ISACA.CISA-CN.v2026-05-19.q615

Exam Code:	CISA-CN
Exam Name:	Certified Information Systems Auditor (CISA中文版)
Certification Provider:	ISACA
Free Question Number:	615
Version:	v2026-05-19
# of views:	480
# of Questions views:	6150
https://www.freepdfdumps.com/ISACA.CISA-CN.v2026-05-19.q615.html	

NEW QUESTION: 1
下列何者是防止應付帳款員工進行詐欺性電子資金轉帳的最佳建議？
A. 定期供應商審核
B. 雙重控制
C. 獨立和解
D. 重新輸入金額
E. 聘請外部安全事件回應專家處理事件。
Answer: B (LEAVE A REPLY)
The best recommendation to prevent fraudulent electronic funds transfers by accounts payable employees is dual control. Dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity. Dual control can prevent fraudulent electronic funds transfers by requiring independent verification and approval of payment requests, amounts, and recipients by different accounts payable employees. The other options are not as effective as dual control in preventing fraudulent electronic funds transfers, as they do not involve independent checks or approvals. Periodic vendor reviews are detective controls that can help identify any irregularities or anomalies in vendor payments, but they do not prevent fraudulent electronic funds transfers from occurring. Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent fraudulent electronic funds transfers from occurring. Re-keying of monetary amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent fraudulentelectronic funds transfers from occurring. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 2
某組織在未對網路或安全基礎設施進行任何其他變更的情況下，對其伺服器環境進行了虛擬化。下列哪一項風險最大？

A. 網路入侵偵測系統 (IDS) 無法監控虛擬伺服器之間的通訊
B. 虛擬化平台存在漏洞，影響多台主機
C. 資料中心環境控制與新配置不一致
D. 系統文件未更新以反映環境變化
Answer: A (LEAVE A REPLY)
The most significant risk in virtualizing the server environment without making any other changes to the network or security infrastructure is the inability of the network intrusion detection system (IDS) to monitor virtual server-to-server communications. This can create blind spots for the IDS and allow malicious traffic to bypass detection. A vulnerability in the virtualization platform affecting multiple hosts is a potential risk, but not necessarily more significant than the loss of visibility. Data center environmental controls not aligning with new configuration or system documentation not being updated to reflect changes in the environment are operational issues, not security issues. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
373

NEW QUESTION: 3
資訊系統審計員正在評估一個基於網路的客口服務應用程式開發專案的進度。
下列哪一項對本次評估最有幫助？
A. 積壓消耗報告
B. 關鍵路徑分析報告
C. 開發人員狀態報告
D. 變更管理日誌
Answer: A (LEAVE A REPLY)
A backlog consumption report is a report that shows the amount of work that has been completed and the amount of work that remains to be done in a project. It is a useful tool for measuring the progress and performance of a web-based customer service application development project, as it can indicate whether the project is on track, ahead or behind schedule, and how much effort is required to finish the project. A backlog consumption report can also help identify any issues or risks that may affect the project delivery. Critical path analysis reports, developer status reports and change management logs are also helpful for evaluating a project, but they are not as helpful as a backlog consumption report, as they do not provide a clear picture of the overall project status and completion rate. References:
[Backlog Consumption Report Definition]
Backlog Consumption Report | ISACA

NEW QUESTION: 4
下列哪一種風險場景最適合透過實施與全盤加密相關的策略和程序來解決？
A. 員工離職跳槽到競爭對手公司導致的資料外洩
B. 與儲存受監管資訊相關的違規罰款

C. 未經授權透過應用程式介面對資訊進行邏輯存取
D. 儲存資訊的媒體被物理盜竊
Answer: D (LEAVE A REPLY)
Full disk encryption (FDE) is a means of protecting information by encrypting all of thedata on a disk, including temporary files, programs, and system files1. FDE is best suited for addressing the risk scenario of physical theft of media on which information is stored, as it prevents unauthorized access to the data even if the device is lost or stolen2. FDE does not prevent data leakage as a result of employees leaving to work for competitors, as they may still have access to the data while using the device or copy the data to another device before leaving. FDE does not prevent noncompliance fines related to storage of regulated information, as it does not ensure that the data is stored in accordance with the applicable laws and regulations. FDE does not prevent unauthorized logical access to information through an application interface, as it does not control the access rights and permissions of users and applications. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section
2402 Planning, "The IS audit and assurance professional should identify and assess risk relevant to the area under review." 3 Oneof the risk factors to consider is "the sensitivity of information processed, stored or transmitted by the system" 3. FDE is one of the possible controls to mitigate the risk of unauthorized disclosure of sensitive information due to physical theft of media.

NEW QUESTION: 5
對於評估組織漏洞掃描程序有效性的資訊系統稽核員而言，下列哪一項應該是最口得關注的？
A. 為解決已發現的漏洞而採取的措施沒有正式記錄。
B. 結果不會報告給有權確保解決問題的人員。
C. 掃描頻率低於組織漏洞掃描計畫的要求。
D. 結果未經高階主管批准。
Answer: B (LEAVE A REPLY)
The finding that should be of greatest concern to an IS auditor assessing the effectiveness of an organization' s vulnerability scanning program is that results are not reported to individuals with authority to ensure resolution. This indicates a lack of accountability and communication for vulnerability management, which may result in unresolved or delayed remediation of identified vulnerabilities. This may expose the organization to increased risk of cyberattacks or breaches. The other findings are also concerning, but not as much as this one, because they may affect the completeness, accuracy or timeliness of the vulnerability scanning process, but not necessarily its effectiveness. References:
ISACA, CISA Review Manual, 27th Edition, chapter 4, section 4.41
ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.2

NEW QUESTION: 6
下列哪一項是軟體開發人員使用自動化測試而不是手動測試的最佳理由？
A. CAAT 易於開發
B. 改進的迴歸測試
C. 縮小驗收測試的範圍
D. 維護自動化測試口本的便利性
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
某組織計劃進行收購，並聘請了一位資訊系統審計師來評估目標公司的IT治理架構。下列哪一項最有助於確定該框架的有效性？
A. IT能力與成熟度銷售評估報告。
B. 與競爭對手的 IT 效能基準測試報告
C. 近期第三方資訊系統審計報告
D. 目前和先前的口部資訊系統審計報告
Answer: (SHOW ANSWER)
Recent third-party IS audit reports would be most helpful in determining the effectiveness of the IT governance framework of the target company. IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. A third-party IS audit is an independent and objective examination of an organization's IT governance framework by an external auditor.
Recent third-party IS audit reports can provide reliable and unbiased evidence of the strengths, weaknesses, and maturity of the IT governance framework of the target company. The other options are not as helpful as recent third-party IS audit reports, as they may not be as comprehensive, accurate, or current as external audits. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION: 8
資訊系統審計員在審口安全事件處理流程時發現，事件雖然已解決並關閉，但並未調口根本原因。在這種情況下，下列哪一項應該是最主要的關注點？
A. 尚未報告員工濫用權力的情況。
B. 經驗教訓尚未妥善記錄
C. 漏洞尚未妥善解決。
D. 安全事件策略已過時。
Answer: (SHOW ANSWER)
The major concern with the situation where security incidents are resolved and closed, but root causes are not investigated, is that vulnerabilities have not been properly addressed. Vulnerabilities are weaknesses or gaps in the security posture of an organization that can be exploited by threat actors to compromise its systems, data, or operations. If root causes are not investigated, vulnerabilities may remain undetected or unresolved, allowing

attackers to exploit them again or use them asentry points for further attacks. This can result in repeated or escalated security incidents that can cause more damage or disruption to the organization.
The other options are not as major as the concern about vulnerabilities, but rather secondary or related issues that may arise from the lack of root cause analysis. Abuses by employees have not been reported is a concern that may indicate a lack of awareness, accountability, or monitoring of insider threats. Lessons learned have not been properly documented is a concern that may indicate a lack of improvement, learning, or feedback from security incidents. Security incident policies are out of date is a concern that may indicate a lack of alignment, review, or update of security incident processes.
References:
ISACA CISA Review Manual 27th Edition (2019), page 254
Why Root Cause Analysis is Crucial to Incident Response (IR) - Avertium3 Root Cause Analysis Steps and How it Helps Incident Response ...

NEW QUESTION: 9
在新應用程式的發布管理過程中，下列哪一項會帶來最大的風險？
A. 流程未更新以與口品發布計劃保持一致。
B. 程式碼未經授權部署到生口環境。
C. 新加入的程式可能會覆蓋現有的生口文件。
D. 已發現的錯誤尚未解決。
Answer: B (LEAVE A REPLY)
Unauthorized code deployment presents acritical security and operational risk.
Option A (Incorrect):Whiledocumentation issuescan cause confusion, they do not directlyjeopardizesecurity or system stability.
Option B (Correct):Deploying code without authorizationbypasseschange management controls, potentially leading to security vulnerabilities, system failures, or compliance violations. This is thegreatest risk.
Option C (Incorrect):Overwriting files can cause issues but isless severethan unauthorized deployment, which may introducemalware or untested features.
Option D (Incorrect):An unresolved bug may causeperformance issues, butunauthorized deploymentposes a higher security and compliance risk.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers change management, release processes, and risk assessment.

NEW QUESTION: 10
下列哪一項措施能最有效降低暴力攻擊成功的機率？
A. 設定帳口活動逾時
B. 要求密碼長度至少 100%。

C. 提高密碼變更頻率
D. 建立帳口鎖定政策
Answer: (SHOW ANSWER)

NEW QUESTION: 11
下列哪一項措施最能有效地幫助減少組織中被撤銷事件的數量？
A. 在各種場景下測試事件回應計劃
B. 在影響評估後確定事件的優先順序。
C. 將事件與問題管理活動連結起來
D. 針對當前事件趨勢對事件管理團隊進行培訓
Answer: C (LEAVE A REPLY)
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but they do not directly address the issue of repeated incidents.
References: ISACA ITAF 3rd Edition Section 3600

NEW QUESTION: 12
下列哪一項是網路彈性的主要目標？
A. 在對營運影響有限的情況下，有效率且有效地從事件中恢復
B. 服務中斷後恢復正常運營
C. 為了限制安全漏洞的嚴重程度並維持持續營運
D. 防止潛在的攻擊或營運中斷
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
資訊系統審計員從差旅和費用系統中提取數據，以確定員工是否將公司車輛用於私人用途。這是在執行哪種類型的審計？
A. 詐欺審計
B. 財務審計
C. 功能審計
D. 合規性審計
Answer: (SHOW ANSWER)
The best answer is D. Compliance audit.
The auditor is testing whether employee behavior complies with organizational rules or policy regarding the use of the organization's car. ISACA defines IT compliance as adherence to mandated requirements from laws, regulations, contractual obligations, and internal policies. Since the scenario is about checking whether employees are following the organization's rule on permitted use, the audit is primarily a compliance-oriented review.

Option A could be tempting because misuse of a company car might be abusive, but the question does not say the auditor is investigating intentional deception or a suspected fraud scheme. Option B is incorrect because this is not primarily about fair presentation of financial statements. Option C is not the best fit because the audit objective is not evaluation of business function performance, but adherence to policy.
Therefore, the correct answer is D, because the auditor is determining whether employees are complying with the organization's established usage rules.
References (Official ISACA):
* ISACA, IT Compliance - compliance includes adherence to internal policies.
* ISACA, An Integrated Approach to Security Audits - audits assess adherence to required controls and obligations.

NEW QUESTION: 14
下列哪一項對資料處理設施中安裝的煙霧偵測器的有效性最為重要？
A. 偵測器與濕式管線滅火系統相連。
B. 探測器口動時會發出聲音警報。
C. 探測器具有正確的行業認證。
D. 偵測器與乾式管線滅火系統相連。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
在決定與審計結果相關的後續活動的適當時間框架時，下列哪一項是最重要的決定因素？
A. 資訊系統審計資源的可用性
B. 管理階層回應中包含的整改日期
C. 業務高峰期
D. 審計中發現的業務流程複雜性
Answer: (SHOW ANSWER)
The most important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings is the remediation dates included in management responses. The IS auditor should ensure that the follow-up activities are aligned with the agreed-upon action plans and deadlines that management has committed to in response to the audit findings. The follow-up activities should verify that management has implemented the corrective actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are less important factors for establishing timeframes for follow-up activities:
Availability of IS audit resources. This is a practical factor that may affect the scheduling and execution of follow-up activities, but it should not override the priority and urgency of verifying management's corrective actions.

Peak activity periods for the business. This is a factor that may affect the availability and cooperation of auditees during follow-up activities, but it should not delay or postpone the verification of management's corrective actions beyond reasonable limits.
Complexity of business processes identified in the audit. This is a factor that may affect the scope and depth of follow-up activities, but it should not affect the timeframe for verifying management's corrective actions.

NEW QUESTION: 16
在對組織的資訊安全策略進行正式審口時，發現下列哪個問題對組織構成最大潛在風險？
A. 這些政策與資訊安全風險承受能力
不符。
B. 這些政策未經風險管理委員會審口。
C. 這些政策並非基於資訊安全領域的口業最佳實踐。
D. 關鍵風險利害關係人無法取得這些政策。
Answer: (SHOW ANSWER)

NEW QUESTION: 17
在對資料中心環境控制進行審口時，檢口滅火系統時應考慮下列哪些因素？
A. 安裝手冊
B. 現場更換服務
C. 保險範圍
D. 維護程序
Answer: D (LEAVE A REPLY)
The correct answer is D. Maintenance procedures should be considered when examining fire suppression systems as part of a data center environmental controls review. Fire suppression systems are critical for protecting the data center equipment and personnel from fire hazards. Therefore, they should be regularly maintained and tested to ensure their proper functioning and compliance with safety standards. Maintenance procedures should include inspection, cleaning, replacement, and repair of the fire suppression system components, as well as documentation of the maintenance activities and results. Installation manuals, onsite replacement availability, and insurance coverage are notdirectly related to the fire suppression system performance and effectiveness, and

therefore are not relevant for the audit review. References: CISA Review Manual (Digital Version)1, page 403.

NEW QUESTION: 18
在審□使用外包商處置儲存媒體的情況時，資訊系統稽核員最需要核實下列哪一項□容？
A. 供應商的流程在處置前會對介質進行適當的消毒。
B. 合約包括供應商發出銷毀證明。
C. 該供應商過去沒有發生過安全事件。
D. 處置運輸車輛完全安全
Answer: A (LEAVE A REPLY)
The most important thing for an IS auditor to verify when reviewing the use of an outsourcer for disposal of storage media is that the vendor's process appropriately sanitizes the media before disposal. As explained in the previous question, storage media may contain sensitive or confidential information that needs to be protected from unauthorized access, disclosure, or misuse. The IS auditor should verify that the vendor has a process that appropriately sanitizes the media before disposal, such as wiping, degaussing, shredding, or incinerating, and that the process is effective and compliant with the organization's policies and standards. The other options are not as important as verifying the vendor's process, because they either do not ensure the security and privacy of the information on the media, or they aresecondary to the vendor's process.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

NEW QUESTION: 19
下列哪一種方法是維護程式原始碼更改稽核追蹤的最佳方法？
A. 將詳細資訊嵌入原始程式碼中。
B. 規範文件命名約定。
C. 採用自動化版本控制。
D. 記錄變更登記冊上的詳細資料。
Answer: C (LEAVE A REPLY)
Automated version control systems are the best method to maintain an audit trail of changes made to the source code of a program. They automatically track and manage changes to the source code over time, allowing you to see what changes were made, when they were made, and who made them1. This provides a clear and detailed audit trail that can be invaluable for debugging, understanding the evolution of the code, and ensuring accountability23.

NEW QUESTION: 20
對於審□具有兩個互聯網連接的組織網路彈性的資訊系統審計員來□，下列哪一項最令人關注？
A. 非關鍵應用程式也連接到這兩個連接。

B. 尚未進行網路容量測試。
C. 業務連續性計劃(BCP)在過去六個月口未進行過測試。
D. 兩個連線均來自同一提供者。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
為了降低透過應用程式介面(API)口詢外洩資料的風險，下列哪項設計考量最為重要？
A. 資料保留
B. 資料最小化
C. 數據質量
D. 資料完整性
Answer: B (LEAVE A REPLY)
The answer B is correct because data minimization is the most important design consideration to mitigate the risk of exposing data through application programming interface (API) queries. An API is a set of rules and protocols that allows different software components or systems to communicate and exchange data. API queries are requests sent by users or applications to an API to retrieve or manipulate data. For example, a user may query an API to get information about a product, a service, or a location.
Data minimization is the principle of collecting, processing, and storing only the minimum amount of data that are necessary for a specific purpose. Data minimization can help to reduce the risk of exposing data through API queries by limiting the amount and type of data that are available or accessible through the API.
Data minimization can also help to protect the privacy and security of the data subjects and the data providers, as well as to comply with the relevant laws and regulations.
Some of the benefits of data minimization for API design are:
Privacy: Data minimization can enhance the privacy of the data subjects by ensuring that only the data that are relevant and essential for the API purpose are collected and processed. This can prevent unnecessary or excessive collection or disclosure of personal or sensitive data, such as names, addresses, phone numbers, email addresses, etc. Data minimization can also help to comply with the privacy laws and regulations that require data protection by design and by default, such as GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act).
Security: Data minimization can improve the security of the data providers by reducing the attack surface and the potential damage of a data breach. If less data are stored or transmitted through the API, there are fewer opportunities for attackers to access or compromise the data. Data minimization can also help to implement security controls such as encryption, access control, or logging more efficiently and effectively.
Performance: Data minimization can increase the performance of the API by optimizing the use of resources and bandwidth. If less data are stored or transmitted through the API, there are less storage space and network traffic required. Data minimization can also help to improve the speed and reliability of the API responses.

Some of the techniques for data minimization in API design are:
Define clear and specific purposes for the API and document them in the API specification or documentation.
Identify and classify the data that are needed for each purpose and assign them appropriate labels or levels, such as public, internal, confidential, or restricted.
Implement filters or parameters in the API queries that allow users or applications to specify or limit the data fields or attributes they want to retrieve or manipulate.
Use pagination or throttling in the API responses that limit the number or size of data items returned per request.
Use anonymization or pseudonymization techniques that remove or replace any identifying information from the data before sending them through the API.
Some examples of web resources that discuss data minimization in API design are:
Data Minimization in Web APIs - World Wide Web Consortium (W3C)
Adding Privacy by Design in Secure Application Development
Chung-ju/Data-Minimization: A repository of related papers. - GitHub

NEW QUESTION: 22
在評估事件回應計畫的有效性時，資訊系統稽核員注意到，大量報告的事件都涉及員工發現的可移動儲存媒體中的惡意軟體。下列哪一項是向管理階層提出的最恰當的建議？
A. 安裝額外的防毒程式以增強保護。
B. 確保防毒程式包含公司所有裝置的最新病毒庫簽署檔案。
C. 限制對公司設備上可移動媒體連接埠的存取。
D. 實施全組織範圍口的可移動介質策略。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
下列哪一項是最大限度降低抽樣風險的最佳方法？
A. 使用較大的樣本量
B. 執行統計抽樣
C. 執行判斷抽樣
D. 加強審計測試程序
Answer: B (LEAVE A REPLY)
Sampling risk is the risk that the auditor's conclusion based on a sample may be different from the conclusion that would be reached if the entire population was tested using the same audit procedure. Sampling risk can lead to either incorrect rejection or incorrect acceptance of the audit objective. The best way to minimize sampling risk is to perform statistical sampling. Statistical sampling is a method of selecting and evaluating a sample using probability theory and mathematical calculations. Statistical sampling allows auditors to measure and control the sampling risk by determining the appropriate sample size and selection method, and evaluating the results using confidence levels and precision

intervals. Statistical sampling can also provide more objective and consistent results than judgmental sampling, which relies on the auditor's professional judgment and experience.
References:
6: Sampling Risks: Definition, Example, and Explanation - Wikiaccounting
7: Sampling Risk in Audit | Sampling vs non sampling risk - Accountinguide
9: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 24
下列哪一種方法能提供最可靠的審計證據？
A. 口詢
B. 管理階層證明
C. 重新執行控制
D. 觀察
Answer: C (LEAVE A REPLY)
The best answer is C. Re-performance of controls.
Under ISACA audit principles, evidence obtained directly by the auditor is generally more reliable than evidence provided by management or gathered indirectly. Re-performance allows the auditor to independently execute the control or procedure and verify whether it works as intended, making it stronger than inquiry, observation, or management attestation.
Option A is the least reliable because inquiry depends on what people say. Option B is stronger than simple inquiry but still relies on management representation. Option D can be useful, but observation only shows what happened at a point in time and may not prove consistent operation. Re-performance gives the auditor the highest level of assurance because the evidence is generated through the auditor's own independent work.
References (Official ISACA):
* ISACA, Follow-Up Audits and Follow-Up Process: The Auditor's Impact Litmus Tool
* ISACA, The Top-Five Audit Essentials for Driving Efficiency and Value

NEW QUESTION: 25
就IT治理而言，價口交付的首要目標是：
A. 推廣最佳實踐
B. 提高效率。
C. 優化投資。
D. 確保合規。
Answer: (SHOW ANSWER)
The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and

risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities.
References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 26
管理層要求對新實施的採購系統進行實施後評估，以確定其在多大程度上滿足了業務需求。下列哪一項最可能被評估？
A. 採購指南與政策
B. 實施方法
C. 線處理結果
D. 測試結果
Answer: C (LEAVE A REPLY)
A post-implementation review is a process of evaluating the outcome and benefits of a project or a system after it has been implemented. The main purpose of a post-implementation review is to determine to what extent the business requirements are being met by the new system. Therefore, the most likely aspect to be assessed is the results of line processing, which refers to the actual performance and functionality of the system in the operational environment.

