previously handled by an external provider).
* (A) Incorrect - Diversification.

* Diversification refers to entering a completely different industry or market (e.g., a restaurant launching a grocery store).
* In this case, the restaurant is expanding within the same industry by adding delivery services.
* (B) Correct - Vertical integration.
* Vertical integration happens when a company takes control of another step in its supply chain
.
* Since the restaurant is now handling its own deliveries instead of outsourcing, this is an example of backward vertical integration.
* (C) Incorrect - Risk avoidance.
* Risk avoidance means eliminating an activity entirely to prevent exposure to risk (e.g., deciding not to offer delivery at all).
* The restaurant is not avoiding risk but taking on additional responsibilities.
* (D) Incorrect - Differentiation.
* Differentiation is a strategy focused on making a product/service unique to stand out from competitors.
* The restaurant is not introducing a unique feature but integrating delivery operations.
* IIA's Global Internal Audit Standards - Business Strategy and Risk Management
* Defines vertical integration and its impact on operational control.
* COSO's ERM Framework - Strategic Risk Considerations
* Discusses how vertical integration influences business risks and cost control.
* Porter's Competitive Strategies - Vertical Integration Analysis
* Explains backward and forward integration in supply chain management.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 128
□□ □ □□□ □□ □□□□□□(UDA)□ □□ □□□□ □□ □□ □□?
A. UDA□ □□ IT □□□□□□□□ □□□□ □□□□ □□□□□ □ □□□□□.
B. UDA□ □□□□□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □ □□□□.
C. UDA□ □□□□□ □□□□□□ □□ □ □□ □□ □□ □□□□□.
D. □□□□□ UDA□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
User-Developed Applications (UDAs) are applications, spreadsheets, databases, or tools created and maintained by end-users rather than IT departments. They provide flexibility but also introduce risks related to security, accuracy, and change management.
* Why Option B is Correct:
* UDAs lack formal change management controls.
* Since they are typically not subject to rigorous testing and documentation, modifications may introduce errors.

* Updating or correcting a formula, macro, or script in a UDA may have unintended consequences that go unnoticed, leading to data integrity issues.
* Why Other Options Are Incorrect:
* Option A (UDAs are less flexible and more difficult to configure than traditional IT applications):
* Incorrect. UDAs are more flexible and easier to modify compared to traditional IT applications, which undergo strict change controls.
* Option C (UDAs typically are subjected to application development and change management controls):
* Incorrect. Most UDAs lack formal governance or IT oversight. They are typically developed by business users with little or no structured IT controls.
* Option D (Using UDAs typically enhances the organization's ability to comply with regulatory factors):
* Incorrect. UDAs introduce compliance risks due to lack of security, audit trails, and formal change controls.
* IIA GTAG - "Auditing User-Developed Applications": Discusses risks and controls related to UDAs.
* IIA Practice Advisory 2130-1 (Control Risk Self-Assessment): Highlights the importance of internal controls over UDAs.
* COSO Internal Control - Integrated Framework: Recommends applying IT general controls (ITGCs) to UDAs.
IIA References:Thus, the correct answer is B. Updating UDAs may lead to various errors resulting from changes or corrections.

NEW QUESTION: 129
Herzberg□ □□ □□ □□□ □□□ □□ □□ □ □□□ □□□ □□ □□ □□□□ □□ □ □□□□□?
A. □□ □ □□
B. □□□ □□
C. □□□□ □ □□
D. □□□□□ □□□
Answer: (SHOW ANSWER)
Herzberg's Two-Factor Theory of Motivation identifies two categories of workplace factors:
* Hygiene Factors - Prevent dissatisfaction but do not create motivation (e.g., salary, job security, work conditions).
* Motivational Factors - Lead to job satisfaction and motivation (e.g., achievement, responsibility, advancement, recognition).
* (A) Salary and status. # Incorrect.
* Salary is a hygiene factor, meaning it prevents dissatisfaction but does not directly drive job satisfaction.
* Status is also not a strong motivator under Herzberg's theory.

* (B) Responsibility and advancement. # Correct.
* These are motivational factors in Herzberg's theory.
* Employees feel satisfied when they have responsibility, career growth, and promotion opportunities.
* IIA GTAG "Auditing Human Resource Management" highlights career development as a key driver of employee motivation and retention.
* (C) Work conditions and security. # Incorrect.
* These are hygiene factors, which help avoid dissatisfaction but do not actively motivate employees.
* (D) Peer relationships and personal life. # Incorrect.
* Good relationships with coworkers help, but they are not primary motivators under Herzberg' s theory.
* IIA GTAG - "Auditing Human Resource Management"
* IIA Standard 2110 - Governance (Employee Motivation & Engagement)
* Herzberg's Two-Factor Theory of Motivation (Workplace Psychology Research) Analysis of Answer Choices:IIA References:Thus, the correct answer is B, as responsibility and advancement are the key motivational factors leading to employee satisfaction.

NEW QUESTION: 130
□□ □ □□□ □□□ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□□□ □□ □□□□ □□□□ □□ □□ □ □□□□.
B. □□□□ □□ □□□ □□□ □ □□□□.
C. □□ □□□, □□□□ □□□ □□□ □ □□
D. □□□□ □□ □□□ □□□□ □□□ □□ □□ □□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
* Remote wipe is not always 100% effective: While remote wiping can delete most user data, some residual data may remain on the device, especially in cases where:
* The device has built-in storage redundancies.
* Deleted data can be recovered using forensic tools.
* The remote wipe command fails to execute properly due to network issues or device settings.
* Security Risk: This limitation poses a risk for organizations handling sensitive or confidential data, as unauthorized individuals may recover wiped data.
* IIA Standard 2110 - Governance: Internal auditors must assess how organizations manage IT security risks, including risks related to mobile devices and data protection.
* IIA Practice Guide: Auditing Cybersecurity Risks highlights the need to evaluate mobile security controls and limitations of data removal techniques.
* A. Encrypted data cannot be locked to prevent further access (Incorrect)
* Encrypted data remains secure even if the device is lost.
* Many enterprise security solutions allow organizations to revoke encryption keys remotely, making data inaccessible.

* IIA Standard 2120 - Risk Management advises that effective encryption reduces the impact of data loss.
* B. Default settings cannot be restored on the device. (Incorrect)
* Most remote wipe solutions allow factory reset, restoring the device to default settings.
* Many mobile device management (MDM) tools support full device restoration.
* D. Mobile device management software is required for a successful remote wipe. (Incorrect)
* While MDM enhances remote wiping capabilities, it is not strictly required.
* Some consumer and enterprise mobile operating systems (e.g., iOS, Android) provide built-in remote wipe functionality without MDM.
Explanation of Answer Choice C (Correct Answer):Explanation of Incorrect Answers:Conclusion:Remote wipe has limitations, and the inability to completely remove all data from the device (Option C) is a primary concern.
IIA References:
* IIA Standard 2110 - Governance
* IIA Standard 2120 - Risk Management
* IIA Practice Guide: Auditing Cybersecurity Risks

NEW QUESTION: 131
□□□ □□□ □□□ □□ □□□ □□□□ □ □ □□ □□ □ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□ □□□□ □□□□ □□ □ □□□ □□□□□.
B. □□□□ □□ □□ □□□□ □□□□ □□□□ □□□ □ □□ □□□□□ □□□□□.
C. □□□ □□□□□ □□□□ □□□□ □□ □ □□ □□ □□□ □□□ □□□ □□□□ □.
D. □□□ □□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
When executive compensation is tied to financial results, there is a strong incentive to manipulate financial reporting or focus solely on short-term performance at the expense of stakeholders' interests.
* Potential for Unethical Behavior:
* Executives may prioritize profit-driven decisions (e.g., cost-cutting, aggressive revenue recognition) over long-term sustainability.
* As per IIA Standard 2110 - Governance, incentive structures should align with ethical business practices and stakeholder interests.
* Increased Risk of Fraud and Misrepresentation:
* The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Fraud Risk Management Guide highlights how executive incentives can lead to financial statement manipulation.
* This could result in actions like aggressive revenue recognition, improper expense deferrals, or overstating earnings to boost compensation.

* Misalignment with Stakeholder Interests:
* Employees, customers, and investors suffer if executive compensation encourages short-term gains over long-term stability.
* IIA GTAG 3: Continuous Auditing supports monitoring financial reporting risks to detect such inconsistencies.
* A. The organization reports inappropriate estimates and accruals due to poor accounting controls. (Incorrect)
* Reason: While poor controls can contribute to misstatements, the root cause in this scenario is compensation structure, not control weakness.
* B. The organization uses an unreliable process for gathering and reporting executive compensation data. (Incorrect)
* Reason: This issue relates to HR and payroll data integrity, not the impact of performance- based compensation on behavior.
* C. The organization experiences increasing discontent of employees, if executives are eligible for compensation amounts that are deemed unreasonable. (Incorrect)
* Reason: While excessive executive pay may cause employee dissatisfaction, the question focuses on behavioral impacts on stakeholders, making D the more relevant choice.
* IIA Standard 2110 - Governance - Ensures executive compensation aligns with organizational ethics and stakeholder interests.
* IIA Standard 2120 - Risk Management - Covers the risks associated with incentive-based compensation.
* COSO Fraud Risk Management Guide - Discusses financial fraud linked to executive compensation.
* IIA GTAG 3: Continuous Auditing - Supports risk-based monitoring of financial statements.
Why is Answer D Correct?Analysis of Incorrect Answers:IIA References:Thus, the correct answer is D. The organization encourages employee behavior that is inconsistent with the interests of relevant stakeholders.

NEW QUESTION: 132
□□ □□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□□□ □□ □□□ □□□□□□. □□□□ □□ □□ □ □□ □□□ □□□□ □□□□□. □□□ □ □ □□□ □□□ □□□□□□?
A. □□□□ □□.
B. □□ □□.
C. □□ □□.
D. □□
Answer: D (LEAVE A REPLY)
A debenture bond is an unsecured bond that is not backed by specific assets or collateral. Instead, it is backed only by the issuer's creditworthiness and general reputation. Since the organization in this scenario has a stable rating from international rating agencies and

guarantees interest and principal payments, it aligns perfectly with the definition of a debenture bond.
* A. A sinking fund bond - A bond that has a special account (sinking fund) where money is set aside to pay off bondholders over time. This is not mentioned in the scenario.
* B. A secured bond - This type of bond is backed by specific assets or collateral to reduce investor risk. However, the scenario states that the bond is not backed by assets or collateral, eliminating this choice.
* C. A junk bond - These are high-risk, high-yield bonds issued by companies with low credit ratings.
The scenario specifies that the company has a stable rating, making this incorrect.
* D. A debenture bond (Correct Answer) - Since this bond is unsecured and relies solely on the organization's financial health, it matches the definition of a debenture bond.
* IIA IPPF Standard 2120 - Risk Management discusses financial risk management, including bond issuance.
* COSO ERM Framework - Financial Risk Management emphasizes evaluating creditworthiness before issuing debt.
* IFRS 9 - Financial Instruments provides accounting guidance on different bond types.
Explanation of Each Option:IIA References:

NEW QUESTION: 133
□□□ □□□□□ □□ □□: □□ □ □□□□□□ □□□ □□□ □□□ □□□□□. □ □□ □□□ □□ □3□ □□□□ □□□ □□ □□□ □□□ □ □□□□□. □□ □ □□□ □ □□□ □□ □□□ □□□□□?
A. □□□□□□ □□
B. □□□ □□ □□
C. □□□ □□ □□□
D. □□□ □□
Answer: B (LEAVE A REPLY)
The organization suffered significant damage to its local file and application servers due to a hurricane but managed to recover all backed-up information through its overseas third-party contractor. This scenario highlights the management of data storage, backup, and recovery processes, which are critical components of data center management.
* Definition of Data Center Management:
* Data center management refers to the administration and control of data storage, backup, recovery, and overall infrastructure to ensure business continuity and disaster recovery (BC /DR).
* As per the IIA's Global Technology Audit Guide (GTAG) on Business Continuity Management (BCM), organizations must have robust backup strategies to mitigate risks from natural disasters.
* Third-Party Backup and Recovery:

* The fact that the organization recovered data from an overseas third-party contractor aligns with offsite data backup and disaster recovery planning, which falls under data center management.
* According to IIA Practice Guide: Auditing Business Continuity and Disaster Recovery, organizations should store critical data at geographically dispersed locations to mitigate disaster risks.
* Why Not Other Options?
* A. Application Management - This pertains to managing software applications throughout their lifecycle but does not focus on disaster recovery.
* C. Managed Security Services - While third-party security services protect against cyber threats, they do not specifically cover data backup and recovery.
* D. Systems Integration - This deals with connecting different IT systems, not managing backup and recovery.
* IIA GTAG (Global Technology Audit Guide) - Business Continuity Management
* IIA Practice Guide: Auditing Business Continuity and Disaster Recovery
* IIA Standard 2110 - Governance: Ensuring IT Governance Supports Business Continuity Step-by-Step Justification:IIA References:Thus, the correct and verified answer is B. Data center management.

NEW QUESTION: 134
□□□□ □□□ □□□ □□ □□□□ □□ □□?
A. □□□ □□□ □□□□ □□□□ □□□ □□□ □□□□□.
B. □□□ □□□ □□□ □□□□ □□□ □□□ □□□□□.
C. □□□ □□□ □□□□ □□□□ □□□ □□□ □□□□□.
D. □□□ □□ □□, □□□ □□
Answer: (SHOW ANSWER)
In accounting, the terms debit (Dr.) and credit (Cr.) refer to the two sides of an account in the double-entry accounting system.
* Definition of Debit and Credit in Accounting:
* Every financial transaction affects at least two accounts in a double-entry system: one account is debited, and another is credited.
* Debits (Dr.) appear on the left side, while credits (Cr.) appear on the right side of an account.
* Accounting Equation:
Step-by-Step Justification:Assets=Liabilities+Equity\text{Assets} = \text{Liabilities} + \text{Equity} Assets=Liabilities+Equity
* Debits increase assets and expenses.
* Credits increase liabilities, equity, and revenues.
* Why the Other Options Are Incorrect:
* A. Debit indicates the right side of an account and credit the left side #

* Incorrect, as debits are always recorded on the left side, and credits are always on the right side.
* B. Debit means an increase in an account and credit means a decrease. #
* Partially incorrect; it depends on the type of account:
* For assets and expenses, debits increase and credits decrease.
* For liabilities, equity, and revenues, credits increase and debits decrease.
* D. Credit means an increase in an account and debit means a decrease. #
* Also incorrect because increases and decreases depend on the type of account (e.g., debits increase assets but decrease liabilities).
* IIA Standard 1210.A1: Internal auditors must be familiar with fundamental accounting principles.
* IIA Practice Guide: Auditing Financial Statements: Ensures proper understanding of debits and credits in financial reporting.
* GAAP & IFRS Accounting Standards: Define how debits and credits are recorded in financial statements.
IIA References:Thus, the correct answer is C. Credit indicates the right side of an account and debit the left side. #

NEW QUESTION: 135
□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□. □□□ □□□ □3□(□□□□ □ □□□)□ □□ □□□ □□□ □□□□ □□ □□□□ □ □□□□ □□ □□ □ □□□ □□□□□ □□□□. □□ □□□□ □□ □□□□ □□ □□□ □□ □□ □□□ □□ □ □□□□□?
A. □□.
B. □□ □□ □□
C. □□□
D. □□□ □□
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Allowing external devices to access proprietary systems introduces compliance risks, as these devices may not meet the organization's security, data protection, and regulatory standards.
Option B (Privacy) - Important but does not fully capture the risk of unauthorized access or non-compliance with security protocols.
Option C (Strategic) - Strategic risks relate to business direction, not security concerns with third-party access.
Option D (Physical security) - Physical risks involve device theft, which is secondary to compliance when granting access.
Since compliance violations can lead to regulatory penalties and data breaches, Option A (Compliance) is the correct answer.
Reference: IIA IT Risk & Compliance Frameworks - BYOD Policies

NEW QUESTION: 136
□□□ CEO□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□. □□ □□□ □□□ □□□□□□□?
A. □□ □□.
B. □□□ □□ □□.
C. □□□ □□ □□.
D. □□□ □□.
Answer: B (LEAVE A REPLY)
A spear phishing attack is a highly targeted email-based attack where an attacker impersonates a trusted individual (e.g., the CEO) to trick recipients into providing sensitive information.
* In this scenario, an intruder posed as the CEO and deceived payroll staff into sharing employees' private tax information.
* Spear phishing is more targeted than general phishing, often using personal details to make the fraudulent request seem legitimate.
* A. Boundary attack. (Incorrect)
* A boundary attack refers to attempts to breach an organization's network perimeter defenses, such as firewalls and intrusion detection systems.
* This scenario describes a social engineering attack, not a technical boundary attack.
* B. Spear phishing attack. (Correct)
* Spear phishing attacks are highly personalized email attacks, usually targeting specific employees within an organization.
* Attackers research their targets and use realistic messages to trick them into divulging sensitive data.
* This fits the scenario, as the attacker impersonated the CEO to steal tax information.
* C. Brute force attack. (Incorrect)
* A brute force attack involves systematically guessing passwords to gain unauthorized access to systems.
* This attack was based on deception, not password cracking.
* D. Spoofing attack. (Incorrect, but closely related)
* Email spoofing is a technique where an attacker falsifies the sender's email address.
* While spear phishing often includes spoofing, the broader technique used here is spear phishing, as it involved social engineering and deception.
* IIA GTAG 16 - Security Risk: IT and Cybersecurity discusses phishing and social engineering threats, emphasizing internal controls to mitigate them.
* IIA Standard 2120 - Risk Management highlights the need for risk assessments in cybersecurity, including employee awareness training for phishing attacks.
* National Institute of Standards and Technology (NIST) Special Publication 800-61 classifies spear phishing as a high-risk cyber threat to organizations.
Explanation of Answer Choices:IIA References:

NEW QUESTION: 137
□□ □ □□ BYOD(Bring-Your-Own-Device) □□□ □□□□□ □□□□ □□□□ □□ □ □ □□□ □□□ □□□ □□ □□□□ □□□□?
A. □□□ □□ □□□□□□ □□□□ □□□□□.
B. □□ □□□□□□ □□□□□ □□□□□□□.
C. □□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Jailbreaking a locked smart device (removing manufacturer-imposed restrictions) increases the risk of infringing on copyright and privacy laws, as it allows unauthorized access to software and applications.
Option A (Not installing anti-malware software) - Increases security risks but does not directly violate regulations.
Option B (Haphazard OS updates) - Can lead to vulnerabilities but is not a legal issue.
Option C (Weak passwords) - Poses a security threat but does not impact compliance with laws.
Since jailbreaking often violates software licenses and may lead to illegal use of software, Option D is the correct answer.
Reference: IIA IT Security & BYOD Compliance Standards

NEW QUESTION: 138
□□ □□ □□□□ □ □□ □□□ □□(EDI)□ □□□□ □□ □ □□□ □□ □ □□ □□ □□□□□?
A. □□□□ □□
B. □□□ □□□ □□
C. □□□□ □□□ □□ □□
D. □□ □□□□□ □□ □□□□
Answer: A (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Supply Chain Management section.

NEW QUESTION: 139
□□ □□□□ □□ □□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□.
□□□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□□. □ □□□□ □ □□□□ □□ □ □□ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□ □□□□ □□□□□ □□□□.
B. □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□□.
C. □□□□ □□ □□□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□□.
D. □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
In data analytics, data cleaning involves identifying and correcting errors, inconsistencies, and redundancies in the dataset to ensure accuracy and reliability. By eliminating duplicate or irrelevant data, the internal auditor enhances the quality of the dataset, which is crucial for accurate analysis and risk assessment. This process is a preparatory step before analyzing the data to identify high-risk areas. Normalization (option A) refers to organizing data to reduce redundancy but is more specific to database design. Analyzing data (option B) and reviewing data prior to defining the question (option D) are steps that occur before and after data cleaning, respectively.

NEW QUESTION: 140
□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□ □ □, □□ □□ □□□ □□□ □□□ □□ □ □□□□□?
A. □□ □□ □□□(CAE)□ □□□ □□ □□□□ □□ □□□□ □□□□ □ □□□ □□ □□ □□□□□ □□□□ □□□.
B. CAE□ □□□ □□ □□□□ □□ □□ □□□□ □□□□□ □□□ □□□□ □□□.
C. CAE□ □□ □□□ □□□□ □□ □□□ □□□ □□□ □□ □□□□ □□□□ □□ □.
D. CAE□ □□□ □□□ □□ □□□ □□ □□□ □□□□□□ □□ □□ □□□□□ □□ □□ □□□.
Answer: C (LEAVE A REPLY)
According to IIA Standards, if senior management accepts a risk that the CAE believes may be unacceptable, the CAE must judge whether the risk is indeed acceptable and, if not, escalate the matter to the board. This ensures that governance bodies are aware of significant exposures. Reporting directly to external stakeholders (Option A) is not internal audit's role. Option B alone is insufficient if the risk is significant. Option D applies only when management's acceptance aligns with tolerance.
Reference:
IIA Standards - Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 141

□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□?
A. □□□□□ □□ □□□□ □□ □ □□
B. □□ □□□ □□ □□ □□□□ □□
C. □□□ □□ □□ □□ □□ □□□ □□□□□.
D. □□□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The CAE should remain aware of emerging risks through ongoing communication and collaboration with senior management and other stakeholders. Building strong relationships allows the CAE to obtain early insights into new and developing risks.
Option B (building a risk management process) is management's responsibility, not internal audit's. Options C and D involve reviewing processes, but they do not directly expose the CAE to emerging risks in real time.
Reference:
IIA Standards - Standard 2010: Planning; Practice Guide - Developing a Risk-based Internal Audit Plan.

NEW QUESTION: 142
□□□ □□□□ □□□ □□ □□□□ □□ □□□ □□ □ □□ □□□□ □□ □□ □□ □□□?
A. □□□.
B. □□.
C. □□.
D. □□□.
Answer: D (LEAVE A REPLY)
Data governance refers to the policies, processes, and controls an organization implements to ensure data integrity, security, and compliance. When an organization has a weak data governance culture, the most compromised attribute of data is "veracity," which refers to the accuracy, reliability, and trustworthiness of data.
* Why Option D (Veracity) is Correct:
* Weak data governance leads to poor data quality, inconsistencies, and errors, reducing data veracity (trustworthiness and accuracy).
* Without strong governance, data may be incomplete, outdated, or manipulated, leading to flawed decision-making.
* Data veracity is critical for risk management, internal audit, and regulatory compliance, as unreliable data can lead to financial misstatements and operational risks.
* Why Other Options Are Incorrect:
* Option A (Variety):
* Variety refers to different types and sources of data (structured, unstructured, semi-structured).
* A weak data governance culture does not necessarily affect the diversity of data sources.
* Option B (Velocity):

* Velocity refers to the speed at which data is generated, processed, and analyzed.
* Weak governance impacts data quality more than processing speed.
* Option C (Volume):
* Volume refers to the quantity of data being processed and stored.
* Weak data governance might lead to data duplication or loss but does not directly impact data volume.
* IIA GTAG - "Auditing Data Governance": Emphasizes the importance of data veracity in decision- making.
* COSO Internal Control Framework: Highlights the role of data integrity in financial and operational controls.
* IIA's Global Technology Audit Guide on Data Analytics: Discusses the risks of poor data governance affecting veracity.
IIA References:

NEW QUESTION: 143
□□ □ □□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□.
B. □□ □□.
C. □□□ □□ □□.
D. □□ □□
Answer: (SHOW ANSWER)
Capital budgeting techniques are used to evaluate investment projects by analyzing potential costs and benefits. One key consideration in capital budgeting is the time value of money (TVM), which states that a dollar received today is worth more than a dollar received in the future due to its earning potential.
* Why Option C (Discounted cash flow) is Correct:
* Discounted Cash Flow (DCF) explicitly incorporates the time value of money by discounting future cash flows to their present value.
* Methods such as Net Present Value (NPV) and Internal Rate of Return (IRR) fall under DCF analysis, making them highly reliable for long-term capital budgeting decisions.
* Why Other Options Are Incorrect:
* Option A (Annual rate of return):
* Incorrect because the annual rate of return (ARR) is based on accounting profits and does not consider the time value of money.
* Option B (Incremental analysis):
* Incorrect because incremental analysis is a decision-making tool that compares alternative costs and revenues but does not discount future cash flows.
* Option D (Cash payback):
* Incorrect because the payback period method only measures the time needed to recover an investment and ignores the time value of money.

* IIA GTAG - "Auditing Capital Budgeting Decisions": Discusses the importance of time value of money in investment decisions.
* COSO ERM Framework - "Risk Considerations in Financial Planning": Recommends using DCF methods for capital investment decisions.
* IFRS & GAAP Financial Reporting Standards: Advocate for using DCF techniques for asset valuation and investment analysis.
IIA References:

NEW QUESTION: 144
□□ □ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□□□□?
1. □□□ □□□□ □□□ □ □□□ □ □□□ □□□ □□ □□□□ □□□ □□□ □ □ □.
2. □□□ □□ □□□ □□ □□ 7□□ □□□ □ □□□□.
3. □□□□ □□□ □□□ □□□□□ □□□.
4. □□ □□□ □□□ □□□ □□ □ □□ □□□ □□□□□ □□□.
A. 1□ 3□
B. 1□ 4□
C. 2 □ 3□
D. 3 □ 4□
Answer: A (LEAVE A REPLY)
Both hierarchies (traditional organizations with a clear chain of command) and open organizational structures (flatter, decentralized decision-making models) share certain fundamental management principles.
Let's analyze each statement:
* A superior can delegate the authority to make decisions but cannot delegate the ultimate responsibility for the results of those decisions.
* Correct. In both hierarchical and open structures, managers can delegate decision-making authority, but they remain accountable for the outcomes.
* IIA Reference: Internal auditors assess governance structures to ensure that accountability remains with senior management, even when authority is delegated. (IIA Standard 2110:
Governance)
* A supervisor's span of control should not exceed seven subordinates.
* Incorrect. While some management theories suggest an ideal span of control, there is no universal limit of seven subordinates. The optimal number depends on factors like task complexity and organizational structure.
* Responsibility should be accompanied by adequate authority.
* Correct. Employees must have the necessary authority to fulfill their responsibilities effectively, regardless of the organizational structure.

* IIA Reference: The IIA's guidelines on effective governance and accountability emphasize the need for clear delegation of authority to ensure operational efficiency. (IIA Practice Guide:
Organizational Governance)
* Employees at all levels should be empowered to make decisions.
* Incorrect. While this principle applies to open organizational structures, it does not align with traditional hierarchies, where decision-making authority is concentrated at higher levels.
Thus, the verified answer is A. 1 and 3 only.

NEW QUESTION: 145
□□□ □; □□□ □□ □□□□ □□ □□□□ □□ □□ □□ □ □□□ □□ □□□ □□ □□ □□□?
A. □□ □□□ □□ □ □□ □□
B. □□ □□ □□.
C. □□ □□ □□
D. □□ □□ □□ □ □□ □□.
Answer: A (LEAVE A REPLY)
A strategic plan outlines an organization's long-term objectives, defining achievable goals and the timelines for reaching them. It serves as a roadmap for future success and ensures alignment with the organization's mission.
Let's analyze each option:
* Option A: Identification of achievable goals and timelines.
* Correct.
* A strategic plan must include clear, measurable objectives and timelines for achieving them.
* Without defined goals and timelines, an organization lacks direction and accountability.
* IIA Reference: Internal auditors assess strategic planning processes to ensure goals are well- defined, realistic, and aligned with business objectives. (IIA Practice Guide: Auditing Strategic Management)
* Option B: Analysis of the competitive environment.
* Incorrect.
* While environmental analysis is an important input into strategic planning (e.g., through SWOT or PESTEL analysis), it is not a core component of the plan itself.
* Option C: Plan for the procurement of resources.
* Incorrect.
* Resource procurement falls under operational or tactical planning, which is separate from high-level strategic planning.
* Option D: Plan for progress reporting and oversight.
* Incorrect.