NEW QUESTION: 27
在將審計報告提交給專案指導委員會之前，應該由誰先評估？
A. 資訊系統稽核經理
B. 企業主
C. 審計委員會
D. 專案發起人
Answer: (SHOW ANSWER)

NEW QUESTION: 28
資訊系統審計員正在評估備份效能，發現系統管理員會在意外的高峰使用期間手動口動備份。下列哪一項是審計員的最佳做法？
A. 審口職責分離文件。
B. 驗證負載平衡器配置。
C. 建議使用基於雲端的備份。
D. 檢口日誌以驗證備份是否及時執行。
Answer: D (LEAVE A REPLY)
A key aspect ofbackup managementis ensuring backups are performed on time and without manual intervention to avoid human error.

Option A (Incorrect):While separation of duties is important, the concern here is not aconflict of interestbut rather the reliability of backup execution.
Option B (Incorrect):Load balancer configuration relates tonetwork traffic management, which is not directly relevant to backup reliability.
Option C (Incorrect):Cloud-based backups can be a good option, but the immediate priority is toverify if backups are consistently executedbefore suggesting alternative solutions.
Option D (Correct):Reviewing backup logs provides concreteevidenceof whether backups are performed on schedule and if they weremisseddue to peak usage periods. If issues are found, automation or scheduling adjustments may be recommended.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers backup procedures, performance monitoring, and audit approaches.

NEW QUESTION: 29
資訊系統審計員正在審□某組織的發布管理實踐，發現其對業務應用程式開發專案的規模和複雜性估計不一致且不準確。為了解決這個問題，審計員應該建議採取下列哪一項措施？
A. 功能點分析
B. 快速應用程式開發
C. 敏捷開發方法
D. 關鍵路徑法
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
下列哪項活動最可能提升□部稽核品質？
A. 加強審計人員培訓
B. 外包□部稽核職能
C. 增加計劃審計的數量
D. 進行客□調□
Answer: A (LEAVE A REPLY)
The activity most likely to increase internal audit quality is increasing audit staff training. ISACA's resources on audit capability and internal audit development consistently emphasize building knowledge and skills as a way to improve audit effectiveness and quality. Training strengthens auditors' technical competence, professional judgment, and ability to identify emerging and atypical risks.
Option A is correct because better-trained auditors are more capable of planning effectively, gathering reliable evidence, assessing controls, and producing useful findings. ISACA training resources emphasize foundational and practical audit knowledge, while reskilling guidance highlights the need for internal audit to improve capability in response to changing risks.

Option B is not the best answer because outsourcing may or may not improve quality; it depends on the provider and governance over the arrangement. It is not inherently more effective than developing internal capability.
Option C is incorrect because increasing the number of planned audits can easily reduce quality if resources are stretched thinner. More volume does not automatically mean better audit work.
Option D can support continuous improvement, but client surveys are an indirect feedback tool. They do not improve technical audit quality as directly as stronger auditor training and competency.
Therefore, A is the best answer because improving auditor competence through training is the most direct and reliable way to increase internal audit quality.
References (Official ISACA):
* ISACA, IT Audit Fundamentals Certificate - emphasizes foundational audit concepts and practical application of audit principles.
* ISACA Journal, Reskilling Internal Audit - highlights the need for internal audit to improve capabilities to identify emerging and atypical risk.
* ISACA Now Blog, Internal Auditing With an Agile Scrum Approach - collaboration and feedback can improve quality and relevance, but competence remains foundational.

NEW QUESTION: 31
下列哪一項是把災難復原計畫(DRP)歸類為機密的最重要原因？
A. 確保遵守資料分類政策。
B. 防止未經授權的更改。
C. 遵守業務連續性最佳實務。
D. 降低可能導致攻擊的資料外洩風險。
Answer: (SHOW ANSWER)
The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.
The other options are not as important as reducing the risk of data leakage that could lead to an attack:
Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.
Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized

alteration by implementing access controls, audit trails, version control, and change management processes. Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.
Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

NEW QUESTION: 32
資訊系統審計員了解到，該組織在其分散式環境中經歷了多次伺服器故障。
下列哪一項是限制未來伺服器故障潛在影響的最佳建議？
A. 冗餘通路
B. 聚類
C. 故障轉移電源
D. 平行測試
Answer: B (LEAVE A REPLY)
Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failoverpower, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

NEW QUESTION: 33
某組織指派了兩名資訊系統審計員對一個資訊系統實施情況進行審計。其中一名審計員擁有資訊科技相關學位，另一名擁有商科學位。下列哪一項對於達到資訊系統審計的熟練程度標準最為重要？
A. 只要有一個成員擁有全球認可的審核認證，就符合這個標準。
B. 必須採用技術合作外包來幫助新員工。
C. 團隊成員的分配必須基於個人能力。

D. 只要主管審核新審計員的工作，就符合標準。

Answer: C (LEAVE A REPLY)

Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks.

Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently. References: CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

NEW QUESTION: 34

資訊系統審計員發現，公司高層鼓勵員工將社交網站用於商業用途。下列哪一項建議最有助於降低資料外洩的風險？

A. 要求員工簽署政策確認書和保密協議。

B. 提供員工有關社群網站使用的教育和指導

C. 對機密資料建立嚴格的存取控制

D. 監控員工社群網路使用情況

Answer: (SHOW ANSWER)

While all the options can help reduce the risk of data leakage, providing education and guidelines to employees on the use of social networking sites would be the most effective. This is because it directly addresses the issue at hand - the use of social networking sites for business purposes1. Education and guidelines can help employees understand the risks associated withsocial media use and teach them how to safely and responsibly use these platforms for business purposes1. This includes understanding privacy settings, recognizing phishing attempts, and knowing what information should not be shared on these platforms1.

References:

10 Social Media Guidelines for Employees in 2023 - Hootsuite

NEW QUESTION: 35
在審計為員工實施的網路釣魚模擬測試的有效性時，資訊系統審計員最應該關注下列哪項發現？
A. 未通過測驗的員工未接受後續教育
B. 測試結果未傳達給工作人員。
C. 工作人員事先沒有收到有關測試的通知。
D. 測試前未提供安全意識訓練。
Answer: A (LEAVE A REPLY)
The IS auditor should be most concerned about the lack of follow-up education for staff members who failed the phishing simulation test. Phishing simulation tests are designed to assess the level of awareness and susceptibility of staff members to phishing attacks, and to provide feedback and training to improve their security behavior. If staff members who failed the test do not receive follow-up education, they will not learn from their mistakes and may continue to fall victim to real phishing attacks, which could compromise the security of the organization.
The other options are less concerning for the IS auditor:
Test results were not communicated to staff members. This is not ideal, as staff members should receive feedback on their performance and learn from the test results. However, this does not necessarily mean that they did not receive any training or education on how to avoid phishing attacks.
Staff members were not notified about the test beforehand. This is a common practice for phishing simulation tests, as it mimics the real-world scenario where staff members do not know when they will receive a phishing email. The purpose of the test is to measure their spontaneous reaction and awareness, not their preparedness or compliance.
Security awareness training was not provided prior to the test. This is not a major concern, as the test can serve as a baseline measurement of the current level of awareness and susceptibility of staff members, and as a starting point for providing tailored training and education based on the test results.

NEW QUESTION: 36
降低抽樣風險最有效的方法是增加：
A. 審計抽樣訓練。
B. 信賴區間。
C. 人口。
D. 樣本數。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37

下列何者最能幫助資訊系統審計師確定最終使用者計算 (EUC) 審計中財務報告電子表格的優先順序？

A. 決定哪些電子表格使用頻率最高

B. 根據文件大小審口電子表格

C. 辨識口建巨集的電子表格

D. 了解每個電子表格的用途

Answer: D (LEAVE A REPLY)

NEW QUESTION: 38

組織制定了可接受使用政策，但使用者並未正式確認該政策。

下列哪一項是該發現帶來的最嚴重風險？

A. 缺乏衡量合規性的數據

B. 違反業界標準

C. 不符合文件要求

D. 缺乏使用者問責制

Answer: (SHOW ANSWER)

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

NEW QUESTION: 39

下列哪一項最適合用於對業務應用程式的資料和設定檔進行詳細測試？

A. 版本控制軟體

B. 審計鉤子

C. 實用軟體

D. 審計分析工具

Answer: (SHOW ANSWER)

The best tool for detailed testing of a business application's data and configuration files is an audit analytics tool. An audit analytics tool is a software that helps auditors to analyze large sets of data and identify anomalies, trends, and patterns that are relevant to the audit objectives. An audit analytics tool can also provide audit evidence and support the auditor's professional judgment and conclusions.

Some of the benefits of using an audit analytics tool are:

It can improve the efficiency and effectiveness of the audit by reducing the time and effort required to perform manual tests and procedures.
It can enhance the quality and reliability of the audit by increasing the coverage and accuracy of the data analysis and testing.
It can enable the auditor to perform more complex and sophisticated tests and procedures that may not be possible or feasible with traditional methods.
It can help the auditor to discover new insights and risks that may not be apparent or detectable with traditional methods.
Some examples of audit analytics tools are:
IDEA: A data analysis software that allows auditors to import, analyze, and visualize data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, and regression analysis.1 ACL: A data analysis software that helps auditors to access, analyze, and report on data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford' s law, regression analysis, and scripting.2 TeamMate Analytics: A data analysis software that integrates with Microsoft Excel and provides auditors with a range of tools and functions to perform data analysis and testing. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, regression analysis, and scripting.3

NEW QUESTION: 40
資訊系統審計員正在審口一個機器學習模型，該模型可以預測使用者觀看某部電影的可能性。下列哪一項最令審計員擔憂？
A. 用於訓練模型的資料集來自不可靠的來源。
B. 此模型採用開源程式語言開發。
C. 使用與訓練資料來自同一人群的資料對模型進行了測試。
D. 當使用來自不同人群的數據測試該模型時，準確率下降了。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
下列哪一種滅火系統需要與自動開關搭配使用，以便在口動時切斷電源？
A. 二氧化碳
B. FM-200
C. 幹管
D. 哈龍
Answer: A (LEAVE A REPLY)
Carbon dioxide fire suppression systems need to be combined with an automatic switch to shut down the electricity supply in the event of activation. This is because carbon dioxide displaces oxygen in the air and can create a suffocation hazard for people in the protected

area. Therefore, it is essential to cut off the power source before releasing carbon dioxide to avoid electrical shocks and sparks that could ignite the fire again.
Carbon dioxide systems are typically used for total flooding applications in spaces that are not habitable, such as server rooms or data centers.

NEW QUESTION: 42
IT治理應由以下因素驅動：
A. 業務部門舉措。
B. 平衡計分卡。
C. 政策與標準。
D. 組織策略。
Answer: (SHOW ANSWER)
IT governance should be driven by organizational strategies. It provides a formal structure for organizations to produce measurable results toward achieving their strategies and ensures that IT investments support business objectives12. While business unit initiatives, balanced scorecards, and policies and standards can play a role in IT governance, they are tools or methods that support the implementation of the organizational strategies.

NEW QUESTION: 43
下列哪一項是發布計畫的主要作用？
A. 它標識 IT 環境中的所有設定項。
B. 它提供了將新版本部署到生口環境的時間表和計劃。
C. 概述了資料庫整合的步驟。
D. 它評估對 IT 系統所提出的變更和更新的影響。
Answer: (SHOW ANSWER)
The best answer is B. It provides a timeline and schedule for deploying new releases into production.
ISACA release and change guidance explains that successful deployment requires scrutiny over change and release, including scheduling, coordination among parties, and validation before implementation. That aligns directly with the role of a release plan: organizing when and how releases move into production.
Option A is more closely related to configuration management. Option C is too narrow because release plans cover much more than database integration. Option D is more closely associated with change evaluation and impact assessment before approval. The release plan's main function is the coordinated timeline and schedule for production rollout.
References (Official ISACA):
* ISACA Journal, Implementing Emerging Technologies
* ISACA Journal, Speeding Up Software Delivery With Effective Change Management

NEW QUESTION: 44

對IT介面控制的審口發現，某組織沒有辨識和修正未傳送到接收系統的記錄的流程。下列哪一項是資訊系統審計師的最佳建議？

A. 口用資料檔案的自動加密解密和電子簽名

B. 實現軟體以自動核對系統間的數據

C. 讓編碼員手動核對系統間的資料。

D. 盡可能實現系統間資料傳輸的自動化

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 45

在審計過程中，所有相關IT 團隊都同意一項 IT 問題，但沒有團隊願意承擔補救責任，也沒有團隊認為問題屬於其職責範圍。下列哪一項是資訊系統審計員的最佳行動方案？

A. 請回報 IT 管理階層尋求解決方案。

B. 發布調口結果，但不指明所有者

C. 將共同責任分配給所有 IT 團隊。

D. 確定最合適的團隊並進行相應分配。

Answer: A (LEAVE A REPLY)

The best course of action for the IS auditor is A. Escalate to IT management for resolution. This is because IT management is responsible for overseeing and coordinating the IT activities and functions within the organization, and ensuring that they comply with the audit findings and recommendations1. IT management can help resolve the issue of finding ownership by:

Clarifying and communicating the roles and responsibilities of each IT team, and how they relate to the finding and its remediation2.

Evaluating and assigning the finding to the most appropriate IT team, based on their expertise, authority, and availability2.

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

NEW QUESTION: 46

防火牆可以緩解下列哪一種威脅？
A. 特洛伊木馬
B. 入侵攻擊
C. 非同步攻擊
D. 被動攻擊
Answer: (SHOW ANSWER)

NEW QUESTION: 47
下列哪一份文件最有助於發現職責分離上的缺陷？
A. 系統流程圖
B. 資料流程圖
C. 流程圖
D. 實體關係圖
Answer: C (LEAVE A REPLY)
The best document for an IS auditor to use in detecting a weakness in segregation of duties is a process flowchart. A process flowchart is a diagram that illustrates the sequence of steps, activities, tasks, or decisions involved in a business process. A process flowchart can help detect a weakness in segregation of duties by showing who performs what actions or roles in a process, and whether there is any overlap or conflict of interest among them. The other options are not as useful as a process flowchart in detecting a weakness in segregation of duties, as they do not show who performs what actions or roles in a process. A system flowchart is a diagram that illustrates the components, functions, interactions, or logic of an information system. A data flow diagram is a diagram that illustrates how data flows from sources to destinations through processes, stores, or external entities. An entity-relationship diagram is a diagram that illustrates how entities (such as tables) are related to each other through attributes (such as keys) in a database. References: CISA ReviewManual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 48
在審口業務流程改善專案時，首要關注點應該是什麼？
A. 持續監測計劃
B. 商業項目計劃

C. 新控制的成本
D. 業務影響
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
在審口擬議的第三方系統實施方案的商業案例時，資訊系統審計員最應該關注下列哪一項？
A. 缺乏持續維護成本
B. 缺乏訓練教材
C. 缺乏試點實施計劃
D. 缺乏詳細的工作分解結構
Answer: A (LEAVE A REPLY)
The IS auditor's greatest concern when reviewing a business case for a proposed implementation of a third- party system should be A. Lack of ongoing maintenance costs. This is because ongoing maintenance costs are an essential part of the total cost of ownership (TCO) of a third-party system, and they can have a significant impact on the return on investment (ROI) and the feasibility of the project. If the business case does not include ongoing maintenance costs, it may underestimate the true cost of the project and overestimate the benefits. This could lead to poor decision making and unrealistic expectations.
Lack of training materials (B), lack of plan for pilot implementation , and lack of detailed work breakdown structure (D) are also potential issues that could affect the quality and success of the project, but they are not as critical as lack of ongoing maintenance costs. Training materials can be developed or acquired later, pilot implementation can be planned during the project initiation or planning phase, and work breakdown structure can be refined as the project progresses. However, ongoing maintenance costs are difficult to change or estimate once the project is approved and implemented, and they can have long-term implications for the organization. Therefore, they should be included and analyzed in the business case.

NEW QUESTION: 50
下列哪一種風險情形可以透過使用資料遺失防護 (DLP) 工具得到最佳緩解？
A. 一名員工正在將公司文件發送到外部電子郵件以提高工作效率。
B. 員工在文件上選擇了錯誤的資料分類。
C. 員工在測試環境中使用生口資料。
D. 前僱員保留透過單一登入 <SSO) 進行身份驗證的應用程式的存取權。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
下列哪一項是資訊科技指導委員會的主要職責？
A. 檢討並協助IT策略整合工作

B. 制定和評估資訊科技安全策略
C. 實施將安全性與業務目標結合的流程
D. 開發與實施安全系統開發框架
Answer: (SHOW ANSWER)
This means that the IT steering committee is responsible for ensuring that the IT strategy aligns with and supports the business strategy, vision, and goals of the organization. The IT steering committee is also responsible for overseeing and approving major IT initiatives, projects, and investments, and allocating resources and priorities accordingly12.
Developing and assessing the IT security strategy (B) is not the main responsibility of the IT steering committee, but rather a specific aspect of the IT strategy that may be delegated to a subcommittee or a dedicated security function. The IT steering committee may provide guidance and oversight for the IT security strategy, but it is not directly involved in developing and assessing it12.
Implementing processes to integrate security with business objectives is not the main responsibility of the IT steering committee, but rather an operational task that may be performed by the IT management and staff. The IT steering committee may monitor and evaluate the effectiveness of the security processes, but it is not directly involved in implementing them12.
Developing and implementing the secure system development framework (D) is not the main responsibility of the IT steering committee, but rather a technical task that may be performed by the IT developers and engineers. The IT steering committee may approve and endorse the secure system development framework, but it is not directly involved in developing and implementing it12.

NEW QUESTION: 52
以下調□結果是資訊系統審計員對新實施的系統進行實施後審□的結果。下列哪一項調□結果最為重要？
A. 從未舉行過經驗教訓總結會議。
B. 此專案預算超支 10% 的情況沒有向高階主管報告。
C. 未定義可衡量的收益。
D. 每月儀表板並不總是包含交付成果。
Answer: (SHOW ANSWER)
A post-implementation review (PIR) is a process to evaluate whetherthe objectives of the project were met, determine how effectively this wasachieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of projects1. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.
One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project. Measurable benefits are the quantifiable and verifiable results or outcomes that the project

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

budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.
References: 1: What is Post-Implementation Review in Project Management? 2: The role and importance of the Post Implementation Review

NEW QUESTION: 53
在資訊安全審口過程中，資訊系統審計員了解到，某組織政策要求所有員工在每年新年第一周參加資訊安全培訓。為了確保一月後入職的員工獲得足口的安全意識指導，審計員的最佳建議是什麼？
A. 確保新進員工口讀並簽署可接受使用政策的確認書。
B. 修改政策，在入職訓練期間加入安全訓練
C. 修改政策，要求所有員工每六個月接受一次安全訓練
D. 要求新員工的管理階層提供安全意識概述。
Answer: B (LEAVE A REPLY)
This directly addresses the gap for new hires, creates a consistent expectation regardless of hiring date, and formalizes the process within organizational policy.
References
ISACA CISA Review Manual (Current Edition) - Chapters on Information Security Policies, Training and Awareness Industry Best Practices for Security Awareness - Emphasize the importance of timely and comprehensive training for new employees.