* While monitoring progress is important, it is part of strategy execution and performance measurement rather than the core strategic plan itself.
Thus, the verified answer is A. Identification of achievable goals and timelines.

NEW QUESTION: 146
□□ □ □□ □□□□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□ □□□ □□ □ □□□□?
A. □□ □□ □□□(CAE)□ □□ □□□□ □□ □□□□ □ □□ □□□ □□□ □ □□□ □.
B. CAE□ □□ □□□□ □□ □□□□ □□□ □□, □□ □ □□□ □□□□□ □□□□ □.
C. □□□□ □□ □□□□ □□□ □□□ □ □□ □□□ □□□□ CAE□ □□□□□.
D. □□□□ □□ □□□□ □□ □□ □□□□□□□ CAE□ □□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)
Reliance on external auditors' work is possible if the CAE has sufficient access to review their programs and workpapers to evaluate the scope, quality, and results. This ensures internal audit can confirm the appropriateness of relying on their work.
Option B is not required-external and internal audit can use different methodologies.
Options C and D represent governance involvement but do not substitute for CAE's independent evaluation of audit work.
Reference:
IIA Standards - Standard 2050: Coordination and Reliance.

NEW QUESTION: 147
□□ □ □□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □ □□□ □□ □□ □ □□□□□?
A. □□□ □□□ □□ □□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□□□ □□□ □□□□□ □□□.
D. □ □□□□ □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
To enable management to receive timely feedback and mitigate unforeseen risks, it is critical to have a performance measurement system in place. Measuring product performance against an established standard is a key control mechanism that allows management to identify deviations, take corrective actions, and mitigate risks proactively.
* Performance Monitoring & Timely Feedback: Comparing actual product performance against set standards helps in detecting quality issues, inefficiencies, or process failures early.
* Risk Mitigation: Ensures that any deviations from expected performance can be addressed before they become major problems.

* Internal Control Best Practices: Measuring against standards aligns with IIA's risk management principles to ensure continuous monitoring and improvement.
* Option B (Develop standard methods for performing established activities): While standardization improves efficiency, it does not provide ongoing feedback or mitigate unforeseen risks in real-time.
* Option C (Require the grouping of activities under a single manager): Centralizing activities may improve coordination, but it does not directly provide timely performance feedback.
* Option D (Assign each employee a reasonable workload): Managing workloads ensures efficiency but does not provide risk mitigation through performance monitoring.
* IIA's Standard 2120 - Risk Management: Requires internal auditors to assess whether an organization's risk management processes enable timely risk identification and mitigation.
* COSO's Internal Control Framework (Performance Monitoring Component): Emphasizes measuring actual performance against expected outcomes as a fundamental internal control.
Why Option A is Correct:Why Other Options Are Incorrect:IIA References:Thus, the most appropriate answer is A. Measure product performance against an established standard.

NEW QUESTION: 148
□□ □□□□ □□ □□ □□□□□□□ □□□ □□□ □□□. □□□□□□□(CAE)□ □ □ □□□□, CAE□ □□ □□ □□□□□ □□ □□ □□□□□□□ □□□□ □□□ □□ □□□□□. □□ □□ □□□□□□□ □□ □□□ □□□□ □□□□?
A. □□ □□□
B. □□ □□ □□□
C. □□
D. □□ □□□
Answer: B (LEAVE A REPLY)
The CAE is ultimately accountable for all final engagement communications, even if dissemination is delegated to others. The Standards hold the CAE responsible for ensuring that reports are accurate, objective, clear, concise, constructive, complete, and timely. Options A and D (supervisor or team) may assist but do not hold accountability. Option C (the board) receives reports but is not responsible for them.
Reference:
IIA Standards - Standard 2400: Communicating Results.

NEW QUESTION: 149
IT□ □□ 11A □□□ □□□ □□ □ □□□ □□ □□□ □□□ □□□□□?
1. □□□□ □□ □□.
2. □□□□ □□ □□□□.
3. □□□ □□ □□ .
4. □□□ □□□□ □□□ □ □□□□.

A. 2 and 3 only.
B. 1, 2, and 3 only
C. 1, 3, and 4 only
D. 2, 3, and 4 only
Answer: D (LEAVE A REPLY)
Effective change management ensures that IT changes (such as software updates, system modifications, or infrastructure upgrades) are well-controlled, minimizing disruptions. Poor change management leads to instability, inefficiencies, and operational risks.
* Unplanned Downtime (2) - Indicates that changes are being implemented without proper testing or failover planning, disrupting business operations.
* Excessive Troubleshooting (3) - Suggests that changes are causing recurring issues, leading to increased workload for IT support teams.
* Unavailability of Critical Services (4) - Highlights that change-related failures are affecting essential business functions, indicating improper risk assessment.
* While inadequate control design is a general IT risk, it is not a direct indicator of poor change management. Instead, it relates more to weaknesses in IT governance and security frameworks.
* IIA's GTAG (Global Technology Audit Guide) on Change Management - Identifies unplanned downtime, excessive troubleshooting, and service unavailability as key red flags of poor change management.
* COBIT 2019 (Governance and Management of IT) - Emphasizes structured change management to minimize disruptions.
* ITIL Change Management Framework - Highlights these issues as symptoms of ineffective change control.
Why 2, 3, and 4 Are Indicators of Poor Change Management?Why Not Option 1 (Inadequate Control Design)?
IIA References:# Final Answer: D. 2, 3, and 4 only.

NEW QUESTION: 150
□□ □□ □□, □□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□□□. □□ □□, □□□□□□ □□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□□ □□ □□□ □□□□□?
A. □□ □□ □□□□□ □□ □□□ □□
B. □□□□□ □□ □□ □□ □□
C. □□□ □□ □□□ □□ □ □□□ □□
D. □□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)
The most effective way to mitigate the risk of poor-quality spare parts is through independent verification of deliveries, such as inspections and testing. This detects defects before acceptance and payment, reducing the likelihood of defective parts entering operations.

Option A adds approval steps but does not address product quality. Option B relies on vendor statements, which may be unreliable. Option D strengthens contract language but does not ensure compliance at delivery.
Reference:
IIA Standards - Standard 2130: Control.

NEW QUESTION: 151
□□□ □□□□ □□ □□□ □□□ □□□ □□ □□ □□ □□ □□□□ □□□□□. □ □ □ □□ □□ □□□ □□□ □□□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□ □□
B. □□ □□□ □□ □□□ □□□□ □□
C. □□□ □□□□
D. □□ □□□ □□
Answer: C (LEAVE A REPLY)
In a vertically centralized organization, decision-making authority is concentrated at the top levels of management. As a company rapidly expands, maintaining tight control by a small management team can lead to inefficiencies, delays, and suboptimal decision-making due to limited input from operational and frontline staff.
Let's analyze each option:
* Option A: Lack of coordination among different business units
* Incorrect. While coordination challenges can exist in a large, decentralized organization, a tightly controlled, centralized structure typically ensures strong coordination but at the cost of slower decision-making.
* Option B: Operational decisions are inconsistent with organizational goals
* Incorrect. In a centralized structure, top management closely controls decision-making, making goal misalignment less likely.
* Option C: Suboptimal decision making
* Correct.
* Decentralized decision-making allows managers closer to operations to make informed, timely decisions.
* A small centralized team may lack specialized knowledge about different departments, leading to inefficient or outdated decisions.
* As the company expands, delays in decision-making and lack of responsiveness to market conditions increase risk exposure.
* IIA Reference: Internal auditors assess organizational structures to identify risks associated with inefficient decision-making and control bottlenecks. (IIA Standard 2110: Governance)
* Option D: Duplication of business activities
* Incorrect. Duplication of activities is more common in decentralized structures, where different departments operate independently. A tightly controlled, centralized structure reduces redundancy but at the cost of decision-making efficiency.

Thus, the verified answer is C. Suboptimal decision making.

NEW QUESTION: 152
□□ □□ □ □□□□ □□ □□□□ □□□□ □□ □□□□□?
A. □□□□ □□□ 2□□ □□□□□. □□□□ □□□ □□□ □□ □□ □□□ □□□ 3 □□ □□□□□.
B. □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□ □□ □□□□ □□□□□.
C. □□□□ □□□□□ □□□□ □□□□ □□□□ □□ □□□ □□□□□.
D. □□□□ □□□ □□ □ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
A router and a switch serve different functions in a network.
* A router is responsible for connecting multiple networks together and directing data packets between them. It determines the best path for data to travel using IP addresses.
* A switch, on the other hand, operates within a single network and connects devices like computers, printers, and servers. It uses MAC addresses to forward data within the local network (LAN).
* A. A router operates at layer two, while a switch operates at layer three of the OSI model - Incorrect. A switch operates at Layer 2 (Data Link Layer), while a router operates at Layer 3 (Network Layer).
* B. A router transmits data through frames, while a switch sends data through packets - Incorrect
. Switches use frames at Layer 2, while routers use packets at Layer 3.
* C. A router connects networks, while a switch connects devices within a network (Correct Answer) - This correctly differentiates their functions.
* D. A router uses a media access control (MAC) address during the transmission of data, while a switch uses an internet protocol (IP) address - Incorrect. A switch uses MAC addresses, and a router uses IP addresses.
* IIA GTAG 17 - Auditing IT Governance discusses network security and the role of routers and switches.
* COBIT 2019 - DSS01 (Managed Operations) emphasizes secure and efficient network management.

* NIST SP 800-53 - Security Controls for IT Systems includes guidelines on network architecture and device functionality.
Explanation of Each Option:IIA References:

NEW QUESTION: 153
□□ □ □□□ □□□ □□ □□□□ □□ □□ □□□□□?
A. □□□ □□□ □□ □□□□□ □□□□ □□□.
B. □□□ □□ □□□ □ □□ □□□ □□□ □□□ □□□□ □□□.
C. □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□.
D. □□ □□□□ □□□□□ □□□□□ □□□ □□□ □□□□ □□□□ □□□.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
The tape rotation schedule is a method used to manage and organize backup media to ensure data is retained for the required period and can be restored when necessary. Different rotation schemes, such as Grandfather- Father-Son (GFS), determine how long each backup tape is kept before being overwritten, directly affecting data retention policies. While real-time backups (option A) provide continuous data protection, they are not always necessary or practical for all systems. Storing backups onsite (option B) offers quick access but may not protect against site-specific disasters; offsite storage is often recommended. Regular restoration tests (contrary to option D) are essential to ensure backup integrity and reliability, not just in failure scenarios.

NEW QUESTION: 154
□□ □□□□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□ □□□□. □□□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□□. a. □□ □ □ □□□□□ □□ □□□□ □□ □□?
A. □□□□ □□□ □□ □□□□ □□□□□ □□□□.
B. □□□□ □□□ □□□□ □□ □□□□ □□□□,
C. □□□□ □□□ □ □□ □□□□□ □□□□ □□ □□□□ □□□□ □□□□.
D. □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
In data analytics, cleaning the data is a crucial step where the auditor eliminates redundancies, corrects inconsistencies, and removes errors to ensure accurate analysis. This step is taken before analyzing the data to identify high-risk areas and relevant processes.
* Correct Answer (C - Cleaning the Data in Preparation for Determining Involved Processes)
* Data cleaning involves:
* Removing duplicate entries to prevent misinterpretation.
* Standardizing data formats for consistency.
* Handling missing or inaccurate values to ensure reliability.

* This step prepares the data for analysis and identification of high-risk processes.
* The IIA's GTAG 16: Data Analysis Technologies emphasizes data cleaning as a critical part of internal audit analytics.
* Why Other Options Are Incorrect:
* Option A (Normalizing data in preparation for analyzing it):
* Normalization refers to structuring data efficiently (e.g., in databases) but does not necessarily involve eliminating redundancies in the way described.
* Option B (Analyzing data in preparation for communicating results):
* The auditor is still in the data preparation phase, not the analysis or reporting phase.
* Option D (Reviewing data prior to defining the question):
* The auditor is already working with data. Defining questions typically happens before data collection.
* GTAG 16: Data Analysis Technologies - Covers data preparation, cleaning, and analytics in internal auditing.
* IIA Practice Guide: Data Analytics in Internal Auditing - Outlines best practices for data validation and cleaning.
Step-by-Step Explanation:IIA References for Validation:Thus, cleaning the data (C) is the correct answer, as it ensures data integrity before identifying relevant processes and risks.

NEW QUESTION: 155
□□ □□ □□□□ □□□ □□ □□ □□□□□□ □□□□□ □□□. □□ □□ □□ □ □ □ □□□□□ □□□ □□ □□□□ □□ □□□□ □□□ □□□ □ □□ □□ □□□ □□?
A. □□ □□ □□.
B. □□□□ □□ □□.
C. □□ □ □□.
D. □□ □□ □□.
Answer: (SHOW ANSWER)
Planning (ERP) software implementation, to evaluate whether the organization is prepared for the change. This type of audit helps identify potential risks, resource availability, process gaps, and stakeholder alignment, which are critical for successful implementation.
* A. Readiness assessment (Correct Answer) - This assessment evaluates if the organization has the necessary resources, technology, and processes in place for a successful ERP implementation.
* B. Project risk assessment - While a project risk assessment identifies potential threats to project success, it does not provide an overall assurance on readiness before implementation.
* C. Post-implementation review - This is conducted after the project is completed and does not help assess the likelihood of success before implementation.
* D. Key phase review - This approach evaluates progress during implementation but does not provide enterprise-wide assurance before starting the project.

* IIA GTAG 12 - Auditing IT Projects recommends a readiness assessment before launching major IT initiatives.
* IIA IPPF Standard 2120 - Risk Management emphasizes identifying pre-implementation risks to improve project success.
* COBIT 2019 - APO03 (Managed Enterprise Architecture) supports readiness evaluations before system rollouts.
Explanation of Each Option:IIA References:

NEW QUESTION: 156
□□ □ □□ □□□ □□□ □□□□ □□ □□ □□?
A. □□□□ □□□ □□□ □□□ □□□□ □□□□□ □□ □ □□□□□ □□ □□□ □ □ □□□ □□□ □ □□□□.
B. □□ □□ □□ □ □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□ □ □□□□ □□□ □ □□□□.
C. □□□□□□□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□ □□ □□□□□ □□□ □□□ □ □□□□.
D. □□□ □ □□ □□□□□□ □□□ □□□ □ □□□ □□□ □ □□ □□□ □ □□□ □□□.
Answer: B (LEAVE A REPLY)
The Internet of Things (IoT) refers to a network of interconnected physical devices that collect and exchange data through the internet. The key benefits of IoT include automation, improved decision-making, cost savings, and efficiency gains.
* (A) Employees can choose from a variety of devices they want to utilize to privately read work emails without their employer's knowledge.
* This is incorrect because it focuses on unauthorized access rather than a benefit of IoT. Security and monitoring are major concerns in IoT environments.
* IIA Standard 2110 - Governance requires organizations to ensure adequate governance structures for IT and data security.
* (B) Physical devices, such as thermostats and heat pumps, can be set to react to electricity market changes and reduce costs. #
* This is correct because IoT enables smart devices to automatically adjust based on real-time data.
* Example: Smart thermostats (e.g., Nest, Honeywell) use IoT to track energy prices and consumption, adjusting temperatures to optimize efficiency.
* IIA Practice Guide "Assessing the Governance of Risks in IT Projects" highlights IoT as a tool for operational efficiency and cost savings.
* (C) Information can be extracted more efficiently from databases and transmitted to relevant applications for in-depth analytics.
* This relates more to big data and data analytics, not necessarily IoT.
* IIA GTAG "Auditing IT Governance" discusses IoT in operational efficiency but distinguishes it from data extraction.

* (D) Data mining and data collection from the internet and social networks is easier, and the results are more comprehensive.
* This describes AI and machine learning rather than IoT, which primarily connects physical devices.
* IIA GTAG "Auditing Cybersecurity Risk" highlights IoT risks but does not emphasize social media data mining.
* IIA GTAG (Global Technology Audit Guide) - "Auditing IT Governance"
* IIA GTAG - "Assessing the Governance of Risks in IT Projects"
* IIA Standard 2110 - Governance
* IIA GTAG - "Auditing Cybersecurity Risk"
Analysis of Answer Choices:IIA References:Thus, the most appropriate answer is B because IoT improves efficiency by automating energy consumption based on market conditions.

NEW QUESTION: 157
□□ □ □□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□□?
A. □□ □□□□□ □□ □□□□□ □□ □□□□ □□□ □□□□ □□□□ □□□□□ □□.
B. □□□ IT □□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□ □□ □□□□ □□ □□ □□□□ □□□□ □□ □□ □□□□ □□□□□□.
C. □□ □□□ □□□ □□ □□ □□□□ □□ □□□ □□□□□□ □□□□ □□□□ □ □□□ □□ □□□□□ □□□□ □□
D. □□ □□□□ □□□□ □□ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□ □ □ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
* Understanding Spear Phishing Attacks:
* Spear phishing is a targeted cyberattack where attackers send personalized emails to trick individuals into providing sensitive data (e.g., passwords, financial information).
* Unlike regular phishing, which casts a wide net, spear phishing is highly customized and often appears to come from a trusted source.
* Why Option C Is Correct?
* The scenario describes a highly personalized email (related to a golf membership) that tricks the recipient into clicking a malicious hyperlink and entering sensitive data.
* This matches the definition of a spear phishing attack, where an attacker tailors a scam specifically for an individual.
* IIA GTAG 16 - Data Analytics and ISO 27001 emphasize the need for security awareness training to mitigate such threats.
* Why Other Options Are Incorrect?
* Option A (Website attack causing a server crash):
* This describes a Denial-of-Service (DoS) attack, not spear phishing.
* Option B (Generic recorded message requesting password data):

* This is vishing (voice phishing), not spear phishing. Spear phishing relies on personalized emails.
* Option D (Fake social media investment opportunity):
* This describes mass phishing, which targets multiple users, unlike spear phishing, which is highly targeted.
* Spear phishing is a targeted attack that uses personal details to deceive individuals, making option C the best choice.
* IIA GTAG 16 and ISO 27001 emphasize cybersecurity awareness to prevent such attacks.
Final Justification:IIA References:
* IIA GTAG 16 - Data Analytics in Cybersecurity Audits
* ISO 27001 - Cybersecurity Best Practices
* NIST SP 800-61 - Incident Response Guidelines for Phishing Attacks

NEW QUESTION: 158
□□ □□□ □□□ □□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□□ □ □□□ □□ □□□□□. □□ □ □□ □□□□ □□ □□□ □□□□□?
A. □□□.
B. □□ □□□.
C. □□□□□□□(CFO).
D. □□ □□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Capital budgeting involves long-term investment decisions, such as purchasing new equipment, expanding facilities, or launching new products. These strategic financial decisions require approval at the highest level of governance.
The Board of Directors (Option A) is responsible for reviewing and approving capital budgets, ensuring alignment with corporate strategy.
Senior management (Option B) and the CFO (Option C) contribute by evaluating proposals, but they typically do not have final approval authority.
Accounting personnel (Option D) manage financial reporting but do not approve budgets.
Thus, the Board of Directors (A) is the correct answer.
Reference: IIA Financial Management - Capital Budgeting Approval Process

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

A decentralized organizational structure distributes decision-making authority across different business units or geographic regions. One major advantage is the ability to tap into a larger talent pool, as decision- making is not restricted to headquarters, and leadership opportunities exist at multiple levels.
* (A) Greater cost-effectiveness.
* Incorrect. A decentralized structure often increases costs due to duplicate resources, additional oversight, and inefficiencies from fragmented decision-making.
* (B) Increased economies of scale.
* Incorrect. Centralized organizations benefit more from economies of scale because they can standardize processes and consolidate purchasing power. Decentralization reduces these benefits by spreading decision-making across multiple locations.
* (C) Larger talent pool. #
* Correct. Decentralization allows organizations to recruit, develop, and retain talent in different locations, rather than relying solely on headquarters for leadership roles.
* This aligns with IIA Standard 2110 - Governance, which emphasizes the importance of leadership distribution and talent management in organizations.
* (D) Strong internal controls.
* Incorrect. Centralized structures typically have stronger internal controls, as decision-making and risk management are closely monitored. Decentralization increases the risk of inconsistent controls across different units.
* IIA Standard 2110 - Governance
* COSO Framework - Organizational Structure and Risk Management
* IIA GTAG - "Auditing Business Strategy Alignment"
Analysis of Answer Choices:IIA References:Thus, the correct answer is C, as decentralization expands the talent pool by enabling local decision-making and leadership development.

NEW QUESTION: 160
□□ □□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□ □□□ □ □□□□ □□ □□□□□ □□ □□□ □□ □□□□. □□ □ □□□ □□ □□□□□ □ □ □□□ □□ □ □□□ □□ □□□□□?
A. □□□□ □□.
B. □□ □□
C. □□ □□.
D. □□□ □□.
Answer: C (LEAVE A REPLY)
Extrinsic rewards are external incentives that motivate an employee to perform a task or stay in a job. These rewards include salary, bonuses, benefits, promotions, and other tangible incentives. In this case, the sales manager explicitly states that she remains in the organization because of the high bonuses, making this an example of extrinsic motivation.
* (A) Incorrect - Intrinsic reward.

* Intrinsic rewards are derived from internal satisfaction, such as personal growth, job fulfillment, or passion for work.
* Since the manager stays primarily for monetary bonuses rather than job satisfaction, this is not intrinsic motivation.
* (B) Incorrect - Job enrichment.
* Job enrichment involves enhancing job roles by adding responsibilities, autonomy, or variety to improve motivation.
* The scenario does not mention job enhancement as a reason for staying.
* (C) Correct - Extrinsic reward.
* High bonuses are a classic example of extrinsic motivation.
* The manager is staying for financial incentives rather than job satisfaction.
* (D) Incorrect - The hierarchy of needs.
* Maslow's Hierarchy of Needs explains different levels of human motivation, but the question asks for a specific type of motivation rather than a broad theoretical framework.
* IIA's Guide on Human Resources Risk Management
* Highlights the impact of extrinsic vs. intrinsic motivation on employee retention.
* COSO's ERM Framework - Employee Retention and Performance Management
* Discusses the role of financial incentives in retaining employees.
* IIA's Global Internal Audit Standards - Organizational Behavior and Employee Motivation
* Explains intrinsic vs. extrinsic rewards in workforce management.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 161
□□ □ □□□□ □□□ □□ □□□ □□ □□□□□?
A. □□ □□ □□ □□□ □□□□ □□□, □□□, □□□□□ □□□ □□□□□ □□□ □□ □□□□□.
B. □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□ □ □□ □□.
C. □□ □□□ □□, □□ □ □□□□ □□□□□ □□□□ □□ □□□ □□ □□□ □ □ □□□.
D. □□ □□□ □□□ □□□□ □□ □□□ □□ □□□□□ □□ □□□ □□□ □□ □ □□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
A matrix organization combines functional and product-based structures, allowing employees to work across multiple departments and report to multiple managers. This enables businesses to utilize expertise from various areas efficiently.
Option A (Unity of command) does not apply to matrix organizations, as employees often report to multiple supervisors.
Option C (Variable authority and accountability) is a secondary characteristic but does not define matrix structures.

Option D (Best for scattered locations/multi-line firms) applies more to divisional rather than matrix structures.
Thus, the correct answer is B, as matrix structures enable collaboration across functional and product teams.
Reference: IIA Business Acumen - Organizational Structures

NEW QUESTION: 162
□□ □ □□□□□□ □□□ □□ □□□□□?
A. □□ □□ □□ □□ □□
B. □□□ □□□ □□ □□□□
C. □□□ □□□ □□ □□□ □□□
D. □□□ □ □□□ □□
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Application controls are specific to software applications and help ensure data integrity and accuracy within systems.
Option A (Automated password change requirements) - A system security control, not specific to a single application.
Option B (System data backup) - A general IT control, not an application control.
Option C (User testing of system changes) - Part of software development controls, not an application-level control.
Formatted data fields ensure that users enter information in the correct format, preventing errors and improving data accuracy.
Since formatted data fields are an application-specific control, Option D is correct.
Reference: IIA IT Controls - Application Security & Data Integrity

NEW QUESTION: 163
□□ IT □□□□□ □□ 3□□ □□ □□□ □□□□□. □□□□□□□(CAE)□ □□□□ □□ □□□ □□ □□□ □□□□□□. □□□ □□□□□ □□□ □□□ □□ □□□□□ □□ □□ □□□□□□□. □ □□ CAE□ □□□ □□ □□□?
A. □□ □□□□ □□ □□□ □□ □□□□□ □□□ □□ □□□□□ □□□ IT □□□□ □□□□□ □□□□□.
B. □□ □□□ □□ □□□□ □□ □□ □□□ □□□□□ □□ □□□ □ □□□□□ □ □□□□.
C. □□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □ □□□ □□□□□.
D. □□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □ □□ □□ □□□ □□ □ □ □□□ □□□.
Answer: C (LEAVE A REPLY)
The internal audit plan must remain dynamic and responsive to changes in circumstances. If a key project is postponed, the CAE should amend the audit plan, reallocate resources

appropriately, and inform the board and senior management for review and approval. This ensures transparency and continued alignment with organizational risks.
Option A improperly shifts audit resources under management's direction. Option B may be considered but requires board and management approval through an amended plan.
Option D leaves resources idle, which is inefficient.
Reference:
IIA Standards - Standard 2020: Communication and Approval.

NEW QUESTION: 164
□□□□□ 2□□ □□ □□□ □□□, □□□ □□□□ □□ □□ □□□□ □□□ □□□ □□?
A. □□□ □□.
B. □□□ □□.
C. □□ □□ □ □□.
D. □□ □□□ □□ □□.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Herzberg's Two-Factor Theory identifies:
Motivators (Intrinsic factors) - Lead to job satisfaction (e.g., responsibility, recognition, growth).
Hygiene factors (Extrinsic factors) - Prevent dissatisfaction but do not create motivation (e.g., salary, work conditions).
Option A (Salary and status) - Hygiene factors that prevent dissatisfaction but do not drive motivation.
Option C (Work conditions and security) - Also hygiene factors, not motivators.
Option D (Peer relationships and personal life) - Affect job satisfaction indirectly, but are not primary motivators.
Since responsibility and advancement directly drive motivation, Option B is correct.
Reference: IIA Human Resource Management - Employee Motivation Theories

NEW QUESTION: 165
□□ □ □□□ □□ □□ □□□□ □□□□ □3□ □□□□□ □□□□ □□ □□□□□?
A. □□ □□ □□□□(VAN).
B. □□□ □□□(LAN).
C. □□□ □□□□(MAN).
D. □□ □□□□(WAN).
Answer: (SHOW ANSWER)
A Value-Added Network (VAN) is a third-party network service that securely connects an organization with its trading partners, facilitating secure electronic data interchange (EDI) and business communications.
* (A) Value-added network (VAN). (Correct Answer)

* A VAN is a private, managed network service that provides secure data transmission between business partners.
* It is commonly used for B2B transactions, supply chain management, and EDI.
* IIA GTAG 7 - IT Outsourcing recognizes VANs as critical third-party networks for secure business data exchange.
* (B) Local area network (LAN).
* Incorrect: A LAN connects computers within a limited area (e.g., an office or building), but it is not designed for external trading partner connections.
* (C) Metropolitan area network (MAN).
* Incorrect: A MAN covers a city or region, but it is not designed for B2B communication.
* (D) Wide area network (WAN).
* Incorrect: A WAN connects multiple geographic locations, but it is a general networking term, not specific to trading partner communications.
* IIA GTAG 7 - IT Outsourcing: Discusses the use of third-party networks like VANs for secure data exchange.
* IIA Standard 2110 - Governance: Recommends secure third-party integration for business continuity and security.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (A) Value- Added Network (VAN) because it is specifically designed for secure communication between an organization and its trading partners.