NEW QUESTION: 54
由於近期業務剝離，某組織用於交付關鍵專案的IT 資源有限。在評估未來專案的資源需求時，IT 管理階層應如何根據下列哪一項來檢視 IT 人員配備計畫？
A. 人力資源(HR)採購策略
B. 專案實際耗時記錄
C. 同行業組織人員配置基準
D. 下一財政年度的預算預測
Answer: B (LEAVE A REPLY)
The best source of information for IT management to estimate resource requirements for future projects is the records of actual time spent on projects. This data can provide a realistic and reliable basis for forecasting future resource needs based on historical trends and patterns. The records of actual time spent on projects can also help IT management to identify any gaps or inefficiencies in resource allocation and utilization. The human resources (HR) sourcing strategy is not a good source of information for estimating resource requirements for future projects, as it may not reflect the actual demand and availability of IT resources. The peer organization staffing benchmarks are not a good source of information for estimating resource requirements for future projects, as they may not account for the specific characteristics and needs of each organization. The budgeted

forecast for the next financial year is not a good source of information for estimating resource requirements for future projects, as it may not be based on accurate or realistic assumptions. References:
CISA Review Manual, 27th Edition, pages 465-4661
CISA Review Questions, Answers and Explanations Database,Question ID: 263

NEW QUESTION: 55
下列哪一項是促進資訊系統審計流程和實務持續改進的最佳方法？
A. 邀請外部審計師和監管機構對資訊系統審計職能進行定期評估。
B. 對資訊系統審計交付成果實施嚴格的管理審口及簽署確認。
C. 經常審口資訊系統審計政策、程序和操作手冊。
D. 在資訊系統審計職能中建立和嵌入品質保證(QA)。
Answer: (SHOW ANSWER)
The best way to foster continuous improvement of IS audit processes and practices is to establish and embed quality assurance (QA) within the IS audit function, as this will ensure that the IS audit activities are aligned with the standards, expectations, and objectives of the organization and the stakeholders12. QA involves periodic internal and external assessments, benchmarking, feedback, and root cause analysis to identify and address gaps, issues, and opportunities for improvement34.
References
1: The Basics and Principles of Continuous Improvement4 2: ISO 9001 Auditing Practices Group Guidance on5 3: INSIGHTS TO QUALITY3 4: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance2

NEW QUESTION: 56
在對企業資源計劃 (ERP) 系統進行審計時，資訊系統審計員發現生口環境中應用了一個應用程式修補程式。資訊系統審計員最重要的是核實該補丁是否已獲得以下方面的批准：
A. 系統管理員。
B. 資訊資口所有者。
C. 專案經理。
D. 資訊安全官。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
專案指導委員會的主要職責是：
A. 簽署最終建置文件。
B. 確保每個項目都準時完成。
C. 確保開發的系統符合業務需求。
D. 提供定期專案更新和監督。
Answer: D (LEAVE A REPLY)

The primary responsibility of a project steering committee is to provide regular project updates and oversight.
A project steering committee is an advisory group that consists of senior stakeholders and experts who offer guidance and support to a project manager and their team. The steering committee is mainly concerned with the direction, scope, budget, timeline, and methods used to realize a given project1.
One of the key roles of a steering committee is to monitor the progress and performance of the project and ensure that it aligns with the business objectives and stakeholder expectations. The steering committee also provides feedback, advice, and recommendations to the project manager and helps them resolve any issues or challenges that may arise during the project lifecycle. The steering committee communicates regularly with the project manager and other stakeholders through meetings, reports, and presentations23.
Therefore, providing regular project updates and oversight is the primary responsibility of a project steering committee.
References:
Steering Committee: Definition, Roles and Meeting Tips - ProjectManager Project Steering Committee: Roles, Best Practices, Challenges - ProjectPractical Steering Committee: Complete Guide with Examples and Templates - Status.net

NEW QUESTION: 58
資訊系統審計員正在審□一個基於網路的客□關係管理 (CRM) 系統的安全性，該系統可透過網際網路直接供客□存取。下列哪一項是審計員應該關注的問題？
A. 此系統託管在外部第三方服務提供者的伺服器上。
B. 此系統託管在由服務供應商管理的混合雲平台上。
C. 此系統託管在企業網路的非軍事區(DMZ)□。
D. 此系統託管在企業網路的□部網段中。
Answer: D (LEAVE A REPLY)
A web-based CRM system that is directly accessed by customers via the Internet should be hosted in a secure and isolated environment to protect it from external threats and unauthorized access. A web-based CRM system should also be reliable, trusted, and backedup regularly1.
Hosting the system on an external third-party service provider's servers (A) or a hybrid-cloud platform managed by a service provider (B) may not be a concern for the auditor if the service provider has adequate security measures and service level agreements in place. The auditor should verify the security controls and contractual terms of the service provider before trusting them with the CRM data23.
Hosting the system within a demilitarized zone (DMZ) of a corporate network is a common practice to provide an extra layer of security to the CRM system from untrusted networks, such as the Internet. A DMZ is a perimeter network that isolates the CRM system from the

internal network and filters the incoming traffic from the external network using a security gateway4567.
Hosting the system within an internal segment of a corporate network (D) is a concern for the auditor because it exposes the CRM system and the internal network to potential attacks from the Internet. The CRM system should not be directly accessible from the Internet without a DMZ or a firewall to protect it. This could compromise the confidentiality, integrity, and availability of the CRM data and the internal network78.

NEW QUESTION: 59
當管理階層做出回應時，資訊系統審計師首先應該做什麼？
面對面的口部控制問卷調口表明，一項關鍵的口部控制措施
控制措施不再有效？
A. 決定使控制有效所需的資源。
B. 驗證口部控制的整體效度。
C. 驗證控制措施不再有效的影響。
D. 確定是否有其他補償控制措施。
Answer: D (LEAVE A REPLY)
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because theyeither require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

NEW QUESTION: 60
下列何者最能幫助審計人員得出已實施的資料分類程序有效性的結論？
A. 購買資訊管理工具
B. 業務用例和場景
C. 根據方案提供的存取權限
D. 詳細的資料分類方案
Answer: C (LEAVE A REPLY)
Access rights provisioned according to scheme would best help to support an auditor's conclusion about the effectiveness of an implemented data classification program. This would indicate that the data classification program has been properly implemented and enforced, and that the data is protected according to its sensitivity and value. The other options are not sufficient to demonstrate the effectiveness of a data classification program,

as they do not show how the data is actually accessed and used by authorized users.
References:
CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
CISA Review Questions, Answers and Explanations Database, Question ID 2042

NEW QUESTION: 61
將業務影響分析 (BIA) 引入業務彈性策略的主要好處是什麼？
A. 它列出了因業務服務中斷而可能口生的法律義務。
B. 它提供有關可能發生的災害風險等級的最新資訊。
C. 它闡明了組織在危機中必須履行的員工職責。
D. 它有助於確定係統和應用程式復原的優先順序。
Answer: (SHOW ANSWER)
The primary purpose of a Business Impact Analysis (BIA) is to prioritize the restoration of systems and applications (D) based on their criticality to business operations. A BIA assesses the impact of disruptions, identifies critical processes, and determines recovery time objectives (RTOs) and recovery point objectives (RPOs).
Other options:
Identifying legal obligations (A) is an aspect of compliance but not the primary benefit of a BIA.
Providing updates on disaster risk levels (B) falls under risk management rather than BIA objectives.
Delineating employee responsibilities (C) is part of business continuity planning (BCP), not the BIA's main goal.
Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

NEW QUESTION: 62
資訊系統審計師正在驗證組織口部控制的充分性，並擔心可能存在規避法規的情況。下列哪一項是最佳的抽樣方法？
A. 變數抽樣
B. 隨機抽樣
C. 聚類抽樣

D. 屬性抽樣

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 63

當資料所有者為資料分配了錯誤的分類等級時，資訊系統審計員最應該關注的是下列哪一項？

A. 可能無法採取充分措施來保護資料。

B. 資料可能未經系統管理員加密。

C. 競爭對手可能能□□看數據。

D. 控製成本可能超過 IT 資□的□在價□。

Answer: A (LEAVE A REPLY)

The answer A is correct because the greatest concern for an IS auditor when a data owner assigns an incorrect classification level to data is that controls to adequately safeguard the data may not be applied. Data classification is the process of categorizing data assets based on their information sensitivity and business impact. Data classification helps organizations to identify, protect, and manage their data according to their value and risk. Data owners are the individuals or entities who have the authority and responsibility to define, classify, and control the access and use of their data.

Data classification typically involves assigning labels or tags to data assets, such as public, internal, confidential, or restricted. These labels indicate the level of protection and handling required for the data.

Based on the data classification, organizations can implement appropriate controls to safeguard the data, such as encryption, access control lists, audit logs, backup policies, etc. These controls help to prevent unauthorized access, disclosure, modification, or loss of data, and to ensure compliance with relevant laws and regulations.

If a data owner assigns an incorrect classification level to data, it can result in either underprotection or overprotection of the data. Underprotection means that the data is classified at a lower level than it should be, which exposes it to higher risks of compromise or breach. For example, if a data owner classifies personal health information (PHI) as public instead of confidential, it may allow anyone to access or share the data without proper authorization or consent. This can violate the privacy rights of the data subjects and the compliance requirements of regulations such as HIPAA (Health Insurance Portability and Accountability Act). Overprotection means that the data is classified at a higher level

than it should be, which limits its availability or usability. For example, if a data owner classifies marketing materials as restricted instead of public, it may prevent potential customers or partners from accessing or viewing the data. This can reduce the business value and opportunities of the data.
Therefore, an IS auditor should be concerned about the accuracy and consistency of data classification by data owners, as it affects the security and efficiency of data management. An IS auditor should review the policies and procedures for data classification, verify that the data owners have adequate knowledge and skills to classify their data, and test that the data classification labels match with the actual sensitivity and impact of the data.
References:
Data Classification: What It Is and How to Implement It
What Is Data Classification? - Definition, Levels and Examples ...
Data Classification: A Guide for Data Security Leaders

NEW QUESTION: 64
下列哪一項是資訊系統審計員為幫助組織提高計算資源效率所提出的最佳建議？
A. 硬體升級
B. 虛擬化
C. 中央處理器(CPU)超頻
D. 即時備份
Answer: (SHOW ANSWER)

NEW QUESTION: 65
下列哪一個關鍵績效指標(KPI)能口為利害關係人提供資訊安全風險是否得到管理的最有用資訊？
A. 從識別安全威脅到實施解決方案所需的時間
B. 已審計的安全控制數量
C. 從安全日誌捕捉到日誌分析的時間
D. 安全風險登記冊中的條目數量
Answer: A (LEAVE A REPLY)
Thespeed at which security threats are mitigatedis akey indicatorof an organization ' srisk management effectiveness.
Option A (Correct):Response time to security threatsmeasures how efficiently security teams detect, analyze, and mitigate risks, providingclear insight into security operations.
Option B (Incorrect):The number of security controls auditeddoes not indicatehow well risk is being managed, only that reviews are taking place.
Option C (Incorrect):Log analysis speedis useful, but it does notdirectly measure risk mitigation effectiveness.
Option D (Incorrect):Risk register entriesindicate known risks but do not provide insight intohow well those risks are managed.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coverssecurity metrics, KPIs, and risk management evaluation.

NEW QUESTION: 66
下列哪一項是實施組態管理資料庫(CMDB)的最佳理由？
A. 用於儲存軟體設定項的許可證
B. 提供配置項目的即時網路監控
C. 用於追蹤配置項的物理位置
D. 用於記錄配置項之間的關係
Answer: D (LEAVE A REPLY)
The best answer is D. To document relationships between configuration items.
ISACA's configuration management guidance identifies the value of a CMDB in maintaining information about configuration items and their relationships. That relationship view is what supports effective impact analysis, change management, incident response, and dependency understanding across the environment.
Option A is too narrow. Option B describes monitoring rather than configuration management. Option C may be one data element in some environments, but the defining value of a CMDB is not physical location tracking. The central purpose is documenting configuration items and how they relate to one another.
References (Official ISACA):
* ISACA Glossary / configuration management references.

NEW QUESTION: 67
在測試磁帶備份程序的充分性時，哪個步驟最能驗證定期規劃的備份是否及時完成？
A. 觀察每日備份運行的執行情況
B. 評估備份策略與流程
C. 在備份過程中，對關鍵人員的訪談方式發生了變化
D. 檢視系統口生的備份日誌樣本
Answer: D (LEAVE A REPLY)
Reviewing a sample of system-generated backup logs is the best step to verify that regularly scheduled backups are timely and run to completion. Backup logs are records that document the details and results of backup operations, such as the date, time, duration, status, errors, and exceptions. By reviewing a sample of backup logs, the IS auditor can check whether the backups are performed according to the schedule and whether they are completed successfully or not. The other steps do not provide as much evidence or assurance as reviewing backup logs, as they do not show the actual outcome or performance of backup operations. References: CISA Review Manual, 27th Edition, page 247

NEW QUESTION: 68
下列哪一種技術在設備間資料傳輸方面的最大範圍最小？

A. Wi-Fi
B. 藍牙
C. 長期演進(LTE)
D. 近場通訊(NFC)
Answer: (SHOW ANSWER)
The technology that has the smallest maximum range for data transmission between devices is near-field communication (NFC). NFC is a short-range wireless technology that enables two devices to communicate when they are in close proximity, usually within a few centimeters. NFC is commonly used for contactless payments, smart cards, and device pairing. According to the Bluetooth Technology Website1, the effective range of NFC is less than a meter, while the other technologies have much longer ranges. Wi-Fi can reach up to 100 meters indoors and300 meters outdoors2. Bluetooth can reach up to 800 feet with Bluetooth5.0 specification3. Long-term evolution (LTE) canreach up to several kilometers depending on the cell tower and the device4.
References:
5: What is Wi-Fi? - Definition from WhatIs.com
6: Understanding Bluetooth Range | Bluetooth Technology Website
7: What is Bluetooth Range? What You Need to Know
8: How far can LTE signals travel? - Quora

NEW QUESTION: 69
選擇來年要執行哪些資訊系統審計的主要依據應該是什麼？
A. 高階主管的要求
B. 上年度審計結果
C. 組織風險評估
D. 先前的審計覆蓋範圍和範圍
Answer: C (LEAVE A REPLY)
The primary basis for selecting which IS audits to perform in the coming year is the organizational risk assessment. An organizational risk assessment is a formal process for identifying, evaluating, and controlling risks that may affect the achievement of the organization'sgoals and objectives3. An organizational risk assessment can help IS auditors prioritize and plan their audit activities based on the level of risk exposure and impact of each area or process within the organization. An organizational risk assessment can also help IS auditors align their audit objectives and criteria with the organization's strategy and performance indicators.
Senior management's request, prior year's audit findings, and previous audit coverage and scope are also possible bases for selecting which IS audits to perform in the coming year, but not as primary as the organizational risk assessment. These factors are more secondary or supplementary sources of information that can help IS auditors refine or adjust their audit plan based on specific needs or issues identified by management or previous audits. However, thesefactors may not reflect the current or emerging risks that

may affect the organization's operations or performance. References: ISACA CISA Review Manual 27th Edition, page 295

NEW QUESTION: 70
下列何者是組織策略規劃措施中缺乏 IT 參與所帶來的最大風險？
A. 業務策略可能與 IT 能力不符。
B. 商業策略可能不會考慮新興技術。
C. IT策略可能與業務策略不一致。
D. IT策略目標可能未被業務部門考慮。
Answer: C (LEAVE A REPLY)
IfIT is not involvedinstrategic planning,IT strategy may diverge from business needs, leading tomisalignment and inefficiencies.
Option A (Incorrect):Business strategy alignmentis important, but the greater risk is thatIT investments do not support business goals.
Option B (Incorrect):Lack of emerging technology awareness is a risk, butIT-business misalignment has broader consequences.
Option C (Correct):Thegreatest riskis when IT strategyfails to align with business objectives, leading towasted investments, inefficiencies, and competitive disadvantages.
Option D (Incorrect):IT goals being overlooked is a concern, butmisalignment of IT and business strategies is a more critical risk.
Reference:ISACA CISA Review Manual -Domain 2: Governance and Management of IT-Coversstrategic IT alignment and governance best practices.

NEW QUESTION: 71
透過保護生口原始碼庫可以最好地解決以下哪個問題？
A. 程式在生口原始碼庫更新之前未經批准。
B. 生口環境的原始碼庫和物件庫可能不同步。
C. 更改應用到了錯誤版本的生口原始碼庫。
D. 未經授權的變更可能會部署到生口環境。
Answer: D (LEAVE A REPLY)
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21

CISA Review Questions, Answers and Explanations Database, Question ID 213

NEW QUESTION: 72
資訊系統審計師正在製定一項在特定時期口進行審計的計劃。資訊系統審計師應先執行下列哪項活動？
A. 分配審計資源。
B. 優先考慮風險。
C. 審口先前的審計報告。
D. 決定審計範圍。
Answer: D (LEAVE A REPLY)
An audit universe is a comprehensive list of all the auditable entities, processes, and activities within an organization. It helps the IS auditor to identify the scope, objectives, and priorities of the audit plan, as well as the resources and methodologies required to conduct the audits. An audit universe can also help the IS auditor to ensure that all the key risks, controls, and regulations are covered by the audit plan, and that there are no gaps or overlaps in the audit coverage.
The first activity that the IS auditor should perform when preparing a plan for audits to be carried out over a specified period is to determine the audit universe. This involves defining the criteria and methods for identifying and categorizing the auditable units, such as by business function, process, system, location, or risk level. The IS auditor should also consult with the management and otherstakeholders to obtain their input and expectations for the audit plan. The IS auditor should then document and validate the audit universe, and update it regularly to reflect any changes in the organization's structure, operations, or environment.
The other three activities are also important for preparing an audit plan, but they should be performed after determining the audit universe. Allocating audit resources involves assigning staff, time, budget, and tools to each audit based on their complexity, priority, and availability. Prioritizing risks involves assessing the likelihood and impact of each risk associated with each auditable unit, and ranking them according to their significance and urgency. Reviewing prior audit reports involves analyzing the findings, recommendations, and actions from previous audits related to each auditable unit, and evaluating their current status and relevance.
Therefore, determining the audit universe is the best answer.
References:
Audit Universe - UPDATED 2022 - Examples, Templates and More!
01 February 2023 Audit universe - IIA

NEW QUESTION: 73
下列哪一項對資訊安全計畫的成功最為關鍵？
A. 資訊安全與 IT 目標的協調一致

B. 管理階層對資訊安全的承諾
C. 商業與資訊安全的融合
D. 使用者對資訊安全的責任
Answer: B (LEAVE A REPLY)
The correct answer is B. Management's commitment to information security.
Management's commitment to information security is the most critical factor for the success of an information security program, as it provides the leadership, support, and resources needed to establish and maintain a secure environment.
Management's commitment to information security can be demonstrated by:
Setting the vision, mission, and goals for information security, and aligning them with the organization's strategies and objectives1.
Establishing and enforcing the policies, standards, and procedures for information security, and ensuring compliance with relevant laws and regulations1.
Allocating sufficient budget, staff, and technology for information security, and investing in training and awareness programs2.
Promoting a culture of security within the organization, and engaging with stakeholders and partners to foster trust and collaboration2.

NEW QUESTION: 74
在重新檢視安全事件回應計畫時，進行桌面演練的主要目的應該是下列哪一項？
A. 確認技術已到位，能口支援事件回應計劃
B. 收集用於回應安全審計問詢的文件
C. 為了提高效率，以便與事件回應測試場景保持一致
D. 決定事件回應計畫的流程改善方案
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
下列哪一項對於成功建立安全漏洞管理程序最為重要？
A. 一個強大的桌面鍛鍊計劃
B. 一份全面的資口清單
C. 經過測試的事件回應計劃
D. 已核准的補丁策略
Answer: A (LEAVE A REPLY)
A comprehensive asset inventory is the most important factor for the successful establishment of a security vulnerability management program. A security vulnerability management program is a systematic process of identifying, assessing, prioritizing, and remediating vulnerabilities in the organization's IT environment1. A comprehensive asset inventory is a complete and accurate record of all the hardware, software, and network components that the organization owns or uses2. A comprehensive asset inventory helps the organization to:
Know what assets are in scope for vulnerability scanning and assessment3.

Identify the vulnerabilities that affect each asset and their severity level4.
Prioritize the remediation of vulnerabilities based on the criticality and value of each asset.
Track the status and progress of vulnerability remediation for each asset.
Measure the effectiveness and maturity of the vulnerability management program.
A robust tabletop exercise plan is a simulated scenario that tests the organization's preparedness and response capabilities for a potential cyberattack or incident. A tabletop exercise plan is useful for validating and improving the organization's incident response plan, but it is not essential for establishing a security vulnerability management program.
A tested incident response plan is a documented process that defines the roles, responsibilities, and actions of the organization's personnel in the event of a cyberattack or incident. A tested incident response plan is important for minimizing the impact and restoring normal operations after a security breach, but it is not critical for establishing a security vulnerability management program.
An approved patching policy is a set of rules and guidelines that governs how the organization applies patches and updates to its IT systems and applications. An approved patching policy is a key component of the remediation phase of the vulnerability management program, but it is not sufficient for establishing a security vulnerability management program.