NEW QUESTION: 166
□□□□ □□□□ □□□□ □□□ □□ □□□ □□ □□□□ □□ □□ □□ □□□ □□ □ □□□□□. □□ □ □□□ □□□ □□□ □□□□□?
A. □□ □□.
B. □□ □□ □□□.
C. □□□
D. □□
Answer: (SHOW ANSWER)
* Understanding Vertical Integration:
* Vertical integration is a business strategy where a company expands its operations into different stages of its supply chain.
* In this case, the chocolate-producing company is moving upstream by producing its own milk rather than purchasing it from suppliers.
* Why This Is Vertical Integration:
* The company controls more of its supply chain, reducing dependency on external suppliers.
* Benefits include:
* Cost savings on raw materials (by producing instead of buying).
* Improved quality control (since the company controls milk production).
* Greater market control (reducing reliance on third-party vendors).

* Why Other Options Are Incorrect:
* B. Unrelated diversification - Incorrect.
* Unrelated diversification occurs when a company expands into a completely different industry (e.g., a chocolate company entering the technology sector).
* C. Differentiation - Incorrect.
* Differentiation refers to creating unique products to gain a competitive advantage, but the strategy here is about controlling supply, not product uniqueness.
* D. Focus - Incorrect.
* Focus strategy targets a narrow market segment, but this scenario involves expanding into the supply chain, not focusing on a niche.
* IIA's Perspective on Business Strategy and Risk Management:
* IIA Standard 2120 - Risk Management requires auditors to assess the risks and benefits of vertical integration strategies.
* COSO ERM Framework advises monitoring operational and financial risks associated with supply chain integration.
* Porter's Value Chain Model supports vertical integration as a way to enhance operational efficiency and cost control.
IIA References:
* IIA Standard 2120 - Risk Management in Business Strategy
* COSO ERM - Managing Vertical Integration Risks
* Porter's Value Chain Model - Supply Chain Control
Thus, the correct and verified answer is A. Vertical integration.

NEW QUESTION: 167
□□ □ □□□ □□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□ □□□□□?
A. □□□ □□□
B. □□ □□□ □□.
C. □□ □□.
D. □□□ □□□ □□□ □□
Answer: D (LEAVE A REPLY)
* Understanding the Financing Section of a Cash Budget:

* A cash budget is a financial plan that outlines expected cash inflows and outflows over a specific period.
* The financing section records activities related to borrowing, repaying debt, issuing securities, and managing interest payments.
* Why Debt and Interest Payments Belong in the Financing Section:
* Debt repayment (principal and interest) is a financial activity rather than an operational or investing activity.
* Companies must plan for financing costs to ensure liquidity and compliance with loan agreements.
* Why Other Options Are Incorrect:
* A. Collections from customers - Incorrect.
* Customer payments belong in the operating section of the cash budget, as they represent core business activities.
* B. Sale of securities - Incorrect.
* The sale of securities is an investing activity unless related to issuing new debt or equity.
* C. Purchase of trucks - Incorrect.
* Buying trucks is a capital expenditure, which belongs in the investing section of the cash budget.
* IIA's Perspective on Financial Planning and Budgeting:
* IIA Standard 2120 - Risk Management requires organizations to assess financial risks, including debt repayment obligations.
* COSO ERM Framework highlights the importance of cash flow forecasting to maintain financial stability.
* GAAP and IFRS Financial Reporting Standards classify debt repayment and interest under financing activities.
IIA References:
* IIA Standard 2120 - Risk Management & Cash Flow Oversight
* COSO ERM - Financial Planning and Liquidity Management
* GAAP & IFRS - Cash Flow Statement Classifications
Thus, the correct and verified answer is D. Payment of debt, including interest.

NEW QUESTION: 168
□□ □ □□ □□□□□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□ □ □□□ □□ □□□□□?
A. □□ □□□□□ □□ □□ □□ □□□ □□□□□ □□ □□□ □□ □□□□ □□□ □□□ □□□□□.
B. □□ □□□□□ □□□ □□□□□ □□ □□ □□, □□ □□ □ □□□ □□□ □□□ □□.
C. □□ □□□□□ □□□□ □□□□□ □□□ □□□ □□□ □□ □□□□ □□□□□ □.
D. □□ □□□□ □□□□ □□□ □□□□ □□□ □□ □□□ □□□□□□.

Answer: B (LEAVE A REPLY)
When auditing logical access controls for a workstation, the focus should be on user authentication methods
, including:
* Password policies (length, complexity, change frequency)
* User access rights and permissions
* Login activity logs to detect unauthorized access attempts
* Correct Answer (B - Reviewing Password Policies and User List for Login Process)
* Logical access controls ensure only authorized users can access a workstation.
* Reviewing password length, complexity, and change frequency helps assess if security best practices are followed.
* Reviewing the list of authorized users ensures that only appropriate personnel have access.
* The IIA's GTAG 9: Identity and Access Management recommends evaluating password policies and user access lists as key control measures.
* Why Other Options Are Incorrect:
* Option A (Reviewing access badges and room logs):
* Physical access controls are important but do not assess logical access (login security, user authentication).
* Option C (Reviewing failed access attempts and error messages):
* Reviewing failed login attempts identifies security breaches but does not directly assess password policies or user access lists.
* Option D (Reviewing unsuccessful passwords and activity logs):
* Passwords should not be reviewed due to privacy and security policies. Logs should be checked, but reviewing actual passwords is a security violation.
* IIA GTAG 9: Identity and Access Management - Covers password controls and user authentication.
* IIA Practice Guide: Auditing IT Security Controls - Recommends reviewing password policies as a key security measure.
Step-by-Step Explanation:IIA References for Validation:Thus, B is the correct answer because reviewing password policies and user lists is essential for auditing logical access controls.

NEW QUESTION: 169
□□ □□□ □□ □□ □ □□□ □□□ □□□ □□ □□□ □□ □□ □□ □□□□□?
A. □□ □.
B. □□□.
C. □□ □□□.
D. □□□ ID □ □□□□□□□.
Answer: C (LEAVE A REPLY)
* Understanding Physical Access Controls:

* Physical access controls protect assets by preventing unauthorized access and detecting potential security violations.
* Controls can be preventive (stop incidents from occurring) or detective (identify incidents after they occur).
* Why Surveillance Cameras Function as Both Preventive and Detective Controls:
* Preventive: The presence of cameras discourages unauthorized access and malicious activities.
* Detective: If an incident occurs, cameras provide recorded evidence for investigation and accountability.
* Why Other Options Are Less Suitable:
* A. Locked doors - Purely preventive, as they block unauthorized access but do not detect breaches.
* B. Firewalls - Primarily an IT security measure, not a physical access control.
* D. Login IDs and passwords - These are logical (IT) access controls, not physical controls.
* IIA GTAG 15 - Auditing Privacy and Security Risks: Highlights the dual role of surveillance as a preventive and detective control.
* IIA Standard 2120 - Risk Management: Encourages controls that both prevent and detect risks.
* COSO's Internal Control Framework: Supports security measures that serve multiple control functions.
Relevant IIA References:# Final Answer: Surveillance cameras (Option C).

NEW QUESTION: 170
□□ □ □□ □□□□ □□□ □□ □□ □□ □□□ □□□ □□□□□?
A. □□□
B. □□
C. □□
D. □□□
Answer: B (LEAVE A REPLY)
* Understanding How IoT Impacts Data Attributes:
* The Internet of Things (IoT) refers to connected devices that continuously collect and transmit data in real-time.
* IoT generates massive amounts of data at high speeds, affecting the velocity of data processing and analysis.
* Why Velocity is the Most Affected Attribute:
* Velocity refers to the speed at which data is generated, processed, and transmitted.
* IoT devices continuously stream data, requiring real-time or near-real-time processing.
* Examples include:
* Smart sensors in factories sending real-time equipment status.
* Wearable devices tracking health metrics every second.

* Smart cities using IoT for traffic monitoring and instant updates.
* Why Other Options Are Incorrect:
* A. Normalization - Incorrect.
* Normalization refers to organizing database structures, but IoT deals with data transmission speed rather than database design.
* C. Structuration - Incorrect.
* Structuration relates to how data is formatted (structured vs. unstructured), but IoT's biggest challenge is real-time data flow.
* D. Veracity - Incorrect.
* Veracity concerns data accuracy and reliability, which is a challenge in IoT but not the most significant impact compared to velocity.
* IIA's Perspective on IoT and Data Management:
* IIA Standard 2110 - Governance emphasizes the need for robust data processing frameworks to handle IoT-generated data velocity.
* IIA GTAG (Global Technology Audit Guide) on Big Data highlights real-time data analytics and IoT challenges.
* ISO 27001 Information Security Standard recommends ensuring real-time data processing controls for IoT security and management.
IIA References:
* IIA Standard 2110 - IT Governance & Data Management
* IIA GTAG - IoT and Big Data Risks
* ISO 27001 - Information Security and Real-Time Data Processing
Thus, the correct and verified answer is B. Velocity.

NEW QUESTION: 171
□□ □□□ □□□□ □□□ □, □□ □□□□ □□ □ □□ □□□ □□□ □□□?
A. □□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
B. □□□□□ □□ □□ □□□ □□ □□ □□□ □□ □□□□□.
C. □ □□ □□□ "□□□"□ □□□□ □□ □□□ □□ □□□□ □□□□□□.
D. □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The auditor's responsibility does not end with reporting a control deficiency. The CAE must monitor progress and follow up periodically with management to confirm whether corrective actions have been implemented.
Option A stops at documentation and fails to ensure corrective action. Option C incorrectly assumes no further audit is needed. Option D assigns management's responsibility to the auditor, which would impair independence.
Reference:
IIA Standards - Standard 2500: Monitoring Progress.

NEW QUESTION: 172

□ □□ □□□□□ 10,000□□ □□ 7□□□□ □□□□ □□ □□□ □□□□. □□□□ □ □□ □□ 10□□□ □□□□□. □□ □□ □□□ □□ 55□□□□ □□ □□ □□□ □□ 3□□. □□□□□ □□□ □□□□□ □□ □ □□ □□□ □□□□ □□□?

A. □□ □ □□ □□ □□□ □□ □□ □□□□ □□□□.

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

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

D. □□□□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

When evaluating a special order, the manufacturer must determine if accepting it will be profitable without disrupting normal operations. The key consideration is whether the company has spare production capacity to handle the order without increasing fixed costs.

* Correct Answer (B - The Manufacturer Can Fulfill the Order Without Expanding Production Facilities)
* Fixed costs ($3 per unit) are already incurred and will not change if the order is accepted.
* The special price ($7 per unit) covers the variable costs ($5 per unit), contributing $2 per unit to profit.
* If the manufacturer has excess production capacity, the order is profitable.
* The IIA Practice Guide: Auditing Financial Performance emphasizes that special order decisions should be based on incremental cost analysis, ensuring no need for capacity expansion.
* Why Other Options Are Incorrect:
* Option A (Fixed and Variable Manufacturing Costs Are Less Than the Special Offer Selling Price):
* Fixed costs should not be considered in short-term pricing decisions if they are already incurred.
* Option C (Costs Related to Accepting This Offer Can Be Absorbed Through the Sale of Other Products):
* The decision should be based on whether the order is profitable on its own, not relying on other products.
* Option D (The Manufacturer's Production Facilities Are Operating at Full Capacity):
* If the company is at full capacity, accepting the order would require sacrificing existing sales or expanding capacity, which increases costs.
* IIA Practice Guide: Auditing Financial Performance - Discusses cost analysis for special pricing decisions.
* IIA GTAG 13: Business Performance - Covers incremental cost and profitability analysis in pricing decisions.

Step-by-Step Explanation:IIA References for Validation:Thus, B is the correct answer because accepting the order is only profitable if the manufacturer has excess capacity.

NEW QUESTION: 173

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

A. □□□ □□□ □□□ □□□□□.

B. □□□□ □□□□ □□□□ □□□ □□□□□□.

C. IT □□□□ □□ □□□ □□□ □□□ □□□□□.

D. □□□ □□ □□□ □□□□ □ □□□ □□□ □□

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:

Prioritizing the restoration of business systems requires input from multiple departments because different teams depend on various systems for operations.

Option A (Backup frequency) - Typically an IT decision, with minimal department-wide input.

Option C (Assigning IT personnel) - An internal IT function.

Option D (Assessing recovery resources) - Primarily handled by IT and finance, but restoration priorities require broader input.

Since business continuity planning involves multiple stakeholders, Option B is correct.

Reference: IIA IT Disaster Recovery - Business Continuity Planning Framework

NEW QUESTION: 174

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

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

B. □□□□ □□ □□□ IT□□□ □□

C. □□□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□

D. □□□□ IT□□□□ □□□ □□□

Answer: B (LEAVE A REPLY)

According to IIA Standards, engagement communications must be complete, objective, and balanced. When disagreements arise, the auditor should present both the audit team's findings and management's perspective so senior management and the board can make informed decisions.

Option A is excessive; raw correspondence is not necessary. Option C omits management's opinion, reducing objectivity. Option D limits reporting to agreed items only, which would conceal significant unresolved issues.

Reference:

IIA Standards - Standard 2410: Criteria for Communicating.

NEW QUESTION: 175

□□□ □□□ □□ □□ □□□ □□(EDI)□ □□ □□ □□(EFT)□ □□ □□□□ □□ □ □□ □□□□ □□□ □□□ □□ □ □□ □□□□?

A. □□ □□□ □□□ □□□ □□□□□.
B. □□ □□□ □ □□□□.
C. □□□ □□.
D. □□□□ □□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
E-commerce systems that automate purchasing and billing typically lead to:
Faster procurement cycles due to automated ordering.
Increased accounts payable, as more transactions are processed quickly.
Option A (Higher cash flow) - Unlikely, since faster billing does not always improve cash flow.
Option B (Higher inventory balances) - Incorrect, as e-commerce often enables just-in-time inventory.
Option C (Higher accounts receivable) - E-commerce speeds up collections, reducing receivables.
Since automated purchasing increases outstanding payments, Option D is correct.
Reference: IIA Financial Management - E-Commerce & Accounts Payable

NEW QUESTION: 176
□□ □□ □□□□ □□ □□ □□□ □□□ □□□ □□□□□ □□□ □□ □□□□ □□ □ □□□□□?
A. □□ □□ □□□ □□
B. □□ □□□□
C. □□ □□ □
D. □□ □□ □□□□□
Answer: (SHOW ANSWER)
The CAE must prioritize engagements based on risk assessment. A risk matrix (considering likelihood and impact of risks) provides the starting point to evaluate which areas of the audit universe present the highest exposure and should be included in the plan.
Option A (maturity model) helps evaluate risk management capability but is not the starting point. Option C (assurance map) supports coordination but follows the risk assessment.
Option D (control framework) provides criteria but not prioritization.
Reference:
IIA Standards - Standard 2010: Planning.

NEW QUESTION: 177
□□ □ □□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□?
A. □ □ □□ □□□
B. □□□ □□□ □□
C. □ □ □□ □
D. □□□ □□ □□

Answer: (SHOW ANSWER)
Reference: IIA Business Knowledge for Internal Auditing, Decentralization Advantages section.

NEW QUESTION: 178
□□ □□□ □□□□□□□(CAE)□ □□ □□ □□□ □□□□□. CAE□ □□ □□□ □ □□□□ □□□ □□□ □□ □□ □□□. □□ □□□□ □□ □□ □□□ □□□ □, □□ □□ □□□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□. □□ □ □ □ □□ □□□ □ □□ □□ □□□□□?
A. □□ □□□ □□ □□ □□□ □□□ □□ □□□□□□□ □□ □□□□□ □□□□□.
B. □□ □□□ □□□ □□ □□ □□□□ □□□□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □□□□□.
C. □□□ □□□ □□ □□ □□□□ □□□ □□ □□ □□ □□□ □□ □□□ □□□□ □.
D. □□□□□□ □□□□□□□ □□ □□□□□□□ □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
Exit meetings are intended to ensure that engagement clients clearly understand the observations, conclusions, and recommendations of the internal audit activity. The IIA's International Standards for the Professional Practice of Internal Auditing emphasize that communication should be clear, constructive, and timely.
Providing engagement clients with written summaries of the observations before the exit meeting allows them to review the facts, prepare questions, and understand the basis for the observations. This preparation improves dialogue, reduces confusion, and increases the effectiveness of the meeting.
Option B is less effective because it limits client engagement and postpones resolution of disagreements.
Option C is impractical, as reading the full draft report during the meeting is time-consuming and may overwhelm clients. Option D eliminates the opportunity for discussion and relationship building with management, which is a critical part of audit communication.
Reference:IIA's International Standards for the Professional Practice of Internal Auditing (Standards 2400 - Communicating Results, Practice Advisory 2410-2).

NEW QUESTION: 179
□□ □ □□□□□ □□ □ □□□ □□?
A. □□□ □□□ □□ □□□ □□□□ □□□□□.
B. □□ □□ □□□□□.
C. □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□□.
D. □□□□ □□ □□□□□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
Depreciation is the systematic allocation of an asset's cost over its useful life. It reflects how much of the asset's value is used up in each accounting period.

* Spreads Cost Over Time - Instead of expensing the total cost immediately, depreciation distributes it across multiple periods.
* Matches Expenses with Revenue - Ensures that the cost of long-term assets is allocated in the periods they generate revenue.
* Required for Financial Reporting - Compliance with GAAP and IFRS requires proper allocation of asset costs.
* B. It is a process of asset valuation - Incorrect because depreciation does not determine market value; it only spreads cost over time.
* C. It is a process of accumulating adequate funds to replace assets - Incorrect because depreciation is an accounting concept, not a savings mechanism.
* D. It is a process of measuring decline in the value of assets because of obsolescence - Incorrect because depreciation allocates cost, not necessarily measuring value decline (which is impairment).
* IIA's GTAG on Financial Controls and Reporting - Defines depreciation as a cost allocation method.
* International Financial Reporting Standards (IFRS 16) & US GAAP (ASC 360) - State that depreciation is used to allocate asset costs over time.
* COSO's Internal Control Framework - Covers accounting treatments for fixed assets.
Why Depreciation is an Allocation Process?Why Not the Other Options?IIA References:#
Final Answer: A.
It is a process of allocating cost of assets between periods.

NEW QUESTION: 180
□□□□ □□□□ □□ □□□ □□□ □ □□ □□ □□□□ □□ □ □□ □□□ □□□ □ □□□□□?
A. □□ □□ □□
B. □□□□
C. □□ □□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
Reference: IIA Business Knowledge for Internal Auditing, Cost Accounting section.

NEW QUESTION: 181
□□□ □□ □□ □ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □ □□ □□□□ □□□□ □□□ □□ □□□ □□ □□□□□ □3□ □□□□□ □□□ □□□. □□ □ □□ □ □□□□ □□ □□□□□? □□ □□ □□□ □□ □ □□ □□□ □□□□□?
A. □□ □□□□ □□,
B. □□□□ □□ □□.
C. □□□□ □□ □□□□ □□ □□□□□.
D. □ □□ □□

Answer: D (LEAVE A REPLY)
A hot recovery plan (hot site) is a fully operational, duplicate site that is pre-configured and ready for immediate use in case of a disaster. This approach allows an organization to recover critical operations quickly with minimal downtime.
* (A) Cold recovery plan.
* Incorrect: A cold site is a facility that has infrastructure but no active IT systems or data until set up after a disaster, resulting in longer recovery times.
* (B) Outsourced recovery plan.
* Incorrect: Outsourcing recovery refers to third-party disaster recovery services, but does not specifically describe a fully operational duplicate site.
* (C) Storage area network recovery plan.
* Incorrect: A storage area network (SAN) recovery plan focuses on data storage redundancy, not a fully operational duplicate facility.
* (D) Hot recovery plan. (Correct Answer)
* A hot site is the fastest and most effective disaster recovery solution, ensuring immediate failover with minimal downtime.
* IIA GTAG 10 - Business Continuity Management highlights hot sites as the most effective for mission-critical operations.
* IIA GTAG 10 - Business Continuity Management: Recommends hot sites for critical recovery scenarios.
* IIA Standard 2120 - Risk Management: Emphasizes preparedness for disaster recovery planning.
Analysis of Each Option:IIA References Supporting the Answer:Thus, the correct answer is (D) Hot recovery plan, as it ensures a fully operational backup site for immediate disaster recovery.

NEW QUESTION: 182
□□ □□□□ □□□ □□□□ □□□□ □□, □□□ □ □□□ □□□□□. □ □□ □□ □ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□ □□□□□.
B. □□□□ □□□□ □□□□ □□□□□.
C. □□□□ □□□□ □□□□ □□□ □□□ □□□□□.

D. □□□□ □□□ □□□ □□□□□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

When an internal auditor calculates the mean (average), median (middle value), and range (difference between highest and lowest values) of a data population, the primary purpose is to assess the distribution of data and detect anomalies. Let's analyze the answer choices:

* Option A: To inform the classification of the data population.
* Incorrect. Classification typically involves categorizing data into specific groups, which requires different statistical or analytical techniques like clustering or decision trees. Mean, median, and range are more useful for identifying distribution patterns.
* Option B: To determine the completeness and accuracy of the data.
* Incorrect. While summary statistics can highlight extreme values, completeness and accuracy are usually assessed through data reconciliation, validation checks, and comparison with source records.
* Option C: To identify whether the population contains outliers.
* Correct.
* The range (difference between the largest and smallest values) helps to detect extreme values.
* The mean and median can show whether the data is symmetrical or skewed (which may indicate outliers).
* If the mean is significantly different from the median, it suggests potential outliers pulling the average in one direction.
* IIA Reference: Internal auditors use data analytics to detect anomalies and potential fraud by identifying outliers. (IIA GTAG: Auditing with Data Analytics)
* Option D: To determine whether duplicates in the data inflate the range.
* Incorrect. Duplicates may affect the data set, but range calculations alone do not determine whether duplicates exist. Duplicate identification usually involves checking for repeated entries, not just extreme values.

NEW QUESTION: 183

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

A. □□

B. □□□□ □□

C. □□□

D. □□ □□□

Answer: C (LEAVE A REPLY)

* Definition of a Firewall:
* A firewall is a network security device (hardware or software) that monitors and controls incoming and outgoing network traffic.
* It is designed to filter or prevent specific information from moving between internal and external networks, ensuring unauthorized access is blocked.

* How a Firewall Works:
* It uses rules and policies to determine whether to allow or block traffic.
* Firewalls can be configured to prevent malware, hacking attempts, and unauthorized data transfers.
* There are different types, including packet-filtering firewalls, stateful inspection firewalls, and next-generation firewalls (NGFWs).
* Why Other Options Are Incorrect:
* A. Authorization:
* Authorization refers to user access control, ensuring users have the correct permissions, but it does not filter network traffic.
* B. Architecture model:
* An architecture model defines the structure of an IT system but does not actively prevent or filter data movement.
* D. Virtual private network (VPN):
* A VPN encrypts data and provides secure remote access but does not filter or block data movement between networks.
* IIA's Perspective on IT Security Controls:
* IIA Standard 2110 - Governance emphasizes strong cybersecurity controls, including firewalls, to protect sensitive data.
* IIA GTAG (Global Technology Audit Guide) on Information Security recommends using firewalls as a primary defense mechanism.
* NIST Cybersecurity Framework and ISO 27001 Security Standards identify firewalls as critical tools for network security and data protection.
IIA References:
* IIA Standard 2110 - Governance and IT Security
* IIA GTAG - Information Security Risks
* NIST Cybersecurity Framework

NEW QUESTION: 184
□□ □ □□□□□□ □ □□□ □ □□ □□□ □□□ □□□□□?
A. □+□□(□□) □□
B. □□ □□ □□
C. □□ □□□□□.
D. □□ □□□.
Answer: A (LEAVE A REPLY)
The acid-test (quick) ratio is a more dependable liquidity indicator than working capital because it excludes inventory, which may not be easily converted to cash in the short term. This ratio measures a company's ability to pay its short-term liabilities using only its most liquid assets (cash, marketable securities, and accounts receivable).
Formula for the Acid-Test Ratio:Acid-Test Ratio=Current Assets#InventoryCurrent Liabilities\text{Acid-Test Ratio} = \frac{\text{Current Assets} - \text{Inventory}}{\text{Current

Liabilities}}Acid- Test Ratio=Current LiabilitiesCurrent Assets#Inventory This ratio is more reliable than working capital since it removes inventory, which may be difficult to liquidate quickly in financial distress.
* A. Acid-test (quick) ratio (Correct Answer) - This provides a stronger measure of liquidity because it excludes inventory, which might not be quickly converted to cash.
* B. Average collection period - This measures the efficiency of accounts receivable collections, but it does not directly measure overall liquidity.
* C. Current ratio - While this ratio is commonly used, it includes inventory, which can distort liquidity assessments if inventory is not easily sold.
* D. Inventory turnover - This measures how quickly inventory is sold, but it does not directly assess liquidity.
* IIA IPPF Standard 2130 - Control emphasizes liquidity monitoring as a key financial control.
* COSO ERM Framework - Financial Performance Measures discusses acid-test ratio as a critical liquidity metric.
* IFRS 7 - Financial Instruments Disclosures outlines the importance of liquidity risk assessments.
Explanation of Each Option:IIA References:

NEW QUESTION: 185
□ □□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□□□□. □□ □□, □□□ □□□ □□□□ □□ □□□ □□ □□□□ □□□ □□□□□, □□□ □□ □□ □□ □ □□ □□□ □□□□□□.
□□ □ □ □□□ □□ □□ □□ □□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□□ □□□□□
B. □□□ □□□ □□□□□
C. □□□□□ □□□□ □□□ □□□ □□□□□
D. □□□ □□□□ □□ □□ □□□ □□□□□
Answer: D (LEAVE A REPLY)
A root cause-based recommendation addresses the underlying problem rather than symptoms. In this case, the real issue is the spider infestation, which attracts the birds, which in turn leads to droppings that require harsh cleaning. By enhancing cleaning and displacement of spiders, the organization eliminates the root cause and prevents recurrence.
Options A, B, and C treat symptoms but do not address the true root cause.
Reference:
IIA Practice Guide - Audit Findings: Condition, Criteria, Cause, Effect, and Recommendation.

NEW QUESTION: 186

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

A. □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□.

B. □□□ □□□ □□ □ □□ □□ □□

C. □□ □□□ □□□ □□□□ □□□

D. □□□ □□□ □□□□ □□□ □□□□ □□

Answer: (SHOW ANSWER)

To assess the success of a piloted data analytics model in identifying anomalies in vendor payments and potential fraud, the most appropriate criterion is the accuracy of the model in identifying true positives-cases flagged as anomalies that were later confirmed as valid fraud risks.