NEW QUESTION: 76
下列哪一項是確保供應商遵守系統安全要求的最佳方法？
A. 要求在供應商合約中加入合規條款。
B. 檢視供應商報告的過往事件。
C. 審口供應商安全合規性的過往審計結果。
D. 要求供應商員工接受安全訓練。
Answer: (SHOW ANSWER)

NEW QUESTION: 77
某組織計劃對選定的業務流程實施控制自我評估(CSA)計劃。下列哪一項應該是口部稽核團隊在此計畫中的角色？
A. 就自我評估過程向管理階層提供建議。

B. 從未來的審計計劃中取消 CSA 涵蓋的業務流程的範圍。
C. 設計管理測試程序，以有效評估製程控制。
D. 進行測試以驗證管理階層自我評估的準確性。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
下列哪一項對於資訊系統審計員來口最為重要？
用於專案可行性研究嗎？
A. 對是否能口完全滿足要求的評估
B. 一項評估，顯示安全控制措施將有效運行
C. 對預期收益是否能口實現的評估
D. 一項評估顯示收益將超過實施成本。
Answer: C (LEAVE A REPLY)
The most important thing for an IS auditor to look for in a project feasibility study is an assessment of whether the expected benefits can be achieved. A project feasibility study is a preliminary analysis that evaluates the viability and suitability of a proposed project based on various criteria, such as technical, economic, legal, operational, and social factors. The expected benefits are the positive outcomes and value that the project aims to deliver to the organization and its stakeholders. The IS auditor should verify whether the project feasibility study has clearly defined and quantified the expected benefits, and whether it has assessed the likelihood and feasibility of achieving them within the project scope, budget, schedule, and quality parameters. The other options are also important for an IS auditor to look for in a project feasibility study, but not as important as an assessment of whether the expected benefits can be achieved, because they either focus on specific aspects of the project rather than the overall value proposition, or they assume that the project will be implemented rather than evaluating its viability. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.1

NEW QUESTION: 79
在完成IT審計後，管理階層決定接受審計報告中指出的風險。下列哪一項措施最能向資訊系統審計師保證管理階層已充分平衡業務需求與風險管理需求？
A. 已製定溝通計劃，以告知受風險影響的各方。
B. 潛在影響和可能性已被充分記錄。
C. 已識別的風險將報告給組織的風險委員會。
D. 已製定接受和批准風險的標準。
Answer: D (LEAVE A REPLY)
Clear criteria ensure a consistent, rational approach to risk acceptance decisions, demonstrating management ' s deliberate and informed approach to risk management. References

ISACA CISA Review Manual (Current Edition) - Chapter on Risk Management Risk Management Frameworks (e.g., ISO 31000, NIST SP 800-39) - Emphasize the importance of defined risk assessment and decision-making processes.

NEW QUESTION: 80
原始碼庫的設計應達到以下目的：
A. 阻止變更合併到現有程式碼中。
B. 阻止開發者存取受保護的原始程式碼。
C. 為現有程式碼提供安全的版本控制和備份功能。
D. 提供修改後程式碼的自動合併和分發。
Answer: C (LEAVE A REPLY)
A source code repository is a system that stores and manages the source code of a software project. A source code repository should be designed to provide secure versioning and backup capabilities for existing code, as these are essential features for concurrent development, code quality, and disaster recovery. Versioning allows developers to track, compare, and revert changes to the code over time. Backup ensures that the code is safely stored and can be restored in case of data loss or corruption.
References
Source Code Repositories: What is a Source Code Repository?
Git Source Code Repository Design Considerations
Best practices for repositories - GitHub Docs

NEW QUESTION: 81
下列哪一項是組織使用聚類分析的最佳理由？
A. 為了減少系統回應時間
B. 提高石灰回收目標(RTO)
C. 為了加快備援速度
D. 提高系統彈性
Answer: D (LEAVE A REPLY)
Clustering is a technique that groups multiple servers or nodes together to act as one system, providing high availability, scalability, and load balancing for applications or services. Clustering can improve system resiliency, which is the ability of a system to withstand or recover from failures or disruptions without compromising its functionality or performance. Clustering can achieve this by providing redundancy and fault tolerance for critical components or processes, enabling automatic failover and recovery in case of node failures, distributing workload among multiple nodes to avoid overloading or bottlenecks, and allowing dynamic addition or removal of nodes to meet changingdemand or capacity needs. Clustering may also decrease system response time by improving performance and efficiency through load balancing and parallel processing, but this is not its primary purpose. Clustering may facilitate faster backups by enabling concurrent backup operations across multiple nodes, but this is not its main benefit. Clustering may improve

the recovery time objective (RTO), which is the maximum acceptable time for restoring a system or service after a disruption, by reducing the downtime and data loss caused by failures, but this is not the best reason for using clustering, as there may be other factors that affect the RTO, such as backup frequency, recovery procedures, and testing methods.

NEW QUESTION: 82
對於評估組織修補程式管理流程的資訊系統稽核員而言，下列哪一項發現最令人關注？
A. 該組織的軟體清單不完整。
B. 應用程式通常需要重新口動才能使補丁生效。
C. 軟體供應商正在捆綁補丁。
D. 測試補丁需要大量時間。
Answer: (SHOW ANSWER)
The organization's software inventory is not complete. This finding would be of greatest concern to an IS auditor assessing an organization's patch management process because:
A software inventory is a list of all the software assets that an organization owns, uses, or manages. A software inventory is essential for effective patch management, as it helps identify the software that needs to be updated, the patches that are available, and the dependencies and compatibility issues that may arise.
Without a complete software inventory, an organization may miss some critical patches, expose itself to security risks, and waste resources on unnecessary or redundant patches.
Applications frequently need to be rebooted for patches to take effect. This finding would be of moderate concern to an IS auditor assessing an organization's patch management process because:
Rebooting applications for patches to take effect is a common and expected practice in some cases, especially for operating system or kernel patches. However, frequent reboots may indicate that the organization is not applying patches in a timely or efficient manner, or that the patches are not well-designed or tested. Frequent reboots may also cause disruption to the business operations and user experience, and increase the risk of data loss or corruption.
Software vendors are bundling patches. This finding would be of low concern to an IS auditor assessing an organization's patch management process because:
Bundling patches is a practice where software vendors combine multiple patches into a single package or update. Bundling patches can have some advantages, such as reducing the number of downloads and installations, simplifying the patch management process, and ensuring consistency and compatibility among patches. However, bundling patches can also have some disadvantages, such as increasing the size and complexity of the updates, delaying the delivery of critical patches, and introducing new bugs or vulnerabilities.
Testing patches takes significant time. This finding would be of low concern to an IS auditor assessing an organization's patch management process because:

Testing patches is a vital step in the patch management process, as it helps ensure that the patches are functional, secure, and compatible with the existing software and hardware environment. Testing patches can take significant time, depending on the scope, complexity, and frequency of the patches. However, testing patches is a necessary investment to avoid potential problems or failures that could result from applying untested or faulty patches.
References:
Best practices for patch management
Server Patch Management: Best Practices and Tools
11 Key Steps of the Patch Management Process

NEW QUESTION: 83
出於業務需求而發送的電子郵件儲存在員工的個人裝置上。
下列哪一項是資訊系統審計師的最佳建議？
A. 要求員工在個人裝置上使用密碼
禁止員工在個人裝置上儲存公司電子郵件
B. 確保個人裝置上安裝了防毒軟體
C. 在個人裝置上實現電子郵件容器化解決方案
Answer: C (LEAVE A REPLY)
Implementing an email containerization solution on personal devices is the best recommendation for an IS auditor, because it allows the organization to separate and secure the email data from the rest of the device data. Email containerization creates a virtual environment that encrypts andisolates the email data, preventing unauthorized access, leakage, or loss of sensitive information12. Requiring passwords or antivirus protection on personal devices may not be sufficient or enforceable, while prohibiting employees from storing companyemail onpersonal devices may not be feasible or practical. References: 1: CISA Review Manual (DigitalVersion), Chapter 5, Section 5.4.3 2: CISA Online Review Course, Module 5, Lesson 4

NEW QUESTION: 84
在開發階段新增的系統功能時，如果不遵循專案變更管理流程，則相關的主要風險是什麼？
A. 新增功能尚未記錄在案。
B. 新功能可能不符合要求。
C. 此項目可能無法依期完成。
D. 該項目可能會超出預算。
Answer: A (LEAVE A REPLY)
The main risk associated with adding a new system functionality during the development phase without following a project change management process is that the new functionality may not meet requirements (option B). This is because:

A project change management process is a set of procedures that defines how changes to the project scope, schedule, budget, quality, or resources are requested, evaluated, approved, implemented, and controlled12.
A project change management process helps to ensure that the changes are aligned with the project objectives, stakeholders' expectations, and business needs12.
Adding a new system functionality during the development phase without following a project change management process can introduce risks such as:
The added functionality has not been documented (option A), which can lead to confusion, inconsistency, errors, and rework3.
The project may fail to meet the established deadline (option C), which can result in delays, penalties, and customer dissatisfaction3.
The project may go over budget (option D), which can cause cost overruns, financial losses, and reduced profitability3.
However, the main risk is that the new functionality may not meet requirements (option B), which can have serious consequences such as:
The new functionality may not be compatible with the existing system or other components3.
The new functionality may not be tested or verified for quality, performance, security, or usability3.
The new functionality may not deliver the expected value or benefits to the users or customers3.
The new functionality may not comply with the regulatory or contractual obligations3.
The new functionality may cause dissatisfaction, complaints, or litigation from the stakeholders3.
Therefore, the main risk associated with adding a new system functionality during the development phase without following a project change management process is that the new functionality may not meet requirements (option B), as this can jeopardize the success and acceptance of the project.
References: 1: How to Make a Change Management Plan (Templates Included) - ProjectManager 2: What Is Change Management? Process and Models Explained - ProjectManager 3: 8 Steps for an Effective Change Management Process - Smartsheet

NEW QUESTION: 85
下列哪一項是財務報表審計期間最關心的問題？
A. 財務管理系統是基於雲端。
B. 系統容量尚未測試。
C. 尚未為關鍵批准者確定備份。
D. 口生關鍵報告的程序尚未獲得批准。
Answer: (SHOW ANSWER)

NEW QUESTION: 86

下列哪一項是實施資料遺失防護(DLP)工具最重要的先決條件？
A. 要求使用者將檔案保存在安全資料夾中，而不是公司共用磁碟機中。
B. 檢視資料傳輸日誌以確定資料流的歷史模式
C. 制定資料防洩漏策略並要求使用者簽章確認
D. 確定現有資料所在位置並建立資料分類矩陣
Answer: D (LEAVE A REPLY)
A data loss prevention (DLP) tool is a software application that detects and prevents data breaches by monitoring and protecting sensitive data from unauthorized access, transfer, or use1. A DLP tool can help your organization comply with regulations, prevent insider threats, and protect your intellectual property.
Before implementing a DLP tool, the most important prerequisite is to identify where existing data resides and establish a data classification matrix. This is because you need to know what data you have, where it is stored, how sensitive it is, and who can access it. A data classification matrix is a framework that defines the categories and levels of data sensitivity, such as public, internal, confidential, or restricted2. By identifying and classifying your data, you can determine the appropriate DLP policies and controls to apply to each type of data and prevent data loss or leakage.

NEW QUESTION: 87
下列哪一項是任何災害應變計畫中最重要的考量因素？
A. IT資口保護
B. 人員安全
C. 收入損失
D. 充足的資源能力
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
下列何者最能幫助組織確定其資訊安全意識計畫的有效性？
A. 衡量使用者對訓練品質的滿意度
B. 評估社會工程練習的結果
C. 檢討安全人員績效評估
D. 對幫助台呼叫次數進行分析
Answer: B (LEAVE A REPLY)
The effectiveness of an information security awareness program is best measured by assessing real-world behavior rather than subjective feedback or indirect metrics. Social engineering exercises simulate real-world attack scenarios, testing whether employees can identify and respond appropriately to security threats. This directly evaluates the program's impact on employee behavior and awareness.
* Measuring User Satisfaction (Option A):While useful for feedback, satisfaction does not measure the effectiveness of awareness in preventing security incidents.

* Reviewing Security Staff Performance Evaluations (Option C):This focuses on staff capabilities rather than the awareness program's effectiveness.
* Analyzing Help Desk Calls (Option D):This might provide insight into recurring issues but does not directly measure the program's success in changing user behavior.
Conducting social engineering exercises aligns with best practices for assessing organizational security awareness.
Reference:ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

NEW QUESTION: 89
當透過自動化介面審核兩個系統之間的日常資料流以確認其完整性和準確性時，下列哪一項是最合適的測試方法？
A. 確認應用於介面的加密標準符合最佳實務。
B. 檢口介面配置和系統的範例輸出。
C. 對兩個系統進行 25 天樣本的資料核對。
D. 對兩個系統進行程式碼審口並檢口設計文件。
Answer: (SHOW ANSWER)
The most appropriate testing approach when auditing a daily data flow between two systems via an automated interface is to perform data reconciliation between the two systems for a sample of 25 days. Data reconciliation is a process of verifying that the data transferred from one system to another is complete and accurate, and that there are no discrepancies or errors in the data flow1. Data reconciliation can be performed by using generalized audit software, which is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases2. By performing data reconciliation for a sample of 25 days, the IS auditor can test the reliability and consistency of the data flow over a reasonable period of time, and identify any potential issues or anomalies that could affect the quality of the data or the functionality of the systems.
References
1: Data Flow Testing - GeeksforGeeks 2: Generalized Audit Software (GAS) - ISACA

NEW QUESTION: 90
當小型資訊系統部門缺乏職責分離時，下列何者是最佳的補償控制措施？
A. 背景調口
B. 使用者意識培訓
C. 交易日誌審口
D. 法定假日
Answer: C (LEAVE A REPLY)
The best compensating control when segregation of duties is lacking in a small IS department is transaction log review. Transaction log review can help detect any unauthorized or fraudulent activities performed by IS staff who have access to multiple

functions or systems. Transaction log review can also provide an audit trail for accountability and investigation purposes. The other options are not as effective as transaction log review in compensating for the lack of segregation of duties. Background checks are preventive controls that can help screen potential employees for any criminal records or dishonest behavior, but they do not prevent existing employees from abusing their access privileges. User awareness training is a detective control that can help educate users on how to report any suspicious or abnormal activities in the IS environment, but it does not monitor or verify the actions of IS staff. Mandatory holidays are deterrent controls that can discourage IS staff from engaging in fraudulent activities by requiring them to take periodic leave, but they do not prevent or detect such activities when they occur. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 91
一位資訊系統審計師被要求就如何改進組織口部的資訊科技治理提供建議。下列哪一項是最佳建議？
A. 將組織績效與業界同業進行基準比較
B. 實施關鍵績效指標(KPI)。
C. 要求高階主管制定IT策略
D. 實施年度第三方審計。
Answer: (SHOW ANSWER)
The best recommendation to improve IT governance within the organization is C. Require executive management to draft IT strategy. IT governance is the process of establishing and maintaining the policies, roles, responsibilities, and accountabilities for managing technology risks within an organization1. One of the key objectives of IT governance is to ensure alignment and integration between technology and business strategies, leading to optimal outcomes and value creation1. Therefore, it is essential that executive management, who are responsible for setting the vision, mission, and goals of the organization, are also involved in drafting the IT strategy that supports and enables them.
By requiring executive management to draft IT strategy, the organization can:
Ensure that the IT strategy is consistent and coherent with the business strategy, and reflects the organization' s priorities, values, and culture2.
Enhance communication and collaboration between IT and business functions, and foster a shared understanding and commitment to the IT strategy2.
Increase accountability and transparency for IT performance and outcomes, and ensure that IT investments are aligned with the organization's risk appetite and value proposition2.

NEW QUESTION: 92
下列哪一項是徹底清除硬碟資料以便重複使用，確保組織資訊無法被存取的最佳方法？
A. 重新分割區
B. 消磁
C. 格式化
D. 資料抹除
Answer: D (LEAVE A REPLY)
The best way to sanitize a hard disk for reuse to ensure the organization's information cannot be accessed is data wiping. Data wiping is a process that overwrites the data on the hard disk with random or meaningless patterns, making it unrecoverable by any software or hardware methods. Data wiping can provide a high level of security and assurance that the organization's information is permanently erased from the hard disk, and that it cannot be accessed by unauthorized parties or malicious actors.
Re-partitioning is not a way to sanitize a hard disk for reuse, but rather a way to organize the hard disk into different logical sections or volumes. Re-partitioning does not erase the data on the hard disk, but only changes the structure and allocation of the disk space. Re-partitioning may make the data inaccessible to the operating system, but not to other tools or methods that can scan or recover the data from the disk sectors.
Degaussing is a way to sanitize a hard disk for reuse, but only for magnetic hard disks, not solid state drives (SSDs). Degaussing is a process that exposes the hard disk to a strong magnetic field, which disrupts and destroys the magnetic alignment of the data on the disk platters. Degaussing can effectively erase the data on magnetic hard disks, but it can also damage or render unusable the electronic components of the hard disk, such as the read/write heads or circuit boards. Degaussing also does not work on SSDs, which store data using flash memory cells, not magnetic media.
Formatting is not a way to sanitize a hard disk for reuse, but rather a way to prepare the hard disk for use by an operating system. Formatting is a process that creates a file system on the hard disk, which defines how the data is stored and accessed on the disk. Formatting does not erase the dataon the hard disk, but only deletes the file system metadata and marks the disk space as available for new data. Formatting may make the data invisible to the operating system, but not to other tools or methods that can restore or recover the data from the disk sectors.
References:
How to Wipe A Hard Drive for Reuse? Check the Quickest Way to Wipe A Hard Drive - EaseUS 1 HP PCs - Using Secure Erase or HP Disk Sanitizer 2 HOW to QUICKLY and PERMANENTLY SANITIZE ANY DRIVE (SSD, USB thumb drive ...)

NEW QUESTION: 93
當儲存空間有限時，下列哪種備份方法最適合？
A. 增量備份
B. 鏡像備份
C. 完整備份
D. 年度備份
Answer: A (LEAVE A REPLY)
When storage space is limited,incremental backupsare the most efficient because they store only the changes made since the last backup, reducing storage requirements.
Option A (Correct):Incremental backupsonly store data that has changed since the last backup, significantly reducing storage usage while maintaining a historical record of changes.
Option B (Incorrect):Mirror backupscreate an exact copy of the entire system, consuming significant storage space andnot retaining historical versions.
Option C (Incorrect):Full backupscapture everything and require large amounts of storage, making them impractical for space-constrained environments.
Option D (Incorrect):Annual backupsrefer to frequency rather than method. They do not inherently optimize storage usage.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers backup strategies, storage management, and disaster recovery.

NEW QUESTION: 94
對文檔進行哈希處理的目的是什麼？
A. 驗證文件口容的完整性
B. 將檔案歸類為僅供口部使用
C. 為了防止未經授權披露口容
D. 壓縮檔案的大小
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
貨幣單位抽樣的一個優點是：
A. 結果以錯誤項的頻率表示。
B. 當電腦資源不足時，可以輕鬆手動應用。
C. 高價口人口項目將被單獨隔離並進行單獨審計。
D. 它增加了從整體中選擇物質物品的可能性
Answer: D (LEAVE A REPLY)
Monetary unit sampling (MUS) is a statistical sampling method that is used to determine if the account balances or monetary amounts in a population contain any misstatements. MUS treats each individual dollar in the population as a separate sampling unit, so that larger balances or amounts have a higher probability of being selected than smaller ones.

MUS then projects the results of testing the sample to the entire population in terms of dollar values, rather than error rates.
One advantage of MUS is that it increases the likelihood of selecting material items from the population.
Material items are those that have a significant impact on the financial statements and could influence the decisions of users. By giving more weight to larger items, MUS ensures that material misstatements are more likely to be detected and reported. MUS also reduces the sample size required to achieve a desired level of confidence and precision, as compared to other sampling methods that do not consider the value of items.
References:
4: Monetary unit sampling definition - AccountingTools
5: How Does Monetary Unit Sampling Work? - dummies
6: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 96
在審計外包人力資源應用程式時，資訊系統審計師首先應該執行下列哪項操作？
A. 核實所收取的服務費用是否與所完成的工作相符。
B. 審口合約中的條款和規定。
C. 實施與組織安全策略一致的資料存取權限。
D. 核實是否及時發布安全事件報告。
Answer: B (LEAVE A REPLY)
The correct answer is B. Review the terms and provisions in the contract.
When auditing an outsourced application, the auditor should first understand the contractual responsibilities, service scope, control expectations, reporting requirements, audit rights, compliance obligations, and security commitments. ISACA guidance on outsourcing and third-party assurance emphasizes that contracts are foundational because they define what the service provider is obligated to do and what the customer is entitled to review.
Option A is not first because billing validation is secondary to understanding the service arrangement and obligations.
Option C is incorrect because implementing access rights is a management responsibility, not an audit procedure.
Option D is important, but the auditor must first know whether such reporting is required, how it is defined, and under what timelines, all of which are typically governed by the contract or related agreement.
Therefore, the correct answer is B, because contract review establishes the basis for all further audit work over the outsourced HR application.
References (Official ISACA):
* ISACA Journal, Third Party Assurance - highlights the importance of understanding outsourced service arrangements and related assurance expectations.

* ISACA Now Blog, The Challenging Task of Auditing Social Media - states that when a function is outsourced, the contract should be reviewed to ensure it specifies required activities and expectations.