* Effectiveness of the Model: The primary goal of the model is to enhance the internal audit activity's ability to detect fraudulent transactions. The best way to measure success is to analyze how many flagged transactions were confirmed as fraudulent or erroneous.
* Reduction of False Positives and False Negatives: A model that generates too many false positives (incorrectly flagged transactions) can lead to inefficiencies, while too many false negatives (missed fraudulent cases) can reduce the effectiveness of fraud detection.
* Alignment with Internal Audit Standards: According to IIA Standard 1220 - Due Professional Care, internal auditors must apply appropriate tools and techniques (such as data analytics) to enhance audit effectiveness. The model's success should be assessed based on its ability to provide reliable, actionable insights.
* IIA Practice Guide on Data Analytics: Recommends assessing the predictive accuracy of models by comparing flagged transactions against actual outcomes.
* B. The development and maintenance costs associated with the model (Incorrect)
* While cost is a consideration, it does not directly assess the effectiveness of the model in detecting fraud.
* High costs may indicate inefficiency, but they do not determine whether the model is accurately identifying fraudulent transactions.
* IIA Standard 2100 - Nature of Work emphasizes that internal audit activities must contribute to the improvement of governance, risk management, and control, which requires a focus on results rather than just cost.
* C. The feedback of auditors involved with developing the model (Incorrect)
* Feedback is useful but subjective. The ultimate test of success is not auditor perception but whether the model correctly identifies fraudulent or anomalous transactions.
* IIA Practice Guide: Auditing Data Analytics suggests that while stakeholder feedback is valuable, empirical validation (accuracy of flagged cases) should be the primary success measure.
* D. The number of criminal investigations initiated based on the outcomes of the model (Incorrect)

* While fraud detection can lead to investigations, the number of investigations is not necessarily an accurate measure of model success.
* Some flagged cases may not lead to criminal investigations due to materiality, lack of sufficient evidence, or management decisions.
* According to IIA Standard 2120 - Risk Management, internal auditors must evaluate fraud risk management effectiveness, which includes detecting and preventing fraud, not just the legal consequences.
Explanation of Answer Choice A (Correct Answer):Explanation of Incorrect Answers:Conclusion:The best success criterion for the piloted data analytics model is the percentage of cases flagged by the model and confirmed as positives (Option A), as it directly measures the model's effectiveness in detecting actual fraud cases.
IIA References:
* IIA Standard 1220 - Due Professional Care
* IIA Standard 2100 - Nature of Work
* IIA Standard 2120 - Risk Management
* IIA Practice Guide: Auditing Data Analytics

NEW QUESTION: 187
□□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□□ □□□□ □□□ □?
A. □□□ □□□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□□.
B. □□□□ □□□ □□ □□□ □ □□ □□□ □□ □□ □□ □□□ □□□□.
C. □□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□□ □.
D. □□□□ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
A core feature of blockchain technology is immutability-once data is recorded, it cannot be altered or deleted. While this supports integrity and transparency, it also creates a conflict with data privacy regulations such as the General Data Protection Regulation (GDPR), which grants individuals the "right to be forgotten." The inability to erase personal data stored on blockchain creates a compliance challenge.
Options A and B are incorrect: phishing is not inherent to blockchain, and transactions are not easily tampered with (immutability actually prevents that). Option C is misleading because regulations address data use but do not "overregulate" blockchain specifically.
Reference:
IIA Global Technology Audit Guide (GTAG): Understanding Blockchain and Related Risks.

NEW QUESTION: 188
□□ □ □□ □□ □□□ □□ □ □□□ □ □□ □□□ □□□□□?
A. □□ □□ □□ □□□ □□□□ □□□ □□□□□.
B. □□ □□□ □□ □□□ □□□□ □□□□□.

C. Inventory Invoice □□□ □□□□ □□□ □□ □□□ □□□□□.
D. □□ □□ □□□□ □□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
* Understanding Inventory Fraud Detection:
* Inventory fraud typically involves overstatement or understatement of inventory, fictitious inventory transactions, or misappropriation of stock.
* A key way to detect fraud is analyzing inventory adjustments (e.g., write-offs, missing stock, excess inventory) to identify unusual patterns or discrepancies.
* Why Stratifying Inventory Adjustments by Warehouse is the Best Approach:
* Identifies high-risk locations: Certain warehouses may show significantly higher inventory losses or adjustments, indicating possible fraud.
* Detects manipulation: Fraudsters may manipulate inventory records to cover theft or misstatements.
* Supports data-driven audit procedures: Stratification allows internal auditors to prioritize high-risk areas for deeper investigation.
* Why Other Options Are Incorrect:
* A. Analyze invoice payments just under individual authorization limits - Incorrect, as this technique detects fraudulent disbursements, not inventory fraud.
* C. Analyze inventory invoice amounts and compare with approved contract amounts - Incorrect, as this method detects pricing or procurement fraud, not inventory manipulation.
* D. Analyze differences discovered during duplicate payment testing - Incorrect, as this technique is used to detect billing fraud, not inventory fraud.
* IIA's Perspective on Fraud Detection and Internal Controls:
* IIA Standard 2120 - Risk Management requires internal auditors to assess fraud risk, including inventory manipulation.
* IIA GTAG (Global Technology Audit Guide) on Fraud Detection recommends data analytics for inventory monitoring.
* COSO Internal Control Framework highlights inventory control as a key component of financial accuracy and fraud prevention.
IIA References:
* IIA Standard 2120 - Risk Management & Fraud Detection
* IIA GTAG - Data Analytics for Fraud Detection in Inventory
* COSO Internal Control Framework - Inventory and Asset Management Controls Thus, the correct and verified answer is B. Analyze stratification of inventory adjustments by warehouse location.

NEW QUESTION: 189
□□ □ □□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □□ □□□□ □□□ □ □□ □□ □□ □□ □□□ □□□□ □□ □□□□□?
A. □□□□□□. □□□□ □□(FIFO).
B. □□ □□ □□(LIFO).

C. □□ □□ □□.
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
The FIFO (First-In, First-Out) method values inventory based on the assumption that older, lower-cost inventory is sold first, leaving newer, higher-cost inventory in stock. During periods of rising prices, FIFO results in lower cost of goods sold (COGS) and higher net income, making it susceptible to manipulation by management.
* (A) Correct - First-in, first-out method (FIFO).
* FIFO lowers COGS when older, cheaper inventory is sold first, inflating net income.
* Management can manipulate earnings by selectively selling older, lower-cost inventory.
* (B) Incorrect - Last-in, first-out method (LIFO).
* LIFO assumes newer, higher-cost inventory is sold first, resulting in higher COGS and lower net income.
* LIFO is typically used to reduce taxable income, not to inflate net income.
* (C) Incorrect - Specific identification method.
* This method tracks the exact cost of each unit, eliminating the ability to manipulate costs easily
.
* (D) Incorrect - Average-cost method.
* The average-cost method smooths out fluctuations in inventory costs, preventing significant income manipulation.
* IIA's Global Internal Audit Standards - Financial Reporting and Inventory Valuation Risks
* Discusses inventory accounting methods and their impact on financial statements.
* IFRS and GAAP Accounting Standards - Inventory Valuation
* Defines how FIFO can be used to influence financial performance.
* COSO's ERM Framework - Financial Manipulation Risks
* Identifies inventory valuation as an area where earnings management can occur.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

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

The immediate corrective action should be to restrict technicians' access to live production data to prevent accidental deletions from recurring. This addresses the condition directly and mitigates immediate risk exposure.
Option A (root cause project) is important but takes time and should follow immediate corrective action.
Option C (reconciliation) helps detect issues but does not prevent them. Option D (dismissal) is inappropriate since the issue was accidental, not fraudulent.
Reference:
IIA Standards - Standard 2130: Control.

NEW QUESTION: 191
□□ □ □□□□□□ □□□□□ □□□□ □□ □□ □□?
A. □□ □□.
B. □□ □□ □□
C. □□□ □□ □□
D. □□ □□ □□□
Answer: B (LEAVE A REPLY)
A centralized organizational structure concentrates decision-making authority at the top levels of management. While this ensures control and consistency, it can lead to slower decision-making due to the need for approvals from higher levels.
Let's analyze each option:
* Option A: Communication conflicts.
* Incorrect.
* Centralized structures generally have clear lines of authority and communication, reducing conflicts.
* Communication conflicts are more common in decentralized structures where multiple decision-makers exist.
* Option B: Slower decision making.
* Correct.
* Since all decisions must pass through top management, it delays responses to market changes and reduces flexibility.
* Lower-level employees have less authority to make operational decisions, leading to bottlenecks.
* IIA Reference: Internal auditors assess organizational governance, including decision-making efficiency in centralized vs. decentralized structures. (IIA Practice Guide: Organizational Governance)
* Option C: Loss of economies of scale.
* Incorrect.
* Centralization improves economies of scale by standardizing processes and consolidating resources.

* Decentralization (not centralization) is more likely to lead to duplication of efforts and a loss of economies of scale.
* Option D: Vulnerabilities in sharing knowledge.
* Incorrect.
* Centralized organizations tend to have structured knowledge-sharing frameworks, such as standardized policies and corporate training programs.

NEW QUESTION: 192
□□□□□ □□□ □□ □□□ □□□□□□□(CAE)□ □□□ □□ □□ □□□ □□□□ □□□ □□ □□□□□. CAE□ □□□ □ □□□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□ □□□□ □□□□□.
B. □□ □□□ □□□□ □□□□ □□ □ □□□ □□□ □□ □□□□□.
C. □□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□.
D. □□□□ □□□ □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The CAE should first discuss the risk and its implications with the responsible management. This provides management the opportunity to reassess, take corrective action, or explain their position. If the issue remains unresolved and the risk is still deemed excessive, then escalation to senior management or the board may follow.
Option A (designing response) is management's role. Option C (scheduling an audit) may be relevant later, but immediate discussion is the first step. Option D is premature without first engaging management.
Reference:
IIA Standards - Standard 2600: Communicating the Acceptance of Risks.

NEW QUESTION: 193
□□□ □□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□□. □□ □ □ □ □□ □□ □ □□□ □ □□ □□?
A. □□□ □□ □□□ □□□□ □□□□.
B. □□□ □□ □□□□□ □□□□□□.
C. □□□□ □□ □□□ □□ □□□□.
D. □□□ □□□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
A declining inventory turnover combined with an increasing gross margin rate suggests that the organization is not selling inventory as quickly as before, but still reporting higher profitability. This can indicate overstated inventory values, meaning that financial statements show higher inventory balances than what actually exists.
* (A) Incorrect - The organization's operating expenses are increasing.
* Operating expenses do not directly affect inventory turnover, which measures how quickly inventory is sold.

* Higher expenses could reduce net profit, but they would not explain a higher gross margin.
* (B) Incorrect - The organization has adopted just-in-time (JIT) inventory.
* JIT inventory systems increase inventory turnover by reducing excess stock.
* Since turnover is declining, this suggests the opposite of JIT.
* (C) Incorrect - The organization is experiencing inventory theft.
* Inventory theft usually reduces inventory levels, potentially increasing inventory turnover due to lower stock.
* Theft could lower gross margins if significant losses occur.
* (D) Correct - The organization's inventory is overstated.
* Overstated inventory leads to lower COGS, artificially inflating gross margin.
* If inventory levels are inflated, turnover appears lower because reported inventory is higher than actual sales justify.
* IIA's Global Internal Audit Standards - Financial Statement Audits and Fraud Risk
* Covers risks related to inventory misstatements and financial fraud.
* IFRS & GAAP Accounting Standards - Inventory Valuation
* Defines how inventory overstatement impacts financial ratios.
Analysis of Answer Choices:IIA References and Internal Auditing Standards:

NEW QUESTION: 194
□□ □□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□ □ □ □ □□□ □□ □□□□ □□□?
A. □□□□ □ □□ □□
B. □□□ □□□ □□
C. □□ □□□□ □□□ □□
D. □□ □□□ □□□ □□□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)
Before an external assessment of the internal audit activity, the CAE should agree with the board on the qualifications and independence of the external assessor or assessment team. This ensures credibility and compliance with the IIA's Quality Assurance and Improvement Program (QAIP) requirements.
Options A and B (specific audit areas or testing levels) are not matters for board approval in external assessments. Option D (specialized skills) is relevant but not as essential as overall qualifications and competence.
Reference:
IIA Standards - Standard 1312: External Assessments; Practice Advisory 1312-1.

NEW QUESTION: 195
□□ □□ □ □□ □□ □□□□ PIN, □□□□ □ □□ □□ □□□ □□□□ □□□□□ □□□□ □□ □□□□□?
/□□ □□□ □□□ □□ □□ □□□□ □□□□□ □□ □□ □□□ □□□ □ □□□□?

A. □□ □□.
B. □□□□□ □□□.
C. □□ □□□.
D. □□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Authentication ensures that only authorized users can access a system by requiring credentials such as PINs, passwords, or biometrics.
Option A (Remote wipe) - Deletes data but does not control initial access.
Option B (Software encryption) - Protects stored data, not user access.
Option C (Device encryption) - Secures the device, but authentication controls access.
Since authentication ensures secure user verification, Option D is correct.
Reference: IIA IT Security - Access Control Mechanisms

NEW QUESTION: 196
□□ □ □□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□□?
A. □□ □□ □□ □□.
B. □□□□ □□□□□.
C. □□□ □□.
D. □□ □□.
Answer: (SHOW ANSWER)
Under International Financial Reporting Standards (IFRS 10 - Consolidated Financial Statements), an entity is required to consolidate its financial statements based on the control principle rather than ownership percentage alone.
* Why Option B (Control ownership) is Correct:
* According to IFRS 10, consolidation is required when an entity has control over another entity.
* Control is defined as having power over the investee, exposure to variable returns, and the ability to influence those returns.
* Even if an entity owns less than 50% of voting rights, it may still have control through contractual arrangements, rights over key decisions, or majority board influence.
* Why Other Options Are Incorrect:
* Option A (Variable entity approach):
* This is a concept used in U.S. GAAP (ASC 810 - Variable Interest Entities) rather than IFRS. IFRS focuses on the broader control model.
* Option C (Risk and reward):
* IFRS previously considered risk and reward under IAS 27/SIC-12, but IFRS 10 replaced this with the control model.
* Option D (Voting interest):
* Voting rights alone do not determine consolidation under IFRS. Control can exist even without majority voting rights through contractual arrangements or potential voting rights.

* IFRS 10 - Consolidated Financial Statements: Defines the principle of control for consolidation.
* IIA GTAG - "Auditing Financial Reporting Risks": Discusses the impact of IFRS consolidation principles.
* COSO ERM Framework: Emphasizes risk assessment in financial reporting, including consolidation decisions.
IIA References:Thus, the correct answer is B. Control ownership.

NEW QUESTION: 197
□□ □□ □□□ □□ □□, □□□, □□□□□□ □□□□ □ □□□ □□□ □□□□ □ □ □□□ □ □ □□ □□□ □□□□□?
A. □□□ □□□□ □□, □□□□ □ □□ □□□ □□□□□.
B. □□ □□□ □□□□ □ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□ □□, □□□□ □□□□ □ □□ □□ □□
D. □□□, □□ □□□ □ □□ □□□□ □□ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first step in defining the internal audit function's structure and processes is to understand the needs and expectations of the board, senior management, and external stakeholders. This ensures alignment with organizational priorities and risk appetite. Option A (recommend improvements) is a later activity. Option B (hiring plan) comes after the structure and resourcing needs are identified. Option C (quality assessments) occurs after processes are established.
Reference:
IIA Standards - Standard 1000: Purpose, Authority, and Responsibility.