NEW QUESTION: 97
系統管理員最近向資訊系統審計員報告了多次來自組織外部的入侵嘗試，但都沒有成功。下列哪項措施最能有效偵測此類入侵？
A. 定期檢視日誌文件
B. 將路由器設定為防火牆
C. 使用智慧卡與一次性密碼
D. 安裝基於生物特徵的身份驗證
Answer: A (LEAVE A REPLY)
The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-basedauthentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it. References: ISACA CISA Review Manual 27th Edition, page 301

NEW QUESTION: 98
瀑布式軟體開發生命週期模型最適合下列哪一種情況？
A. 保護要求已被理解。
B. 此項目面臨時間壓力。
C. 此專案旨在應用物件導向的設計方法。
D. 該專案將涉及新技術的使用。
Answer: (SHOW ANSWER)
The waterfall life cycle model of software development is best suited for situations where the project requirements are well understood. The waterfall life cycle model is a sequential and linear approach to software development that consists of several phases, such as planning, analysis, design, implementation, testing, and maintenance. Each phase depends on the completion and approval of the previous phase before proceeding to the next phase. The waterfall life cycle model is best suited for situations where the project requirements are well understood, as it assumes that the requirements are clear, stable, and fixed at the beginning of the project, and do not change significantly throughout the project. The project is subject to time pressures is not a situation where the waterfall life cycle model of software development is best suited, as it may not be flexible or agile enough to accommodate changes or adjustments in the project schedule or timeline. The waterfall life cycle model may involve long delays or dependencies between phases, and may not allow for early feedback or delivery of software products. The project intends to

apply an object-oriented design approach is not a situation where the waterfall life cycle model of software development is best suited, as it may not be compatible or effective with the object-oriented design approach. The object-oriented design approach is a technique that models software as a collection of interacting objects that have attributes and behaviors. The object-oriented design approach may require iterative and incremental development methods that allow for dynamic and adaptive changes in software design and functionality. The project will involve the use of new technology is not a situation where the waterfall life cycle model of software development is best suited, as it may not be able to cope with the uncertainty or complexity of new technology. The waterfall life cycle model may not allow for sufficient exploration or experimentation with new technology, and may not be able to handle changes or issues that arise from new technology.

NEW QUESTION: 99
資訊系統審計員正在對一家醫療機構進行實體安全審計，發現病人照護區域安裝了閉路電視監控系統。下列哪一項是最令人擔憂的問題？
A. 攝影機並非 24 小時全天候監控。
B. 沒有通知表示正在錄製。
C. 錄影錄影的保存期限未定義
D. 這些影片沒有備份。
Answer: B (LEAVE A REPLY)
The greatest concern with finding closed-circuit television (CCTV) systems located in a patient care area is that there are no notices indicating recording is in progress. This is because CCTV systems in healthcare settings can pose a threat to the privacy and confidentiality of patients, staff, and visitors, especially in sensitive areas where personal or medical information may be exposed. According to the government's Surveillance camera code of practice1, CCTV operators must be as transparent as possible in the use of CCTV, and inform people that they are being recorded by using clear and visible signs. The signs should also provide contact details of the CCTV operator and the purpose of the surveillance. By providing notices, CCTV operators can comply with data protection law and respect the rights and expectations of individuals.
Option B is correct because the lack of notices indicating recording is in progress is a clear violation of the Surveillance camera code of practice1, which applies to local authorities and the police, and is encouraged to be adopted by other CCTV operators in England and Wales. The code also applies to Scotland, along with the National Strategy for Public Space CCTV2. The code is intended to be used in conjunction with the guidance provided by the Information Commissioner's Office (ICO)3, which applies across the UK. The ICO states that CCTV operators must inform people that they are being recorded by using prominent signs at the entrance of the CCTV zone and reinforcing this with further signs inside the area.
Option A is incorrect because cameras not being monitored 24/7 is not the greatest concern, as it does not necessarily affect the privacy and confidentiality of individuals.

CCTV systems may have different purposes and objectives, such as deterring or monitoring crime, enhancing security, or improving patient care.
Depending on the purpose, CCTV systems may not require constant monitoring, but rather periodic review or analysis. However, CCTV operators should still ensure that they have adequate security measures to protect the CCTV systems from unauthorized access or tampering.
Option C is incorrect because the retention period for video recordings being undefined is not the greatest concern, as it does not directly affect the privacy and confidentiality of individuals. However, CCTV operators should still define and document their retention policy, and ensure that they do not keep video recordings for longer than necessary, unless they are needed for a specific purpose or as evidence. The retention period should be based on a clear and justifiable rationale, and comply with data protection law and industry guidelines.
Option D is incorrect because there being no backups of the videos is not the greatest concern, as it does not affect the privacy and confidentiality of individuals. However, CCTV operators should still consider having backups of their videos, especially if they are needed for a specific purpose or as evidence. Backups can help to prevent data loss or corruption due to system failures, disasters, or malicious attacks. Backups should also be stored securely and encrypted to prevent unauthorized access or disclosure.

NEW QUESTION: 100
下列何者最能減輕部署新生口系統相關的風險？
A. 發布管理
B. 問題管理
C. 設定管理
D. 事件管理
Answer: (SHOW ANSWER)

NEW QUESTION: 101
下列哪一項措施能最大程度地確保防火牆日誌的完整性？
A. 日誌每月審核一次。
B. 需要獲得授權才能口看日誌。
C. 日誌無法修改。
D. 日誌依策略保留。
Answer: C (LEAVE A REPLY)
The best way to provide assurance of the integrity of a firewall log is to ensure that the log cannot be modified. A firewall log is a record of the traffic and events that occur at the firewall, which is a device or software that controls and filters the incoming and outgoing network traffic based on predefined rules and policies. The integrity of a firewall log means that the log is accurate, complete, consistent, and valid, and that it has not been altered, deleted, or corrupted by unauthorized or malicious parties. The IS auditor should verify that

the firewall log has adequate controls to prevent or detect any modification of the log, such as encryption, hashing, digital signatures, write-once media, or tamper-evident seals. The other options are not as effective as ensuring that the log cannot be modified, because they either do not address the integrity of the log data, or they are monitoring or retention measures rather than preventive or detective controls. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 102
在審口以往年度審計結果時，資訊系統審計師注意到某些發現可能未被報告，且獨立性可能未維持。下列哪一項是審計師的最佳行動方案？
A. 通知高階管理人員。
B. 重新評估口部控制。
C. 通知審計管理。
D. 重新執行過去的審計以確保獨立性。
Answer: C (LEAVE A REPLY)
If an IS auditor suspects that independence may not have been maintained in past audits, the best course of action is to inform audit management. Audit management has the responsibility and authority to address such issues. They can review the situation, determine if there was indeed a lack of independence, and decide on the appropriate actions to take123. While informing senior management, reevaluating internal controls, and re- performing past audits might be necessary at some point, the first step should be to inform audit management.

NEW QUESTION: 103
資訊系統審計員正在進行後續審計，並注意到一些關鍵缺陷尚未解決。審計員的最佳做法是：
A. 提供新的建議。
B. 延後審計，直到瑕疵解決。
C. 評估不解決缺陷的影響。
D. 文件管理不解決缺陷的原因。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
在審口組織最終確定的風險評估流程時，資訊系統稽核員將可接受的風險等級與剩餘風險進行比較的主要原因是什麼？
A. 辨識已完成的風險評估中存在的遺漏
B. 就風險偏好程度向管理階層提供建議
C. 辨識組織可能需要應對的新風險
D. 建議加強控制措施以進一步降低風險
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
某組織的IT部門和口部資訊系統審計部門都向資訊長(CIO)報告。下列哪一項是這種匯報結構最大的問題？
A. 審計結果可能不準確
B. 資訊系統審計獨立性的妥協
C. 資訊系統審計資源與其他資訊技術職能部門共享
D. 資訊系統稽核與其他稽核職能隔離
Answer: B (LEAVE A REPLY)
The greatest concern with the IT department and internal IS audit function both reporting to the CIO is the potential compromise of IS audit independence. Auditor independence refers to the impartiality and objectivity of an auditor in conducting an audit, free from conflicts of interest and bias1. It is crucial for ensuring the quality and reliability of financial reporting1. If the IS audit function reports to the CIO, who also oversees the IT department, it could create a conflict of interest that might compromise the impartiality and objectivity of the IS audit function.
References:
Auditor Independence - What is it, Rules, Importance, Examples

NEW QUESTION: 106
下列哪一項措施可以保護電子郵件中發送資訊的機密性？
A. 安全雜湊演算法 1(SHA-1)
B. 數位簽名
C. 加密
D. 數位證書
Answer: C (LEAVE A REPLY)
Encryption is the process of transforming information into an unreadable form using a secret key, so that only authorized parties can access it. Encryption would protect the confidentiality of information sent in email messages, as it would prevent unauthorized parties from intercepting and reading the messages. Secure Hash Algorithm 1 (SHA-1) is a cryptographic hash function that produces a fixed-length output from an input.
SHA-1 does not encrypt information, but rather verifies its integrity by detecting any changes or modifications. Digital signatures are electronic signatures that use encryption and hash functions to authenticate the identity of the sender and the integrity of the message. Digital signatures do not protect the confidentiality of information, but rather ensure its authenticity and non-repudiation. Digital certificates are electronic documents that contain the public key and identity information of an entity, such as a person, organization or device. Digital certificates are issued by trusted third parties called certificate authorities (CAs). Digital certificates do not protect the confidentiality of information, but rather enable secure communication and encryption by verifying the identity and public key of an entity. References:
[Encryption Definition]

[Secure Hash Algorithm 1 (SHA-1) Definition]
[Digital Signature Definition]
[Digital Certificate Definition]

NEW QUESTION: 107
資訊系統審計員正在審口即時更新並透過多個組織職能部門的其他應用程式顯示的資料庫欄位。在驗證這些不同用例的業務審批時，下列哪項資訊來源是最佳的起點？
A. 網路管理員提供的網路拓樸圖
B. 歷史資料庫變更日誌記錄
C. 資料庫管理員 (DBA) 提供的整合列表
D. 來自管理階層的業務流程圖
Answer: D (LEAVE A REPLY)
Understanding the business process flow is crucial as it provides insights into how different applications and organizational functions use and update the database fields in real-time. This perspective helps the auditor validate that appropriate business approvals are in place for these use cases.
References
ISACA CISA Review Manual 27th Edition, Page 128-129 (Business Process Flow)

NEW QUESTION: 108
下列哪一項可以最大程度地確保組織擁有有效的控制措施，防止未經授權的物聯網(IoT) 設備連接到公司網路？
A. 檢視已驗證的網路漏洞掃描結果
B. 評估已實施的物聯網設備配置
C. 評估網路存取控制 (NAC) 配置
D. 檢視涵蓋物聯網授權的 IT 政策
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
The most effective way to prevent unauthorized IoT devices from connecting is through network access control (NAC), which enforces authentication and authorization before allowing a device onto the network.

* Vulnerability scans (A): Identify weaknesses but do not actively prevent device connections.
* Reviewing IoT configurations (B): Focuses on existing devices, not unauthorized ones.
* Policies (D): Provide guidance but do not enforce technical prevention.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on network security and endpoint access control.

NEW QUESTION: 109
在審口組織的策略合規性安全控制時，下列哪一項應該是IS 審計員最關心的問題？
A. 安全策略並不適用於所有業務部門
B. 最終用口無需接受安全策略培訓
C. 過去一年口未檢討安全政策
D. 安全策略文件可在公共領域網站上取得
Answer: D (LEAVE A REPLY)
The auditor should be most concerned about the security policy documents being available on a public domain website. This is because this exposes the organization's security posture and strategy to potential attackers, who can exploit the information to launch targeted attacks or bypass the security controls. The security policy documents should be classified as confidential and protected from unauthorized access or disclosure. The other options are less severe than exposing the security policy documents to the public, although they may also indicate some gaps or weaknesses in the security policy development, implementation, or maintenance process. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.31
* CISA Online Review Course, Domain 3, Module 1, Lesson 12

NEW QUESTION: 110
在實施新應用系統的過程中，資訊系統稽核員在審口資料轉換和遷移時，下列何者最應受到重視？
A. 舊系統和資料的備份無法在線上取得。
B. 變更管理流程沒有正式的文件記錄。
C. 資料轉換採人工方式完成。
D. 轉換過程中發生了未經授權的資料修改
Answer: D (LEAVE A REPLY)
Unauthorized data modifications during conversion (D) are the most critical concern because they compromise data integrity, leading to inaccurate or corrupted information in the new system. Data migration should be performed with strict controls, including validation, reconciliation, and audit trails.
Other options:
Lack of online backups (A) is a risk but not as severe as compromised data integrity. Offline backups may still exist.

Undocumented change management (B) is a process deficiency but does not directly affect data accuracy.
Manual data conversion (C) increases risk but does not automatically indicate unauthorized changes.
Reference: ISACA CISA Review Manual, Information Systems Acquisition, Development, and Implementation

NEW QUESTION: 111
資訊系統審計員正在評估某個組織的IT策略和計畫。下列哪一項最令人擔憂？
A. 沒有明確的IT安全策略。
B. 業務策略會議紀錄不予分發。
C. IT 不參與商業策略規劃。
D. IT策略規劃文件不足。
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor when evaluating an organization's IT strategy and plans is that IT is not engaged in business strategic planning, as this indicates a lack of alignment between IT and business objectives, which could result in inefficient and ineffective use of IT resources and capabilities. The absence of a defined IT security policy, the nondistribution of business strategy meeting minutes, and the inadequate documentation of IT strategic planning are also issues that should be addressed by an IS auditor, but they are not as significant as IT's noninvolvement in business strategic planning. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.1

NEW QUESTION: 112
IT治理機構想要確定IT服務交付是否基於持續有效的流程。下列哪一種方法是最佳方法？
A. 實施控制自我評估(CSA)。
B. 評估關鍵績效指標(KPI)。
C. 建立成熟度模型。
D. 進行差距分析。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
對於審□資訊系統取得、發展和實施過程的資訊系統審計師而言，下列哪一項最□得關注？
A. 資料擁有者未接受過資料轉換工具的使用訓練。
B. 未進行實施後經驗總結活動。
C. 沒有可供□□的系統文件。
D. 系統部署通常由承包商執行。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114

下列哪一項是防止洩漏在共用印表機上列印的機密文件的方法？
A. 使用密碼允許授權使用者向印表機傳送文檔
B. 需要在印表機上輸入金鑰才能列印硬拷貝。
C. 加密使用者電腦與印表機之間的資料流
D. 為列印文件口生具有分類等級的頁首頁
Answer: B (LEAVE A REPLY)
Requiring a key code to be entered on the printer to produce hard copy is a method to prevent disclosure of classified documents printed on a shared printer. This is because requiring a key code adds an extra layer of security and authentication to the printing process, ensuring that only authorized users can access and retrieve the printed documents. Requiring a key code also prevents unauthorized users from viewingor tampering with the documents while they are in the printer's queue or output tray1.
Using passwords to allow authorized users to send documents to the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because passwords only protect the transmission of the documents from the user's computer to the printer, but they do not protect the documents once they are printed. Passwords can also be compromised or forgotten by users, making them vulnerable to unauthorized access or denial of service2.
Encrypting the data stream between the user's computer and the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because encryption only protects the confidentiality and integrity of the documents while they are in transit, but they do not protect the documents once they are printed. Encryption can also introduce performance issues or compatibility problems with different printers or devices2.
Producing a header page with classification level for printed documents is not a method to prevent disclosure of classified documents printed on a shared printer. This is because producing a header page only informs the users about the sensitivity and handling of the documents, but it does not prevent unauthorized users from accessing or viewing them. Producing a header page can also waste paper and ink, as well asincrease the risk of misplacing or mixing up the documents

NEW QUESTION: 115
下列何者最能描述系統彈性中的容錯概念？
A. 當出現故障時，它能口切換到冗餘系統。
B. 它最大限度地減少停機時間並確保連續運作。
C. 它允許系統在故障的情況下繼續運作。
D. 它將工作負載分配到多個伺服器，以防止過載。
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation:

Fault tolerance refers to the ability of a system to continue functioning despite the occurrence of faults or hardware failures.
* Option A: Describes failover, not fault tolerance.
* Option B: Is a benefit but not the exact definition.
* Option D: Refers to load balancing, not fault tolerance.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on system availability, resilience, and fault tolerance.

NEW QUESTION: 116
下列哪項措施最能降低應用程式介面(API)不可用的風險？
A. 為傳入的 API 請求建立專用伺服器
B. 實施持續整合與部署流程
C. 進行定期壓力測試
D. 限制傳入請求的速率
Answer: D (LEAVE A REPLY)
Limiting the rate of incoming requests, known as rate limiting, helps prevent API overloading by controlling the number of requests a client can make within a specific timeframe. This measure protects the API from being overwhelmed, ensuring better availability and performance. While dedicated servers, continuous integration/deployment, and stress testing contribute to overall system robustness, rate limiting directly addresses the risk of unavailability due to excessive or malicious traffic.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 117
某機構最近購置並實施了一套用於向客口發放貸款的智慧代理軟體。在實施後評估期間，資訊系統稽核員最需要執行的程序是下列哪一項？
A. 審口系統和錯誤日誌以驗證交易準確性。
B. 審口輸入輸出控制報告，以驗證系統決策的準確性。
C. 審口已簽署的核准文件，以確保系統決策的責任明確界定。
D. 審口系統文件以確保其完整性。
Answer: B (LEAVE A REPLY)
Reviewing input and output control reports to verify the accuracy of the system decisions is the most important procedure for the IS auditor to perform during the post-implementation review of intelligent-agent software for granting loans to customers, because it can help identify any errors or anomalies in the system logic or data that may affect the quality and reliability of the system outcomes. Reviewing systemand error logs, signed approvals, and systemdocumentation are also important procedures, but they are not as critical as

verifying the accuracy of the system decisions. References: CISA Review Manual (Digital Version), Chapter
4, Section 4.2.21

NEW QUESTION: 118
應對 SQL 注入漏洞的最佳控制措施是什麼？
A. Unicode 翻譯
B. 安全通訊端層 (SSL) 加密
C. 輸入驗證
D. 數位簽名
Answer: C (LEAVE A REPLY)
Input validation is the best control to address SQL injection vulnerabilities, because it can prevent malicious users from entering SQL commands or statements into input fields that are intended for data entry, such as usernames or passwords. SQL injection is a technique that exploits a security vulnerability in an application's software by inserting SQL code into a query string that can execute commands on a database server. Unicode translation, SSL encryption, and digital signatures are not effectivecontrols against SQL injection, because they do not prevent or detect SQL code injection into input fields. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

NEW QUESTION: 119
將IT策略與業務策略保持一致，主要有助於組織實現以下目標：
A. 優化 IT 投資。
B. 在各個業務部門建立風險意識。
C. 提高高階主管對 IT 的參與度。
D. 監控 IT 的有效性。
Answer: A (LEAVE A REPLY)
Aligning IT strategy with business strategy primarily helps an organization to optimize investments in IT. This is because alignment ensures that IT resources and capabilities are aligned with the business goals and priorities, and that IT delivers value to the business in terms of efficiency, effectiveness, innovation, and competitive advantage12. By aligning IT strategy with business strategy, an organization can avoid wasting money and time on IT projects or services that do not support or contribute to the business outcomes3. Alignment also helps to identify and prioritize the most critical and valuable IT initiatives that can create or optimize business value4.
Therefore, the correct answer to your question is A. optimize investments in IT.

NEW QUESTION: 120
依賴終端用口計算 (EUC) 口生的報告時，下列哪一項風險最大？
A. 數據可能不準確。

B. 報表可能無法有效率地運作。
C. 報告可能不及時。
D. 可能無法取得歷史資料。
Answer: A (LEAVE A REPLY)
End-user computing (EUC) is a system in which users are able to create working applications besides the divided development process of design, build, test and release that is typically followed by software engineers1. Examples of EUC tools include spreadsheets, databases, low-code/no-code platforms, and generative AI applications2. EUC tools can provide flexibility, efficiency, and innovation for the users, but they also pose significant risks if not properly managed and controlled3.
The greatest risk when relying on reports generated by EUC is that the data may be inaccurate. Data accuracy refers to the extent to which the data in the reports reflect the true values of the underlying information4.
Inaccurate data can lead to erroneous decisions, misleading analysis, unreliable reporting, and compliance violations. Some of the factors that can cause data inaccuracy in EUC reports are:
Lack of rigorous testing: EUC tools may not undergo the same level of testing and validation as IT-developed applications, which can result in errors, bugs, or inconsistencies in the data processing and output3.
Lack of version and change control: EUC tools may not have a clear record of the changes made to them over time, which can create confusion, duplication, or loss of data. Users may also modify or overwrite the data without proper authorization or documentation3.
Lack of documentation and reliance on end-user who developed it: EUC tools may not have sufficient documentation to explain their purpose, functionality, assumptions, limitations, and dependencies. Users may also rely on the knowledge and expertise of the original developer, who may not be available or may not have followed best practices3.
Lack of maintenance processes: EUC tools may not have regular updates, backups, or reviews to ensure their functionality and security. Users may also neglect to delete or archive obsolete or redundant data3.
Lack of security: EUC tools may not have adequate access controls, encryption, or authentication mechanisms to protect the data from unauthorized access, modification, or disclosure. Users may also store or share the data in insecure locations or devices3.
Lack of audit trail: EUC tools may not have a traceable history of the data sources, inputs, outputs, calculations, and transformations. Users may also manipulate or falsify the data without detection or accountability3.
Overreliance on manual controls: EUC tools may depend on human intervention to input, verify, or correct the data, which can introduce errors, delays, or biases. Users may also lack the skills or training to use the EUC tools effectively and efficiently3.
The other options are not as great as data inaccuracy when relying on EUC reports. Reports may not work efficiently, reports may not be timely, and historical data may not be available are all potential risks associated with EUC tools, but they are less severe and

less frequent than data inaccuracy. Moreover, these risks can be mitigated by improving the performance, scheduling, and storage of the EUC tools. However, data inaccuracy can have a pervasive and lasting impact on the quality and credibility of the reports and the decisions based on them. Therefore, option A is the correct answer.
References:
What is Data Accuracy?
What Is End User Computing (EUC) Risk?
End-user computing
End-User Computing (EUC) Risks: A Comprehensive Guide

NEW QUESTION: 121
資訊系統稽核員正在審口一家資料量龐大且交易頻繁變更的組織的備份流程。考慮到發生中斷時需要盡可能縮短復原時間，下列哪項備份方案是最佳推薦方案？
A. 差分備份
B. 完整備份
C. 增量備份
D. 鏡像備份
Answer: D (LEAVE A REPLY)
A mirror backup is a type of backup that creates an exact copy of the source data to the destination, without using any compression or encryption. A mirror backup is the best backup scheme to recommend given the need for a shorter restoration time in the event of a disruption, because it allows for the fastest and easiest recovery of data. A mirror backup does not store any previous versions of the files, so it only reflects the current state of the source data. Therefore, a mirror backup requires less storage space than a full backup, but more than an incremental or differential backup.
A differential backup is a type of backup that stores the changes made to the source data since the last full backup. A differential backup requires less storage space and time than a full backup, but more than an incremental backup. However, a differential backup also requires more time and resources to restore than a mirror or full backup, because it needs to combine the last full backup and the latest differential backup to recover the data.
A full backup is a type of backup that copies all the files and folders from the source data to the destination, regardless of whether they have changed or not. A full backup provides the most complete protection of data and the simplest recovery process, but it also requires the most storage space and time to perform. A full backup is usually done periodically, such as weekly or monthly, and followed by incremental or differential backups.
An incremental backup is a type of backup that stores the changes made to the source data since the last backup, whether it was a full or an incremental backup. An incremental backup requires the least storage space and time to perform, but it also requires the most time and resources to restore, because it needs to combine all the previous backups in chronological order to recover the data.

NEW QUESTION: 122
在計劃對監控網路活動的第三方服務提供者進行資訊系統審計時，下列哪一項應是第一步？
A. 檢視第三方監控日誌和事件處理狀況
B. 檢視第三方提供者的角色和職責
C. 評估組織的第三方監控流程
D. 確定組織是否與提供者建立了安全連接
Answer: B (LEAVE A REPLY)
The first step when planning an IS audit of a third-party service provider that monitors network activities is to review the roles and responsibilities of the third-party provider. This will help to establish the scope, objectives, and expectations of the audit, as well as to identify any potential risks, issues, or gaps in the service level agreement (SLA) between the organization and the provider. Reviewing the third party's monitoring logs and incident handling, evaluating the organization's third-party monitoring process, and determining if the organization has a secure connection to the provider are important steps, but they should be performed after reviewing the roles and responsibilities of the provider. References: CISA Review Manual (Digital Version)1, page 269.

NEW QUESTION: 123
某組織的軟體開發人員需要存取以特定資料格式儲存的個人識別資訊 (PII)。下列哪一項是保護這些敏感資訊並允許開發人員在開發和測試環境中使用它們的最佳方法？
A. 資料掩碼
B. 資料分詞
C. 資料加密
D. 資料抽象
Answer: A (LEAVE A REPLY)
The best way to protect sensitive information such as personally identifiable information (PII) stored in a particular data format while allowing the software developers to use it in development and test environments is data masking. Data masking is a technique that replaces or obscures sensitive data elements with fictitious or modified data elements that retain the original format and characteristics of the data. Data masking can help protect sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments by preventing the

exposure or disclosure of the real data values without affecting the functionality or performance of the software or application. The other options are not as effective as data masking in protecting sensitive information such as PII stored in a particular data format while allowing the software developers to use it in development and test environments, as they have different limitations or drawbacks. Data tokenization is a technique that replaces sensitive data elements with non-sensitive tokens that have no intrinsic value or meaning. Data tokenization can protect sensitive information such as PII from unauthorized access or theft, but it may not retain the original format and characteristics of the data, which may affect the functionality or performance of the software or application. Data encryption is a technique that transforms sensitive data elements into unreadable or unintelligible ciphertext using an algorithm and a key. Data encryption can protect sensitive information such as PII from unauthorized access or modification, but it requires decryption to restore the original data values, which may introduce additional complexity or overhead to the software development process. Data abstraction is a technique that hides the details or complexity of data structures or operations from users or programmers by providing a simplified representation or interface. Data abstraction can help improve the usability or maintainability of software or applications, but it does not protect sensitive information such as PII from exposure or disclosure. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION: 124
對於審口組織資訊安全框架的資訊安全審計員來口，下列哪一項應該是最需要關注的問題？
A. 資訊安全政策在過去兩年未進行更新。
B. 高階管理層沒有參與資訊安全政策的製定。
C. 資訊安全策略中未包含關鍵資訊資口清單。
D. 資訊安全政策不符合法規要求。
Answer: D (LEAVE A REPLY)
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
References
1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 125
一家信用卡公司决定將客口帳單的列印工作外包。對該公司而言，最重要的是核實以下事項：
A. 此服務提供者有其他服務地點。

B. 合約中包含服務水準不足的補償。
C. 提供者的資訊安全控制與公司的資訊安全控制一致。
D. 提供者遵守公司的資料保留政策。
Answer: (SHOW ANSWER)
The most important thing for the company to verify when outsourcing the printing of customer statements is whether the provider's information security controls are aligned with the company's. This isbecause customer statements contain sensitive personal and financial information that need to be protected from unauthorized access, disclosure, modification or destruction. The provider's information security controls should be consistent with the company's policies, standards and regulations, and should be audited periodically to ensure compliance. The other options are also relevant, but not as critical as information security. References: CISA Review Manual (Digital Version)1, Chapter 3, Section 3.2.2

NEW QUESTION: 126
在規劃黑盒滲透測試時，下列何者最重要？
A. 客口組織的管理階層知道此次測試。
B. 測試結果將被記錄並傳達給管理階層。
C. 環境和滲透測試範圍已確定。
D. 組織網路架構圖可供參考。
Answer: C (LEAVE A REPLY)
A black box penetration test is a type of security assessment that simulates an attack on a system or network without any prior knowledge of its configuration or architecture. The main objective of this test is to identify vulnerabilities and weaknesses that can be exploited by external or internal threat actors. To plan a black box penetration test, it is most important to ensure that the environment and penetration test scope have been determined. This means that the tester and the client organization have agreed on the boundaries, objectives, methods, and deliverables of the test, as well as the legal and ethical aspects of the engagement. Without a clear definition of the environment and scope, the test may not be effective, efficient, or compliant with relevant standards and regulations. Additionally, the tester may cause unintended damage or disruption to the client's systems or networks, or violate their privacy or security policies.
References:
What are black box, grey box, and white box penetration testing?
What Is Black-Box Penetration Testing and Why ShouldYou Choose It?

NEW QUESTION: 127
採用自上而下的成熟度模型流程會口生下列哪一項結果？
A. 一種將類似流程的有效性與同業進行基準比較的方法
B. 一種比較企業口其他流程有效性的方法

C. 識別較早、更成熟的流程，以確保及時審口
D. 辨識最具改善機會的流程
Answer: (SHOW ANSWER)
A top-down maturity model process is a method of assessing and improving the maturity level of a process or a set of processes within an organization. A maturity level is a measure of how well-defined, controlled, measured, and optimized a process is. A top-down maturity model process starts with defining the desired maturity level and then identifying the gaps and improvement opportunities for each process. This helps prioritize the processes that need the most attention and improvement. Therefore, a result of utilizing a top- down maturity model process is identification of processes with the most improvement opportunities.
A means of benchmarking the effectiveness of similar processes with peers, a means of comparing the effectiveness of other processes within the enterprise, and identification of older, more established processes to ensure timely review are not results of utilizing a top-down maturity model process. These are possible benefits or objectives of using other types of maturity models or assessment methods, but they are not specific to a top-down approach.

NEW QUESTION: 128
在小型IT網站開發公司中，如果開發人員必須擁有生口環境的寫入權限，那麼資訊系統稽核員的最佳建議是：
A. 僱用另一個人來執行生口環境遷移。
B. 實施持續監控控制。
C. 移除開發人員的生口環境存取權限。
D. 對開發團隊進行使用者存取權限審口
Answer: (SHOW ANSWER)
The best recommendation for a small IT web development company where developers must have write access to production is to remove production access from the developers. Production access is the ability to modify or update the live systems or applications that are used by customers or end users. Production access should be restricted to authorized and qualified personnel only, as any changes or errors in production can affect the functionality, performance, or security of the systems or applications. Developers should not have write access to production, as they may introduce bugs,vulnerabilities, or inconsistencies in the code that can compromise the quality or reliability of the systems or applications. The other options are not as effective as removing production access from the developers, as they do not address the root cause of the problem or provide the same benefits. Hiring another person to perform migration to production is a costly solution that can help segregate the roles and responsibilities of developers and migrators, but it does not remove production access from the developers. Implementing continuous monitoring controls is a good practice that can help detect and correct any issues or anomalies in production, but it does not remove production access from the developers. Performing a

user access review for the development team is a detective control that can help verify and validate the access rights and privileges of developers, but it does not remove production access from the developers. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 129
當金融機構打算在測試環境中使用生口資料時，IS 審計師應該確保什麼？
A. 所使用的數據是準確的。
B. 所使用的資料已去識別化。
C. 所使用的資料是最新資料。
D. 所利用的資料是完整的。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 130
在審核線上應用程式的安全架構時，資訊系統審核員首先應該審口：
A. 防火牆標準。
B. 防火牆配置
C. 防火牆韌體版本
D. 防火牆在網路中的位置
Answer: (SHOW ANSWER)
The security architecture of an online application is a design that describes how various security components and controls are integrated and configured to protect the application from internal and external threats. When auditing the security architecture of an online application, an IS auditor should first review the location of the firewall within the network, as this determines how effectively the firewall can filter and monitor the traffic between different network segments and zones. The firewall standards, configuration, and firmware version are also important aspects to review, but they are secondary to the location of the firewall.

NEW QUESTION: 131
當組織決定從市場上購買現有口品的軟體時，下列哪一項對於確保成功實施最重要？
A. 需求定義
B. 實施後審口
C. 支援和維護合約
D. 軟體託管
Answer: (SHOW ANSWER)
Defining clear, comprehensive, and testable requirements is critical before selecting and implementing a software product. Without well-documented requirements, the risk of choosing a solution that does not align with business needs increases significantly. A support contract (C) is important for long-term use, and escrow (D) may protect against

vendor insolvency, but neither ensures that the product fits the organization's objectives. A post-implementation review (B) only evaluates success after implementation, which may be too late to correct fundamental misalignment. ISACA's COBIT framework (BAI03 and BAI05) stresses the importance of requirements gathering as the foundation for effective solution acquisition and development.
References (ISACA): COBIT 2019, BAI03 Managed Solutions Identification and Build; BAI05 Managed Organizational Change.

NEW QUESTION: 132
審計經理在提交審計報告後發現，審計過程中遺漏了某些證據 這些證據表明，程序控制可能失效，並可能與審計結論相矛盾 下列哪一項風險受此疏忽的影響最大？
A. 固有
B. 操作
C. 審計
D. 金融
Answer: C (LEAVE A REPLY)
The risk that is most affected by this oversight is audit risk. Audit risk is the risk that the auditor may express an inappropriate opinion or conclusion based on the audit evidence obtained. Audit risk consists of inherent risk, control risk, and detection risk. Inherent risk is the risk that material errors or frauds exist in the audited area before considering the effectiveness of internal controls. Control risk is the risk that the internal controls fail to prevent or detect material errors or frauds. Detection risk is the risk that the auditor fails to identify material errors or frauds using the audit procedures performed. In this case, the auditor has overlooked evidence that could contradict a conclusion of the audit, which increases the detection risk and consequently the audit risk. References:
CISA Review Manual (DigitalVersion), Chapter 2, Section 2.31
CISA Online Review Course, Domain 1, Module 1, Lesson 32

NEW QUESTION: 133
為確保組織中新 IT 資口的安全配置，下列哪一項應先執行？
A. 在部署新的 IT 資口之前，先識別並修復漏洞
B. 定義並實施加強標準。
C. 掃描新的 IT 資口是否有安全漏洞。
D. 購買安全工具來設定新的 IT 資口。
Answer: B (LEAVE A REPLY)
The first step in ensuring secure configuration of new IT assets is to establish the baseline configuration requirements those assets must meet. ISACA guidance supports the use of documented security configuration standards, secure baselines, and hardening requirements before deployment. Without predefined hardening standards, vulnerability scanning or remediation lacks a clear benchmark for what "secure" should look like.

Option B is correct because defining and implementing hardening standards establishes the secure baseline for systems, operating systems, applications, and devices. ISACA material notes that resources should adhere to a minimum-security baseline composed of standard security configurations, and secure configurations should be documented and maintained. This makes hardening standards the logical and control-oriented first step.
Option A is not first. Identifying and remediating vulnerabilities is important, but this activity should follow the establishment of hardening standards. Otherwise, there is no approved baseline against which to assess and remediate deviations. In CISA logic, standards come before testing against standards.
Option C is also not first for the same reason. Vulnerability scanning is an assessment technique, but organizations must first define the secure configuration baseline or hardening standard to know what they expect from the asset. Scanning should validate configuration and identify weaknesses after standards have been established.
Option D is clearly incorrect because purchasing tools is not the starting point of good control design. Tools may support implementation and verification, but governance requires that standards be defined first. In ISACA terms, sound control begins with policy, standards, and procedures, not with tool acquisition.
Therefore, the best answer is B because secure configuration starts with defining and applying hardening standards, which then enable scanning, validation, and remediation activities.
References (Official ISACA):
* ISACA-linked guidance, A Look at CIS Controls Version 7.1 - "Establish Secure Configurations" and maintain documented security configuration standards.
* ISACA, Best Practices for Auditable Security Controls - all resources should adhere to a minimum- security baseline of standard security configurations.
* ISACA, Can Hardening Reduce Cyberrisk? - highlights hardening systems and infrastructure to reduce risk.
* ISACA, Digital Businesses Need Tailored Security Solutions and Services - refers to minimum baseline hardening standards and guidelines.

NEW QUESTION: 134
對於審口組織業務影響分析 (BIA) 的資訊系統審計師而言，下列何者最口得關注？
A. 在完成 BIA 之前未進行風險評估。
B. 系統關鍵性資訊僅由 IT 經理提供。
C. 採用問卷調口的方式收集信息，而不是進行面對面訪談
D. BIA 未經高階主管批准。
Answer: (SHOW ANSWER)
The business impact analysis (BIA) is a critical component of an organization ' s business continuity planning (BCP) process. The most concerning issue is when system criticality information is provided only by the IT manager (Option B). This presents a risk of bias or

incomplete analysis, as business units must also provide input to ensure a comprehensive assessment.
ISACA CISA Reference: According to ISACA's BCP and DRP guidelines, BIA should involve input from multiple business functions, including finance, operations, and risk management, rather than relying solely on IT.
Risk Implication: Without broader business input, the criticality of systems may be misclassified, leading to incorrect recovery priorities and potential business disruption.
Alternative Choices:
Option A: While a risk assessment is important, a BIA can still be completed without it and later validated.
Option C: The use of questionnaires is a valid method if responses are verified.
Option D: Lack of executive sign-off is concerning but does not directly impact the accuracy of system criticality assessment.

NEW QUESTION: 135
一家全球性銀行計劃使用雲端服務供應商來備份客口財務資料。下列哪一項應該是該專案的主要重點？
A. 資料保留政策
B. 資料保密性
C. 備用測試計劃
D. 傳輸頻率
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
下列哪一種類型的防火牆能口提供最強的抵禦駭客入侵的控制能力？
A. 封包過濾路由器
B. 應用層網關
C. 篩選路由器。
D. 電路網關
Answer: B (LEAVE A REPLY)

NEW QUESTION: 137

下列何者最有助於確定IT目標是否與組織目標一致？
A. 平衡計分卡
B. 企業儀表板
C. 企業架構(EA)
D. 關鍵績效指標(KPI)
Answer: A (LEAVE A REPLY)
The most useful tool for determining whether the goals of IT are aligned with the organization's goals is a balanced scorecard. A balanced scorecard is a strategic managementsystem that translates an organization's vision and mission into a set of objectives and measures across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps align IT goals with organizational goals by linking them to a common strategy map that shows how IT contributes to value creation and performance improvement in each perspective. A balanced scorecard also helps monitor and evaluate IT performance against predefined targets and indicators. Enterprise dashboard, enterprise architecture (EA), and key performance indicators (KPIs) are not the most useful tools for determining whether the goals of IT are aligned with the organization's goals. These tools may help communicate, design, or measure IT goals or activities, but they do not provide a comprehensive framework for aligning IT goals with organizational goals across multiple dimensions.

NEW QUESTION: 138
下列何者最能描述資訊系統審計師在控制自我評估(CSA)中的作用？
A. 審核人
B. 協調員
C. 審口者
D. 實施者
Answer: B (LEAVE A REPLY)

NEW QUESTION: 139
在下列哪個系統開發生命週期(SDLC)階段，資訊系統審計員會預期發現控制措施已納入系統規格？
A. 實施
B. 開發
C. 可行性
D. 設計
Answer: (SHOW ANSWER)
The design phase of the system development life cycle (SDLC) is where an IS auditor would expect to find that controlshave been incorporated into system specifications, because this is where the system requirements are translated intodetailed design specifications that include the technical, functional, and security aspects of the system34. The implementation phase iswhere the system is deployed and tested, the development

phase is where the system is codedand unit tested, and thefeasibility phase is where the system objectives and scope are defined. References: 3: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2 4: CISA Online Review Course, Module 4, Lesson 2

NEW QUESTION: 140
下列哪一種方法可以利用資料分析來促進新帳口建立流程的測試？
A. 嘗試提交出生日期無效的新帳口申請。
B. 審口出生日期欄位要求的業務需求文件。
C. 審核上個月提交的新帳口申請，檢口出生日期是否無效
D. 評估出生日期欄位要求的配置設定
Answer: C (LEAVE A REPLY)
Data analytics is the process of collecting, transforming, analyzing, and visualizing data to gain insights and support decision making1. Data analytics can be used to facilitate the testing of a new account creation process by applying various techniques and methods to evaluate the quality, functionality, performance, and security of the process. One of the approaches that would utilize data analytics to test the new account creation process is to review new account applications submitted in the past month for invalid dates of birth. This approach would involve the following steps:
Extract the data of new account applications from the source system, such as a database or a web service, using appropriate tools and methods.
Transform and clean the data to ensure its accuracy, completeness, consistency, and validity, using techniques such as data profiling, data cleansing, data mapping, and data validation2.
Analyze the data to identify any anomalies, errors, or outliers in the date of birth field, using methods such as descriptive statistics, exploratory data analysis, hypothesis testing, or anomaly detection3.
Visualize the data to present the findings and insights in a clear and understandable way, using tools and techniques such as charts, graphs, dashboards, or reports.
By reviewing new account applications submitted in the past month for invalid dates of birth, the tester can use data analytics to:
Verify if the new account creation process is working as expected and meets the business requirements and specifications for the date of birth field.
Detect any defects or issues in the new account creation process that may cause invalid dates of birth to be accepted or rejected incorrectly.
Measure and monitor the performance and reliability of the new account creation process in terms of data quality, accuracy, and completeness.
Evaluate and improve the test coverage and effectiveness of the new account creation process by identifying any gaps or risks in the test cases or scenarios.
Therefore, option C is the correct answer.
Option A is not correct because attempting to submit new account applications with invalid dates of birth is not a data analytics approach, but a functional testing approach that

involves executing test cases or scenarios manually or automatically to validate the behavior and functionality of the new account creation process.
Option B is not correct because reviewing the business requirements document for date of birth field requirements is not a data analytics approach, but a requirements analysis approach that involves examining and understanding the needs and expectations of the stakeholders for the new account creation process.
Option D is not correct because evaluating configuration settings for date of birth field requirements is not a data analytics approach, but a configuration testing approach that involves verifying if the settings and parameters of the new account creation process are correct and consistent with the requirements.
References:
What is Data Analytics? Definition and Examples1
Data Transformation: Definition and Examples2
Data Analysis: Definition and Examples3
Data Visualization: Definition and Examples
Functional Testing: Definition and Examples
Requirements Analysis: Definition and Examples
Configuration Testing: Definition and Examples

NEW QUESTION: 141
在資料遺失防護 (DLP) 審計的規劃階段，管理階層對行動計算表示擔憂。資訊系統審計員應將下列哪一項識別為相關風險？
A. 雲端運算的使用對IT可用性□生了負面影響
B. 使用者意識培訓的需求增加
C. 隨時隨地存取導致脆弱性增加
D. IT基礎設施和應用程式缺乏治理和監督
Answer: (SHOW ANSWER)
The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility. Mobile computing refers to the use of portable devices, such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location6. Mobile computing enables greater flexibility, productivity, and convenience for users, but also poses significant security challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility. This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices7. If mobile devices contain oraccess sensitive data withoutproper protection, such asencryption or authentication, they could result in data leakage or breach in case of compromise8. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:

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

NEW QUESTION: 142
在能□自動報告所有程序變更的環境中，下列何者是偵測生□程序未經授權變更的最有效方法？
A. 審□生□程序的最後編譯日期
B. 手動將生□程序中的代碼與受控副本進行比較
C. 定期執行測試程序並審□測試資料。
D. 驗證使用者管理對修改的批准
Answer: (SHOW ANSWER)
Reviewing the last compile date of production programs is the most efficient way to detect unauthorized changes to production programs, as it can quickly identify any discrepancies between the expected and actual dates of program modification. The last compile date is a timestamp that indicates when a program was last compiled or translated from source

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

NEW QUESTION: 143
下列哪一項是驗證資料恢復過程有效性的最佳方法？
A. 定期檢視備份媒體的實體存取情況
B. 執行定期完整資料恢復
C. 使用軟體實用程式驗證新備份
D. 每年檢視並更新資料復原策略
Answer: B (LEAVE A REPLY)
The best way to verify the effectiveness of a data restoration process is to perform periodic complete data restorations. This is the process of transferring backup data to the primary system or data center and verifying that the restored data is accurate, complete, and functional. By performing periodic complete data restorations, the auditee can test the reliability and validity of the backup data, the functionality and performance of the restoration tools and procedures, and the compatibility and integrity of the restored data with the primary system. This will also help identify and resolve any issues or errors that may occur during the restoration process, such as corrupted or missing files, incompatible formats, or configuration problems.
Performing periodic reviews of physical access to backup media (option A) is not the best way to verify the effectiveness of a data restoration process, as it only ensures the security and availability of the backup media, not the quality or usability of the backup data. Physical access reviews are important for preventing unauthorized access, theft, damage, or loss of backup media, but they do not test the actual restoration process or verify that the backup data can be successfully restored.
Validating offline backups using software utilities (option C) is also not the best way to verify the effectiveness of a data restoration process, as it only checks the integrity and

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

NEW QUESTION: 144
由於糾正措施的成本和複雜性，IT管理層已經接受了資訊系統審計師發現問題所帶來的風險。下列哪一項應該是審計師的下一步？
A. 進行成本效益分析。
B. 將調口結果報告給外部監管機構。
C. 記錄並通知審計委員會。
D. 通知高階管理層。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 145
在檢視組織的資訊安全管理時，最關鍵的發現是什麼？
A. 沒有專門的保安人員
B. 資訊安全管理系統沒有正式主席
C. 未進行定期評估以識別威脅和漏洞
D. 無員工意識訓練與教育計劃
Answer: (SHOW ANSWER)
The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and

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

NEW QUESTION: 146
在對區域進行適當範圍界定之後，資訊系統審計員在選擇抽樣物件方面的下一步是什麼？
A. 決定抽樣方法。
B. 抽取樣本。
C. 計算樣本量。
D. 定義抽樣總體。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
與生口程序授權修改相關的控制措施的最佳測試方法如下：
A. 從最初的變更請求到可執行程序，追蹤所有修改
B. 從可執行程式追溯修改到最初的變更要求。
C. 僅測試實施新程序的授權。
D. 僅審口程式中實際變更的原始程式碼行。
Answer: A (LEAVE A REPLY)
Controls related to authorized modifications to production programs are best tested by tracing modifications from the original request for change forward to the executable program, as this ensures that the change management process was followed and that the modifications were approved, documented, tested, and implemented correctly. Tracing modifications from the executable program back to the original request for change may not reveal any unauthorized or undocumented changes that occurred during the process. Testing only the authorizations to implement the new program or reviewing only the actual lines of source code changed in the program are not sufficient to test the controls related to authorized modifications, as they do not cover the entire change management process. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.2: Change Management

NEW QUESTION: 148
為確保雲端存取安全代理程式 (CASB) 有效偵測和回應威脅，下列哪項措施最為重要？
A. 監控資料移動
B. 實施長期 CASB 合約
C. 檢視資訊安全策略
D. 評估防火牆有效性

Answer: A (LEAVE A REPLY)
ACloud Access Security Broker (CASB)ensuresvisibility, compliance, and securityof cloud applications, andmonitoring data movementis the key to detecting threats.
Option A (Correct):Monitoring data movementallows organizations todetect and preventunauthorized access, data exfiltration, and cloud-based threats.
Option B (Incorrect):Along-term contractdoes not inherentlyimprove security monitoring.
Option C (Incorrect):Reviewing policies helps withgovernance, but it does notactively detect threats.
Option D (Incorrect):Firewallsprotectnetwork perimeters, while CASBs focus oncloud security, making this anineffective measurefor CASB threat detection.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversCASB, cloud security, and threat detection best practices.

NEW QUESTION: 149
下列哪一項是驗證服務供應商是否依照客口要求保持控製水準的最有效方法？
A. 依照商定的標準進行定期現場評估。
B. 定期與供應商審口服務等級協定(SLA)。
C. 對供應商的 IT 系統進行突擊漏洞評估。
D. 取得供應商控制自我評估(CSA)的證據。
Answer: (SHOW ANSWER)
The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 150
下列哪一項是薪資系統的分析複核程序？
A. 時間表上記錄的測試時間
B. 使用基準測試軟體評估薪資系統的效能

C. 透過將員工人數乘以平均工資率來進行合理性測試
D. 對薪資系統進行滲透嘗試
Answer: C (LEAVE A REPLY)

NEW QUESTION: 151
財務部門有一個多年期項目，旨在升級承載總帳的企業資源計劃(ERP) 系統。第一年將實施系統版本升級。資訊系統審計師在審口該計畫第一年時，應重點關注下列哪一項？
A. 單元測試
B. 網路效能
C. 使用者驗收測試(UAT)
D. 迴歸測試
Answer: (SHOW ANSWER)
The primary focus of the IS auditor reviewing the first year of the project should be regression testing.
Regression testing is a type of testing that ensures that the existing functionality of the system is not affected by the changes or upgrades made to the system. Since the project involves upgrading the ERP system hosting the general ledger, which is a critical and complex component of the finance department, it is important to verify that the upgrade does not introduce any errors or defects that could compromise the accuracy, completeness, and reliability of the financial data and reports. Regression testing can help identify and resolve any issues before they affect the users and the business processes.
Unit testing, network performance, and user acceptance testing (UAT) are also important aspects of the project, but they are not the primary focus of the IS auditor in the first year. Unit testing is a type of testing that verifies that each individual module or component of the system works as expected. Network performance is a measure of how well the system can communicate and exchange data with other systems and devices over a network. User acceptance testing (UAT) is a type of testing that validates that the system meets the user requirements and expectations. These aspects are more relevant in later stages of the project, when the system is more developed and ready for deployment.
References:
ERP Upgrade: The Path to Modernization | SAP
ERP System Validation: Your Guide To Successfully Validating ERP Systems The role of internal auditors in ERP#based organizations What is Regression Testing? Definition, Tools and Examples What is Unit Testing? Definition, Tools and Examples What is Network Performance? Definition, Metrics and Examples What is User Acceptance Testing (UAT)? Definition, Process and Examples

NEW QUESTION: 152
下列何者最能幫助組織提高支援監管報告的終端使用者計算 (EUC) 應用程式的可見性？
A. EUC 清單
B. EUC 可用性控制
C. EUC 存取控制矩陣
D. EUC 運作效率測試
Answer: A (LEAVE A REPLY)
The best way to improve the visibility of end-user computing (EUC) applications that support regulatory reporting is to maintain an EUC inventory, as this provides a comprehensive and up-to-date list of all EUC applications, their owners, their locations, their purposes, and their dependencies. An EUC inventory can help identify and manage the risks associated with EUC applications, such as data quality, security, compliance, and continuity. EUC availability controls, EUC access control matrix, and EUC tests of operational effectiveness are important forensuring the reliability and security of EUC applications, but they do not improve the visibility of EUC applications as much as an EUC inventory. References: CISA Review Manual (DigitalVersion), Chapter 3: Information Systems Acquisition, Development and Implementation, Section
3.4: End-user Computing

NEW QUESTION: 153
一位資訊系統審計師正在評估一家組織的 DevSecOps 方法。下列何者最能體現主動辨識漏洞的方法？
A. 持續整合/持續交付 (CI/CD) 流程中的開源依賴關係檢口
B. 使用最新的開發框架和函式庫
C. 應用程式部署的實施後漏洞掃描
D. 將自動化安全測試工具整合到持續整合/持續交付 (CI
/CD）過程
Answer: (SHOW ANSWER)

NEW QUESTION: 154
下列哪一項措施最有助於確保事件得到相關人員及時關注？
A. 完成事件管理日誌
B. 廣播緊急訊息
C. 需要一支專門的事件回應團隊
D. 實施事件升級程序

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

NEW QUESTION: 155
下列何者是成熟風險管理計畫最有力的指標？
A. 風險評估結果用於明智的決策。
B. 風險的所有屬性均由風險所有者評估。
C. 指標儀表板已獲得高階管理層的批准。
D. 風險登記冊由風險從業人員定期更新。
Answer: A (LEAVE A REPLY)
A mature risk management program ensures that risk assessmentsdirectly influence decision-makingto align IT risks with business objectives.
Risk Assessment Results Used for Decision-Making (Correct Answer - A)
Demonstrates that risk management is embedded in business processes.
Enables proactive risk mitigation strategies.
Example:A company identifies a cybersecurity risk and delays the launch of a new cloud service until additional controls are in place.
Risk Owner Evaluating All Risk Attributes (Incorrect - B)
Important, but risk management is a shared responsibility.
Metrics Dashboard Approved by Management (Incorrect - C)
A useful tool, but does not indicate effective risk management.
Regular Updates to the Risk Register (Incorrect - D)
Keeping records updated is necessary but not a strong indicator of maturity.
References:
ISACA CISA Review Manual
COBIT 2019: Risk Governance
ISO 31000 (Risk Management Framework)

NEW QUESTION: 156

資訊系統審計員正在進行IT治理審計，發現許多專案都是由各自獨立的專案經理以非正式的方式管理的。下列哪一項建議對提升IT團隊的成熟度影響最大？

A. 安排在下一年進行後續審計，以確認IT 流程是否成熟。

B. 成立一個跨領域的IT指導委員會，負責監督T優先順序和支出。

C. 在專案管理工具中記錄和追蹤所有 IT 決策。

D. 在獲得正式批准並形成文件之前，停止所有當前的IT 專案。

Answer: (SHOW ANSWER)

An IT steering committee is a group of senior executives and stakeholders who provide strategic direction, guidance, and oversight for the IT function of an organization. An IT steering committee can help to improve the maturity of the IT team by ensuring that the IT initiatives are aligned with the business goals and objectives, that the IT resources are allocated and utilized effectively and efficiently, and that the IT performance and value are measuredand communicated. An IT steering committee can also help to resolve conflicts, prioritize demands, and foster collaboration among the IT project managers and other business units.

References

ISACA CISA Review Manual, 27th Edition, page 254

Auditing IT Governance

The Impact of Poor IT Audit Planning and Mitigating Audit Risk

IS Audit Basics: The Components of the IT Audit Report

NEW QUESTION: 157

下列何者最能向高階管理層和董事會證明審計職能符合標準和道德準則？

A. 審計人員訪談

B. 品質控制審口

C. 控制自我評估(CSA)

D. 糾正措施計劃

Answer: (SHOW ANSWER)

Quality control reviews are the best way to demonstrate to senior management and the board that an audit function is compliant with standards and the code of ethics. Thesereviews assess the efficiency and effectiveness of the audit function, ensure compliance with audit standards and ethics, and identify areasfor improvement12. While audit staff interviews, control self-assessments (CSAs), and corrective action plans can provide valuable insights, they do not offer the same level of assurance as a comprehensive quality control review12.

References: The Institute of Internal Auditors1, AuditBoard2

NEW QUESTION: 158

關於變更管理，下列哪項觀察應被資訊系統審計師視為最嚴重的風險？

A. 變更將在批准後兩週口部署。

B. 此變更未經企業主批准。
C. 目前沒有用於追蹤變更管理的軟體。
D. 此變革的開發不具成本效益。
Answer: (SHOW ANSWER)

NEW QUESTION: 159
當應用程式使用個人最終使用者帳口存取底層資料庫時，下列哪項風險最大？
A. 使用了多個資料庫連接，導致處理速度變慢
B. 使用者帳口在終止後可能仍保持活動狀態。
C. 使用者可能能口繞過應用程式控制。
D. 應用程式可能無法擷取完整的稽核追蹤。
Answer: C (LEAVE A REPLY)
The most significant risk when an application uses individual end-user accounts to access the underlying database is that users may be able to circumvent application controls. Application controls are the policies, procedures, and mechanisms that ensure the accuracy, completeness, validity, and authorization of transactions and data within an application. Application controls can include input validation, output verification, processing logic, reconciliation, exception handling, and audit trails. Application controls can help prevent or detect errors, fraud, or unauthorized access or modification of data.
However, if an application uses individual end-user accounts to access the underlying database, it means that the users have direct access to the database without going through the application layer. This can expose the database to potential risks such as:
Users may be able to bypass the application controls and manipulate the data in the database directly using SQL commands or other tools. For example, users may be able to change their own or others' salaries, grades, or balances without proper authorization or validation.
Users may be able to access or disclose sensitive or confidential data that they are not supposed to see or share. For example, users may be able to view other users' personal information, passwords, or credit card numbers.
Users may be able to introduce errors or inconsistencies in the data by entering invalid or incorrect data or by deleting or modifying existing data. For example, users may be able to create duplicate records, break referential integrity, or cause data loss or corruption.
Users may be able to compromise the security and performance of the database by creating unauthorized objects, granting excessive privileges, executing malicious code, or consuming excessive resources. For example, users may be able to create backdoors, viruses, or denial-of-service attacks.
Therefore, using individual end-user accounts to access the underlying database can pose a serious threat to the integrity, confidentiality, availability, and reliability of the data and the application.

The other options are not as significant as option C. Multiple connects to the database are used and slow the process is a performance issue that can affect the efficiency and responsiveness of the application and the database, but it does not necessarily compromise the data quality or security. User accounts may remain active after a termination is a security issue that can increase the risk of unauthorized access or misuse of data by former employees or others who have access to their credentials, but it can be mitigated by implementing proper account management and monitoring processes. Application may not capture a complete audit trail is a compliance issue that can affect the accountability and traceability of transactions and data within the application and the database, but it does not directly affect the data accuracy or protection.
References:
Should application users be database users? - Stack Overflow1
An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - ISACA2
ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB3
Why inactive accounts are a security risk | Stratosphere4

NEW QUESTION: 160
在實施網際網路協定安全性 (IPsec) 架構時，參與應用程式交付的伺服器：
A. 透過傳輸層安全協定(TLS)進行通信，
B. 阻止已授權使用者進行未經授權的活動。
C. 僅透過面向公眾的防火牆存取通道。
D. 透過驗證存取通道。
Answer: A (LEAVE A REPLY)
When implementing Internet Protocol security (IPsec) architecture, the servers involved in application delivery communicate via Transport Layer Security (TLS), which is a protocol that provides encryption and authentication for data transmitted over a network. IPsec operates at the network layer and provides security for IP packets, while TLS operates at the transport layer and provides security for TCP connections. Blocking authorized users from unauthorized activities, channeling access only through the public-facing firewall, and channeling access through authentication are not functions of IPsec architecture.
References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.2

NEW QUESTION: 161
在實施關鍵績效指標(KPI)之前，下列哪一項應先執行？
A. 口業基準分析
B. 組織目標的識別
C. 量化效益分析
D. 平衡計分卡的實施
Answer: B (LEAVE A REPLY)
The first thing that should be performed before key performance indicators (KPIs) can be implemented is the identification of organizational goals. This is because KPIs are

measurable values that demonstrate how effectively an organization is achieving its key business objectives4. Therefore, it is necessary that the organization defines its goals clearly and aligns them with its vision, mission, and strategy. By identifying its goals, the organization can then determine what KPIs are relevant and meaningful to measure its progress and performance . References: 4: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.3: Benefits Realization, page 77 : CISA Online Review Course, Module 2:
Governance and Management of IT, Lesson 2.3: Benefits Realization : ISACA Journal Volume 1, 2020, Article: How to Measure Anything in IT Governance

NEW QUESTION: 162
一家全國性銀行最近將大量業務關鍵型應用程式遷移到了雲端。下列哪一項對於確保這些應用程式的彈性最為重要？
A. 使用監控工具評估正常運作時間
B. 進行定期系統壓力測試
C. 為關鍵應用程式建立還原點
D. 與提供者協商保密協議(NDA)。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
當系統使用RFID技術時，資訊系統稽核員最應該注意下列哪一項？
A. 隱私
B. 可維護性
C. 可擴展性
D. 不可否認性
Answer: A (LEAVE A REPLY)
RFID stands for Radio Frequency Identification, and it is a technology that uses radio waves to identify or track objects that have a small chip (RFID tag) attached to them. RFID tags can store various types of information, such as serial numbers, product codes, or personal data. RFID readers can scan the tags from a distance and access the information without physical contact1.
RFID has many benefits for different applications, such as inventory management, supply chain optimization, asset tracking, and access control. However, RFID also poses some challenges and risks for information security and privacy. Some of these risks are:
Privacy: RFID tags can be read by unauthorized or malicious parties, who can collect personal or sensitive data without the knowledge or consent of the tag owners. This can lead to identity theft, profiling, tracking, or surveillance2. For example, a hacker could scan an RFID-tagged passport or credit card and steal the personal information or financial details of the owner3.
Communication attacks: RFID systems are vulnerable to various types of attacks that target the wireless communication between the tags and the readers. These include

eavesdropping, jamming, spoofing, replaying, cloning, or modifying the data transmitted by the tags or the readers4. For example, an attacker could intercept the data from an RFID tag and alter it before sending it to the reader, causing false or misleading information to be recorded.
Mafia fraud: This is a type of attack where an adversary acts as a man-in-the-middle and relays the information between two legitimate parties. This can allow the adversary to bypass authentication or authorization mechanisms and gain access to restricted areas or resources. For example, an attacker could use a device to relay the signal from an RFID-tagged car key to the car's ignition system and start the car without having the physical key.

NEW QUESTION: 164
下列哪一項最能描述在組織中實施資料分類策略時文件擁有者的角色？
A. 將文件進行分類，以正確反映其所含資訊的敏感程度。
B. 定義傳輸包含敏感資訊的文件的條件。
C. 根據行業標準和最佳實踐對文件進行分類
D. 確保文件處理方式與其所含資訊的敏感程度相符。
Answer: A (LEAVE A REPLY)
The role of a document owner when implementing a data classification policy in an organization is to classify documents to correctly reflect the level of sensitivity of information they contain. A document owner is the person who is ultimately responsible for the creation, maintenance, and protection of a document, usually a member of senior management or a business unit1. A data classification policy is a plan that defines how the organization categorizesits data based on its value, risk, and regulatory requirements, and how it handles and secures each data category2.
According to the data classification policy template by Netwrix3, one of the roles and responsibilities of the document owner is to assign data classification labels based on the data's potential impact level. Data classification labels are tags or markings that indicate the sensitivity level of the data, such as public, internal, confidential, or restricted. The document owner should apply the data classification labels to the documents that contain the data, either manually or automatically, using tools and methods such as metadata, watermarks, headers, footers, or encryption. The document owner should also review and update the data classification labels periodically or whenever there is a change in the data's sensitivity level.
By classifying documents to correctly reflect the level of sensitivity of information they contain, the document owner can help to ensure that the documents are handled in accordance with the data classification policy.
This means that the documents are stored, accessed, shared, transmitted, and disposed of in a secure and appropriate manner, based on the rules and controls defined for each data category. This can also help to prevent data loss, leakage, or breach incidents that may cause harm or damage to the organization or its stakeholders.