NEW QUESTION: 198
□□ □ □□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□□?
A. □□ □□□□□ □□ □□□□□ □□ □□□□ □□□ □□□□ □□□□ □□□□□ □□.
B. □□□ IT □□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□ □□ □□□□ □□ □□ □□□□ □□□□ □□ □□ □□□□ □□□□□□.

C. □□ □□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□□ □□□□ □□□ □ □□□□ □□ □□□□□ □□□□□□.
D. □□ □□□□ □□□□ □□ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□ □ □ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
A spear phishing attack is a targeted email attack aimed at a specific individual, organization, or business.
Unlike general phishing, which casts a wide net, spear phishing is highly personalized and designed to deceive the recipient into providing sensitive information.
* Personalization - The email references a golf membership renewal, making it relevant and believable to the recipient.
* Social Engineering - The attacker exploits the victim's trust by pretending to be a legitimate entity.
* Malicious Link - The victim clicks a fraudulent hyperlink and enters sensitive credit card details.
* Financial Fraud - The goal is to steal payment information, leading to unauthorized transactions.
* A. Numerous and consistent attacks on the company's website caused the server to crash.
* This describes a Denial-of-Service (DoS) attack, not spear phishing.
* B. A person posing as an IT help desk representative called employees and played a generic message requesting passwords.
* This describes vishing (voice phishing) rather than spear phishing.
* D. Many users of a social network service received fake notifications about a new investment opportunity.
* This is general phishing, as it targets multiple users instead of one individual.
* IIA's GTAG (Global Technology Audit Guide) on Cybersecurity - Emphasizes the risk of spear phishing in cyber fraud.
* NIST SP 800-61 (Computer Security Incident Handling Guide) - Defines spear phishing as a highly targeted attack method.
* COBIT 2019 (Governance and Management of IT) - Highlights social engineering risks in IT security.
Why Option C is Correct?Why Not the Other Options?IIA References:# Final Answer: C. A person received a personalized email regarding a golf membership renewal, and he clicked a hyperlink to enter his credit card data into a fake website.

NEW QUESTION: 199
□□□□ □□□□ □□□□ □□□ □□ □□□ □□□□□□. □□□ □□ □□□ □□□ □□ □□□□ □□ □□□ □□□□□.
□□ □ □□□□ □□□ □□□□□□□ □ □□□ □□□ □□ □□□□ □□ □□ □□□ □□□□□?

A. ☐
B. ☐☐☐☐
C. ☐☐☐
D. ☐
Answer: (SHOW ANSWER)
* Understanding the BCG Matrix and Investment Classifications:
* The Boston Consulting Group (BCG) Matrix classifies business investments into four categories:
* Stars: High growth, high market share.
* Cash Cows: Low growth, high market share.
* Question Marks: High growth, low market share.
* Dogs: Low growth, low market share.
* Why the Investment is a Cash Cow:
* The organization operates in a mature, slow-growth industry but has a dominant market position and generates consistent positive financial income.
* This aligns with the definition of a Cash Cow, as it represents a stable and profitable business with low reinvestment needs.
* Investors typically use Cash Cows to fund other investments, as they generate steady cash flow with minimal risk.
* Why Other Options Are Incorrect:
* A. A star:
* A Star requires high growth and high market share, but the organization operates in a slow-growth industry, disqualifying it from this category.
* C. A question mark:
* A Question Mark is in a high-growth industry but lacks market dominance. Since this company is already dominant, it does not fit this category.
* D. A dog:
* A Dog has low growth and low market share, meaning it does not generate strong financial returns. The company described produces positive income, ruling out this category.
* IIA's Perspective on Business Strategy and Portfolio Management:
* IIA Standard 2120 - Risk Management states that internal auditors must assess the strategic positioning of business investments.
* COSO ERM Framework supports the use of strategic models like the BCG Matrix to evaluate investment performance and risk exposure.
IIA References:
* IIA Standard 2120 - Risk Management and Strategic Planning
* COSO Enterprise Risk Management (ERM) Framework
* Boston Consulting Group (BCG) Matrix in Investment Analysis
Thus, the correct and verified answer is B. A cash cow.

NEW QUESTION: 200
□□ IT □□ □□ □□ □ □□□ □ □□□ □□ □□ □□□□ □□□ □ □□ □□□ □□ □□□□□ □□□ □□ □□□□ □□□□□ □□□ □□□ □□□ □□ □□ □□□□□?
A. □□□□ □□□
B. □□ □□□
C. □□□□
D. □□□□
Answer: B (LEAVE A REPLY)
A Cold Site is a remote disaster recovery facility that provides physical space and basic utilities such as electricity, internet, and telecommunications but does not include pre-installed servers, networking equipment, or other IT infrastructure. It requires a longer recovery time since the organization must procure, install, and configure necessary hardware and software before resuming operations.
* A. Frozen Site - This is not a recognized term in IT disaster recovery planning.
* C. Warm Site - A warm site has some pre-installed hardware and infrastructure but requires additional setup before full operation.
* D. Hot Site - A hot site is a fully functional duplicate of the original site, with real-time data replication, allowing for immediate recovery.
* The IIA Global Technology Audit Guide (GTAG) 10: Business Continuity Management emphasizes that organizations should classify recovery sites based on risk tolerance and recovery time objectives (RTO).
* The IIA's International Professional Practices Framework (IPPF) - Practice Advisory 2110-2 discusses IT continuity and disaster recovery as a critical element of internal audit assessments.
* NIST Special Publication 800-34 (Contingency Planning Guide for Information Technology Systems) defines and categorizes disaster recovery sites, aligning with the cold site definition.
Explanation of the Other Options:IIA References & Best Practices:Thus, the correct answer is B. Cold Site.

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

NEW QUESTION: 202
□□ □□□□ □□ □□ □□□□□ □□ □□□□□ □□□□ □□ □□□ □□ □□□ □ □□□□□. □□ □□: □□□ $2□ 1,000□; □□: □□□ $3□ 5,000□; □□: □□□ $7□

3,000□. □□□□□ $8,500□□ □□□□□□□. □ □□ □□□□ □ □□ □□ □□ □ □ □ □□ □□□□□□?

A. □□□□□

B. □□□□(FIFO) □□

C. □□ □□ □□

D. □□□□□□□□□

Answer: B (LEAVE A REPLY)

Reference: IIA Business Knowledge for Internal Auditing, Inventory Valuation section.

NEW QUESTION: 203

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

A. □□□□ □

B. □□□ □□□.

C. □□□□

D. □□□

Answer: C (LEAVE A REPLY)

An Intranet is a private network that is accessible only to an organization's personnel. It is used for internal communication, data sharing, and collaboration while ensuring security and restricted access.

Let's analyze each option:

* Option A: An extranet

* Incorrect. An extranet extends an organization's internal network to external parties such as vendors, suppliers, or business partners. Since the organization wants to allow access only to its personnel, an extranet is not the right choice.

* Option B: A local area network (LAN)

* Incorrect. While a LAN is a network within a limited geographic area (such as an office), it does not necessarily restrict access only to personnel. Additionally, an intranet operates over a LAN but includes access controls and authentication mechanisms.

* Option C: An Intranet

* Correct. An intranet is specifically designed for internal use, allowing employees to securely share documents, collaborate, and access internal resources. Organizations can implement access control mechanisms to restrict access to authorized personnel only.

* IIA Reference: Internal auditors assess IT security to ensure that internal networks (such as intranets) have appropriate access restrictions to protect sensitive data. (IIA GTAG: Auditing IT Networks)

* Option D: The internet

* Incorrect. The internet is a public network that does not restrict access. Using the internet for internal communication would expose sensitive data to external threats.

Thus, the verified answer is C. An Intranet.

NEW QUESTION: 204
□□ □□□ □□□□□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□ □□ □□. □□□ □□ □□□ □□ □□□ □□ □ □□ □□□ □□ □□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□.
B. □□□ □□□□ □□ □□□ □□ □□□□□ □□□□ □□□ □□□.
C. □□□□ □□□□ □□□□ □□ □□□□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□ □□□ □□.
Answer: B (LEAVE A REPLY)
Phishing attacks often target financial institutions by impersonating customers and requesting fraudulent fund transfers. The best way to verify such requests is to independently contact the customer using a trusted communication channel, such as the phone number on record.
* Verbal confirmation via a trusted number prevents fraudsters from exploiting email spoofing or compromised accounts.
* This aligns with industry best practices, including multi-factor verification for high-risk transactions.
* A. Reviewing the customer's wire activity to determine whether the request is typical. (Incorrect)
* While reviewing transaction history can help detect anomalies, fraudsters can mimic previous transaction patterns, making this method unreliable on its own.
* B. Calling the customer at the phone number on record to validate the request. (Correct)
* Direct phone verification ensures that the actual account owner is making the request.
* This is a widely recommended anti-fraud measure in financial institutions.
* C. Replying to the customer via email to validate the sender and request. (Incorrect)
* If the email account is compromised, the fraudster will control the response.
* Email validation is not secure for financial transactions.
* D. Reviewing the customer record to verify whether the customer has authorized wire requests from that email address. (Incorrect)
* While this can help identify unregistered emails, attackers often spoof or hack real customer emails.
* Email-based verification alone is not sufficient.
* IIA GTAG 16 - Security Risk: IT and Cybersecurity recommends multi-factor authentication for high-risk financial transactions.
* IIA Standard 2120 - Risk Management highlights the need for robust fraud prevention mechanisms, including direct customer verification.
* FFIEC (Federal Financial Institutions Examination Council) Cybersecurity Guidelines emphasize the importance of out-of-band authentication for wire transfers.
Explanation of Answer Choices:IIA References:Thus, the correct answer is B. Calling the customer at the phone number on record to validate the request.

NEW QUESTION: 205
□□ □ □□□□□ □□□ □ □ □□ □□ □□□□□?
A. □□□□ □□ □□□□ □□□□□□.
B. □□ □□□ □□□ □□.
C. □□ □□□ □□ □□□ □□
D. □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
* Understanding Outsourcing and Its Impact:
* Outsourcing refers to contracting external vendors to handle business functions that were previously managed in-house.
* While it can reduce costs and improve efficiency, it increases reliance on external suppliers for critical services.
* Why Increased Dependence on Suppliers is the Most Likely Result:
* Loss of Internal Control: Companies lose direct oversight over quality, delivery times, and operational processes, depending on the supplier's performance.
* Risk of Supplier Disruptions: If the supplier faces financial difficulties, operational failures, or compliance issues, the outsourcing company is directly affected.
* Vendor Lock-in: Over time, switching suppliers becomes difficult due to integration costs and proprietary dependencies.
* Why Other Options Are Incorrect:
* B. Increased importance of market strategy - Incorrect.
* While outsourcing can free up resources to focus on core business strategy, it does not necessarily increase the importance of market strategy.
* C. Decreased sensitivity to government regulation - Incorrect.
* Outsourcing often increases regulatory risks, as companies must ensure third-party compliance with data protection, labor laws, and industry regulations.
* D. Decreased focus on costs - Incorrect.
* Outsourcing is typically done to reduce costs, not decrease cost focus. Organizations still monitor costs closely to ensure vendor contracts remain cost-effective.
* IIA's Perspective on Outsourcing and Risk Management:
* IIA Standard 2120 - Risk Management requires internal auditors to evaluate risks associated with outsourcing.
* IIA GTAG (Global Technology Audit Guide) on Third-Party Risk Management highlights risks related to supplier dependence, service quality, and compliance.
* COSO ERM Framework recommends ongoing supplier performance monitoring to mitigate risks of over-dependence.
IIA References:
* IIA Standard 2120 - Risk Management & Vendor Oversight
* IIA GTAG - Third-Party Risk Management
* COSO ERM - Managing Outsourcing Risks
Thus, the correct and verified answer is A. Increased dependence on suppliers.

NEW QUESTION: 206
□□ □ □□ □□□ □□ □ □□□ □□?
A. □□□ □□□ □□□ □□□□ □□□.
B. □□ □□□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□ □□□□.
D. □□□ □ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The matching principle is a fundamental accounting concept that ensures that expenses are recorded in the same period as the revenues they help generate.
* Why Option C (Expense recognition is tied to revenue recognition) is Correct:
* The matching principle states that expenses should be recognized in the same period as the revenue they help generate to ensure accurate financial reporting.
* This principle is applied in accrual accounting under GAAP and IFRS, ensuring that expenses and revenues are properly aligned.
* Why Other Options Are Incorrect:
* Option A (Revenues should be recognized when earned):
* This describes the revenue recognition principle, not the matching principle.
* Option B (Revenue recognition is matched with cash):
* Incorrect because the matching principle applies to accrual accounting, not cash accounting. Revenue can be recognized before cash is received.
* Option D (Expenses are recognized at each accounting period):
* Incorrect because expenses are not necessarily recognized in every period; they are matched to revenue.
* IIA Practice Guide - "Auditing Financial Reporting Controls": Discusses the importance of the matching principle.
* GAAP & IFRS Accounting Standards: Define and require the application of the matching principle.
* COSO Internal Control Framework: Emphasizes revenue-expense alignment for accurate financial reporting.
IIA References:

NEW QUESTION: 207
□□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □ □□ □□□ □□□□□□. □□□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□□. □□ □□ □□□ □□ □□□□ □□ □□□□□ □□□□□□. □□ □□□□ □□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□□□ □□□□□□ □. □□ □□ □□□ □□ □□□□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□□ □□□ □□□ □□□□□ □□ □□ □□□ □□ □□□□ □□ □□ □ □□□□□□.
B. □□ □□ □□□ □□ □□ □□□ □□ □□□□ □□□□□□.

C. □□ □□□□□ □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□.
D. □□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □□□ □□ □□□ □□□ □ □□□ □□□.

Answer: B (LEAVE A REPLY)

Action plans should be agreed upon collaboratively, with both the responsible managers and senior management involved. Involving senior management earlier in the draft report and action plan stage ensures alignment on deadlines and accountability before final issuance.

Option A would reduce input and transparency. Option C creates fragmented reporting. Option D is excessive and bypasses proper reporting procedures.

Reference:

IIA Standards - Standard 2410: Criteria for Communicating; Standard 2440: Disseminating Results.