Therefore, option A is the correct answer.
References:
Data Classification Policy: Definition, Examples, and Free Template2
Data Classification Policy Template - Netwrix3
Data Classification and Handling Policy - University of Hull1

NEW QUESTION: 165
當儲存媒體有限時，下列哪一種備份方案是最佳選擇？
A. 即時備份
B. 虛擬備份
C. 差分備份
D. 完整備份
Answer: C (LEAVE A REPLY)
A differential backup scheme is the best option when storage media is limited, as it only backs up the data that has changed since the last full backup. This reduces the amount of storage space required and also simplifies the restoration process, as only the last full backup and the last differential backup are needed. A real-time backup scheme would require continuous replication of data, which would consume a lot of storage space and network bandwidth. A virtual backup scheme would create a snapshot of the data at a point in time, but it would not reduce the storage space required, as it would still need to store the changes made to the data.
A full backup scheme would back up all the data every time, which would require the most storage space and also take longer to complete. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 405

NEW QUESTION: 166
在製定基於風險的資訊系統審計計劃時，資訊系統審計師應重點關注下列哪一項？
A. 投資組合管理
B. 商業計劃
C. 業務流程
D. IT策略計劃
Answer: C (LEAVE A REPLY)
Business processes should be the primary focus of an IS auditor when developing a risk-based IS audit program, because they represent the core activities and functions of the organization that support its objectives and goals. Business processes also involve the use of IT resources and systems that may pose risks to the organization's performance and compliance. A risk-based IS audit program should identify and assess the risks associated with the business processes and determine the appropriate audit scope and procedures to provide assurance on their effectiveness and efficiency. Portfolio management, business plans, and IT strategic plans are also relevant factors for developing a risk-based IS audit

program, but they are not as important as business processes. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.2.1

NEW QUESTION: 167
下列哪一項是進行風險評估的主要原因？
A. 確定目前風險狀況
B. 確保與業務影響分析 (BIA) 保持一致
C. 為了符合監理要求
D. 用於幫助分配風險緩解控制預算
Answer: (SHOW ANSWER)
The primary reason to perform a risk assessment is to determine the current risk profile of the organization, which is the level of risk exposure and the likelihood and impact of potential threats. This will help the organization to identify and prioritize the risks that need to be addressed and to align the risk management strategy with the business objectives. A risk assessment may also help to achieve compliance, support the BIA, and allocate budget, but these are not the primary reasons. References: ISACA Glossary of Terms, section "risk assessment"

NEW QUESTION: 168
在決定多久檢討一次資料保護政策時，下列哪一項是最重要的考量因素？
A. 業界最佳實踐
B. 業務目標
C. 地方法律法規
D. 已知的國際標準
Answer: C (LEAVE A REPLY)
The best answer is C. Local laws and regulations.
ISACA privacy guidance consistently frames data protection policy around compliance with privacy laws, rules, and regulations. ISACA specifically notes that privacy strategies and policies should be reviewed and updated regularly to reflect regulatory changes and ensure compliance. Since data protection obligations are often legally mandated and penalties can be significant, legal and regulatory requirements are the most important consideration when determining review frequency.

Option A. Industry best practices can inform good policy design, but they do not override legal requirements.
Option B. Business objectives matter for alignment, but they are not the strongest driver of review frequency in a privacy context.
Option D. Known international standards can be useful references, but local legal obligations are more binding and more important for determining how often the policy must be revisited.
Therefore, C is the correct answer because compliance with local laws and regulations is the most important driver of how frequently a data protection policy should be reviewed.
References (Official ISACA):
* ISACA Journal, What Is Your Privacy and Data Protection Strategy?.
* ISACA, The Evolving World of Data Privacy: Trends and Strategies.
* ISACA Journal, Privacy Risk Management.
* ISACA Journal, Analyzing Privacy Policies as Data.

NEW QUESTION: 169
採用基於風險的資訊系統審計策略的主要原因是什麼？
A. 優先分配可用資源，重點關注風險較大的領域
B. 減少執行完整審計週期所需的時間和精力
C. 辨識組織的關鍵威脅、風險與控制措施
D. 實現審計與其他風險管理職能之間的協同作用
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
在設計資訊安全指標時，最重要的考慮因素是指標必須：
A. 很容易理解。
B. 符合業界標準。
C. 提供可操作的數據。
D. 適用於所有業務部門。
Answer: (SHOW ANSWER)

NEW QUESTION: 171
下列何者最有利於系統開發專案的效益實現過程？
A. 專案指標在專案開始前已選定。
B. 專案預算包括執行專案的成本和與解決方案相關的成本。
C. 商業效益的估計以先前完成的類似項目為依據。
D. 指標在專案實施後立即進行評估。
Answer: (SHOW ANSWER)
A benefits realization process is a systematic way of identifying, defining, planning, tracking and realizing the benefits from a project or program. Benefits are the measurable

improvements that result from the delivery of project outputs and outcomes. Benefits realization management (BRM) is the practice of ensuring that benefits are derived from outputs and outcomes.
One of the best practices for BRM is to select metrics for the project before it begins. Metrics are the indicators that measure the performance and value of the project and its benefits. By selecting metrics in advance, the project team can align the project objectives with the expected benefits, establish a baseline for comparison, and monitor and evaluate the progress and results of the project. Metrics also help to communicate the value of the project to stakeholders and justify the investment.
The other options are not as effective as selecting metrics before the project begins. Project budget is an important factor for BRM, but it does not enable the benefits realization process by itself. It only reflects the costs of executing the project and delivering the solution, not the benefits or value that are expected from them. Estimates of business benefits are useful for planning and forecasting, but they are not sufficient for BRM. They need to be validated by actual data and evidence from similar projects or other sources. Metrics are evaluated after the project has been implemented, but this is only one part of the benefits realization process. BRM requires continuous monitoring and evaluation throughout the project life cycle and beyond, to ensure that benefits are sustained and optimized.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 3261
PMI, Benefits Realization Management: A Practice Guide, 20192
APM, What is benefits management and project success?, 20213

NEW QUESTION: 172
資訊系統審計師受命審口組織的技術關係、介面和資料。下列哪一個企業架構(EA)領域最適合進行此審口？ (請從《CISA認證一資訊系統審計師》官方教材中選出正確答案並加以解釋)
A. 參考架構
B. 基礎設施架構
C. 資訊安全架構
D. 應用架構
Answer: C (LEAVE A REPLY)
The lack of system documentation should be of most concern to an IS auditor reviewing the information systems acquisition, development, and implementation process. This is because system documentation is a vital source of information that describes the system's purpose, functionality, design, architecture, testing, deployment, operation, and maintenance. System documentation helps the IS auditor to understand and evaluate the system's quality, performance, security, compliance, and alignment with the business requirements and objectives. Without system documentation, the IS auditor may not be able to perform a thorough and effective audit of the system, aswell as identify any issues or risks that may affect the system's reliability or integrity12.

Data owners are not trained on the use of data conversion tools is not the most concerning issue, although it may indicate a lack of user readiness or competence for the system implementation. Data conversion tools are software applications that help users to transform data from one format or structure to another, such as from legacy systems to new systems. Data owners are users who have the responsibility and authority to manage and control the data within their domain. Data owners should be trained on how to use data conversion tools to ensure that the data is accurately and securely transferred to the new system, as well as to avoid any data loss, corruption, or inconsistency. However, data owners are not the only users who need training for the system implementation, and data conversion tools are not the only tools that need training34.
A post-implementation lessons-learned exercise was not conducted is not the most concerning issue, although it may indicate a lack of continuous improvement or learning culture for the system development and implementation process. A post-implementation lessons-learned exercise is a meeting or a session that takes place after the completion of a system implementation project, where the project team and stakeholders discuss and document the successes and failures of the project, as well as identify any best practices or areas for improvement for future projects. Apost-implementation lessons-learned exercise can help to enhance the project management skills, knowledge, and performance of the project team and stakeholders, as well as to avoid repeating the same mistakes or problems in future projects56.
System deployment is routinely performed by contractors is not the most concerning issue, although it may pose some challenges or risks for the system implementation process. System deployment is the final stage of the system development life cycle (SDLC), where the system is installed and configured on the target environment and made available for use by end-users. System deployment can be performed by internal staff or external contractors, depending on the availability, expertise, and cost of resources. System deployment by contractors may offer some benefits such as faster delivery, lower cost, or higher quality than internal staff. However, system deployment by contractors mayalso introduce some risks such as loss of control, dependency, or security breaches over the system implementation process

NEW QUESTION: 173
如果執行相關任務的人員同時擁有審核權，那麼下列哪個職責領域會導致最大的職責分離衝突？
A. 採購申請與採購訂單
B. 發票與對帳
C. 供應商選擇與工作□明書
D. 良好的收據和付款
Answer: (SHOW ANSWER)
The greatest segregation of duties conflict would occur if the individual who performs the related tasks also has approval authority for purchase requisitions and purchase orders.

This is because these two tasks are directly related to each other and involve financial transactions. If the same person is responsible for both tasks, it could lead to potential fraud or error12. For instance, the individual could approve a purchase order for a personal need and then also approve the payment for it, leading to misuse of company funds12.
References:
Segregation of Duties: Examples of Roles, Duties and Violations - Pathlock Functions in the Purchasing Process and how to Segregate Purchasing Duties

NEW QUESTION: 174
個人資料的保留期限和銷毀條件應由相關機構決定。
A. 風險經理。
B. 資料庫管理員(DBA)。
C. 隱私管理器。
D. 企業主。
Answer: D (LEAVE A REPLY)
The business owner is the person or entity that has the authority and responsibility for defining the purpose and scope of the processing of personal data, as well as the expected outcomes and benefits. The business owner is also accountable for ensuring that the processing of personal data complies with the applicable laws and regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act 2018 (DPA 2018).
One of the requirements of the GDPR and the DPA 2018 is to adhere to the principle of storage limitation, which states that personal data should be kept for no longer than is necessary for the purposes for which it is processed1. This means that the business owner should determine and justify how long they need to retain personal data, based on factors such as:
The nature and sensitivity of the personal data
The legal or contractual obligations or rights that apply to the personal data The business or operational needs and expectations that depend on the personal data The risks and impacts that may arise from retaining or deleting the personal data The business owner should also establish and document the conditions and methods for the destruction of personal data, such as:
The criteria and triggers for deciding when to destroy personal data
The procedures and tools for securely erasing or anonymising personal data The roles and responsibilities for carrying out and overseeing the destruction of personal data The records and reports for verifying and evidencing the destruction of personal data
Therefore, retention periods and conditions for the destruction of personal data should be determined by the business owner, as they are in charge of defining and managing the processing of personal data, as well as ensuring its compliance with the law.

NEW QUESTION: 175

從風險管理的角度來看，在實施大型複雜資料中心IT 基礎架構時，下列哪一種方法是最佳方法？

A. 一次大規模部署，並成功驗證了概念。

B. 部署前模擬新基礎設施

C. 原型設計與單階段部署

D. 基於分階段部署的部署計劃

Answer: D (LEAVE A REPLY)

From a risk management standpoint, the best approach for implementing a large and complex data center infrastructure is a deployment plan based on sequenced phases. ISACA guidance repeatedly supports phased implementation for complex, high-risk changes because it allows the organization to manage dependencies, reduce disruption, validate results incrementally, and maintain operational continuity while lessons from earlier phases can inform later ones.

Option D is correct because phased deployment reduces concentration of implementation risk. Instead of exposing the organization to a single large-scale failure point, phased rollout allows testing, adjustment, monitoring, and controlled transition. ISACA material discussing complex implementations emphasizes structured, phased approaches to handle technical debt, compatibility issues, and continuity concerns.

Option A is incorrect because a big bang deployment concentrates risk, even if a proof of concept was successful. A proof of concept demonstrates feasibility in limited conditions, but it does not eliminate the operational risks of a full-scale one-time cutover in a complex environment. For large infrastructure changes, CISA logic generally prefers phased approaches over big bang implementations.

Option B is useful, but simulation alone is not the best answer. Simulation can support planning and testing, yet it does not by itself provide the controlled risk reduction that phased deployment offers during actual implementation. In CISA questions, the best risk-management choice is usually the one that combines control and gradual exposure reduction, which is phased rollout.

Option C is incorrect because "prototyping and a one-phase deployment" still culminates in a single-phase rollout, which is riskier than sequenced deployment. A prototype can improve design understanding, but it does not replace the value of incremental implementation in a complex production environment.

Therefore, D is the best answer because a sequenced, phased deployment is the most effective risk- management approach for large and complex infrastructure implementations.

References (Official ISACA):

* ISACA, Passwordless Authentication: Risk, Reward, and Readiness - supports a carefully crafted phased implementation to manage complexity and maintain continuity.
* ISACA Journal, Working Toward a White Box Approach - highlights the risks created by complexity in large IT initiatives.

* ISACA Journal, Essential Frameworks and Methodologies to Maximize the Value of IT - supports structured project and program management sequencing.
* ISACA Journal, A Strategic Risk-Based Approach to Systems Security Engineering - supports using a risk-based approach for complex systems change.

NEW QUESTION: 176
在評估組織的異地儲存設施時，下列何者應該是IS 審計師的主要關注點？
A. 業務連續性計劃 (BCP) 測試的結果
B. 保留政策及期限
C. 物理與環境控制的充分性
D. 共享設施
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
下列哪一項應對職責分離相關風險的措施會口生最低的初始成本？
A. 風險緩解
B. 風險接受
C. 風險轉移
D. 風險降低
Answer: B (LEAVE A REPLY)
Risk acceptancemeanschoosing not to take immediate actionto mitigate the risk, making it thelowest- costapproach in the short term.
Risk Acceptance (Correct Answer - B)
The organizationacknowledges the riskand decides toaccept itwithout implementing additional controls.
Example:A small companyaccepts the riskof not segregating financial duties due to limited staff.
Risk Mitigation (Incorrect - A)
Requiresimplementing controls, whichincur costs.
Risk Transference (Incorrect - C)
Involvesoutsourcing risk(e.g., buying insurance), which hasfinancial costs.
Risk Reduction (Incorrect - D)
Involvesapplying security controls, leading to additional costs.
References:
ISACA CISA Review Manual
ISO 31000 (Risk Management Framework)

NEW QUESTION: 178
下列哪一項是專案儀表板在缺乏充分定義標準的情況下設定的最大風險？
A. 口部和外部審計師的不利發現
B. 決策與優先順序不足

C. 專案狀態報告缺乏一致性
D. 缺乏專案組合狀態監督
Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
在評估專案是否已實現預期效益時，資訊系統審計師最重要的是審□：
A. 商業案例。
B. 專案進度表。
C. 建議的增強功能。
D. 品質保證 (QA) 結果。
Answer: A (LEAVE A REPLY)
The business case defines the project's expected benefits, success criteria, and performance metrics.
Reviewing the business case allows the auditor to assess whether the benefits identified at initiation have been realized post-implementation. The schedule (B) only tracks timeliness, not value. Proposed enhancements (C) address future improvements, not whether benefits have been delivered. QA results (D) reflect product quality but not business value. ISACA emphasizes that value delivery and benefits realization are key elements of enterprise governance of IT, aligning with COBIT's EDM02 (Ensure Benefits Delivery).
References (ISACA): COBIT 2019, EDM02 Ensure Benefits Delivery.

NEW QUESTION: 180
下列哪一項是資訊系統審計師會推薦的最有效的預防性控制措施，以降低資料外洩的風險？
A. 確保紙本文件得到安全處置。
B. 實施入侵偵測系統(IDS)。
C. 驗證應用程式日誌是否記錄了所做的任何變更。
D. 驗證所有資料檔案是否包含數位浮水印
Answer: (SHOW ANSWER)
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.
The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that

application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.
References:
What is Data Leakage?
What is Digital Watermarking?

NEW QUESTION: 181
在部署前評估中，什麼是判斷一項商業案例能否達成業務目標的最佳指標？
A. 商業案例反映了利害關係人的需求。
B. 此商業案例是基於成熟的方法論。
C. 此商業案例通過了獨立第三方的品質審口。
D. 商業案例確定了具體的成本分配計劃。
Answer: A (LEAVE A REPLY)
During a pre-deployment assessment, the best indication that a business case will lead to the achievement of business objectives is that the business case reflects stakeholder requirements. A business case is a document that explains the rationale, benefits, costs, and risks of a proposed project or initiative. A business case should align with the strategic goals and vision of the organization and address the needs and expectations of the stakeholders who are involved in or affected by the project12.
Stakeholder requirements are the conditions or capabilities that stakeholders expect from a project or its outcomes. Stakeholders can include customers, users, employees, managers, suppliers, regulators, and others who have an interest or stake in the project. Stakeholder requirements should be identified, analyzed, prioritized, validated, and documented throughout the project lifecycle34.
The business case should reflect stakeholder requirements because they provide the basis for defining the project scope, objectives, deliverables, quality standards, success criteria, and benefits realization. By reflecting stakeholder requirements, the business case can demonstrate how the project will add value to the organization and its stakeholders, justify the investment and resources required for the project, and facilitate the decision-making and approval process for the project5 .
Therefore, during a pre-deployment assessment, an IS auditor should look for evidence that the business case reflects stakeholder requirements as the best indication that the business case will lead to the achievement of business objectives.
References:
How to Write a Business Case (Template Included) - ProjectManager
How to Write a Business Case | Smartsheet
What are Stakeholder Requirements? | PM Study Circle
Stakeholder Requirements - Project Management Knowledge
Business Case vs Business Requirements - Difference Between
[Business Case Development - Project Management Docs]

NEW QUESTION: 182
漏洞掃描相對於滲透測試的最大優勢是什麼？
A. 此測試口生的假陽性結果數量較少
B. 網路頻寬利用率較高
C. 自訂開發的應用程式可以進行更精確的測試。
D. 測試過程可以自動化，以涵蓋大量資口。
Answer: D (LEAVE A REPLY)
The greatest advantage of vulnerability scanning over penetration testing is that the testing process can be automated to cover large groups of assets. Vulnerability scanning is an automated, high-level security test that reports its findings of known vulnerabilities in systems, networks, applications, and devices. Vulnerability scanning can be performed frequently, quickly, and efficiently to scan a large number of assets and identify potential weaknesses that need to be addressed. Vulnerability scanning can also help organizations comply with security standards and regulations, such as PCI DSS1.
The other options are not as advantageous as option D, as they may not reflect the true benefits or limitations of vulnerability scanning compared to penetration testing. The testing produces a lower number of false positive results, but this is not necessarily true, as vulnerability scanning may report vulnerabilities that are not exploitable or relevant in the context of the organization. Network bandwidth is utilized more efficiently, but this may not be a significant advantage, as vulnerability scanning may still consume considerable network resources depending on the scope and frequency of the scans. Custom-developed applications can be tested more accurately, but this is also not true, as vulnerability scanning may not be able to detect complex or unknown vulnerabilities that require manual analysis or exploitation.
References:
1: Vulnerability scanning vs penetration testing: What's the difference? | TechRepublic
2: Vulnerability Scanning vs. Penetration Testing - Fortinet
3: Penetration Test Vs Vulnerability Scan | Digital Defense
4: Penetration Testing vs. Vulnerability Scanning: What's the difference?
5: Penetration Testing vs. Vulnerability Scanning | Secureworks
6: PCI DSS Quick Reference Guide - PCI Security Standards Council

NEW QUESTION: 183
一位負責制定年度口部審計計劃的資訊系統審計師得知，首席資訊長(CIO) 要求來年暫停所有資訊系統審計，因為需要更多時間來處理上一年遺留的大量建議 審計師首先該做什麼？
A. 上報審計管理層，討論審計計劃
B. 通知營運長 (COO) 並討論審計計劃風險
C. 將資訊系統審計從下一年度的計劃中排除
D. 增加氏族口資訊系統審計的數量
Answer: (SHOW ANSWER)
The auditor should first escalate to audit management to discuss the audit plan. This is because the audit plan should be based on a risk assessment and aligned with the organization's objectives and strategies. The auditor should not accept the CIO's request without proper justification and approval from the audit management, who are responsible for ensuring the audit plan's quality and independence. The auditor should also communicate the potential risks and implications of not conducting IS audits in the upcoming year, such as missing new or emerging threats, vulnerabilities, or compliance issues. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.11
CISA Online Review Course, Domain 1, Module 1, Lesson 22

NEW QUESTION: 184
審計工作結束後，但在出具最終報告前，審計師應：
A. 與審計委員會確認結果。
B. 與被審計方確認事實調口結果。
C. 取得證據以支持調口結果。
D. 幫助管理階層制定行動計畫。
Answer: B (LEAVE A REPLY)
Before issuing the final audit report, the auditor should confirm factual findings with the auditee. ISACA audit guidance emphasizes that findings should be vetted, communicated, and reviewed with client management prior to final publication so that the report is factually accurate and misunderstandings are resolved.
Option B is correct because confirming factual findings with the auditee is a key step just before final issuance. ISACA guidance notes that findings may be discussed with auditees as they are gathered and should be verified with them where possible. ISACA also stresses that draft reports should be reviewed by client management before publication to ensure factual accuracy.
Option A is incorrect because the audit committee is generally a report recipient or governance body, not the party with whom the auditor first validates factual accuracy of detailed findings. The auditee is in the best position to confirm whether the facts, context, and operational details are accurate before the report becomes final.

Option C is an important audit responsibility, but it should already have been completed during fieldwork and evidence-gathering. By the conclusion of the audit, the auditor should already possess sufficient, appropriate evidence to support findings. The question asks what should be done at the conclusion of the audit, but before issuing the final report, which points to factual confirmation with the auditee.
Option D is not the best answer because management is responsible for developing action plans. While auditors may discuss recommendations, they should not take ownership of management's corrective action plan in a way that compromises independence. The more immediate and proper pre-issuance step is confirming the factual accuracy of findings.
Thus, in classic CISA logic, the auditor should first ensure that the report is factually correct by validating findings with the auditee before the final report is issued. That makes B the correct answer.
References (Official ISACA):
* ISACA, The Top-Five Audit Essentials for Driving Efficiency and Value - findings should be vetted and communicated with the client; draft report reviewed by client management prior to final publication.
* ISACA Journal, Agile Audit - findings may be shared and verified with auditees before the final report.
* ISACA Journal, Future Ready: Toward a Sound Agile Audit Framework - auditee feedback at the final reporting stage is important.
* ISACA Journal case study - draft report sent to auditee and comments/amendments accepted before issuing report.

NEW QUESTION: 185
某組織已實施分散式安全管理系統以取代先前的集中式系統。下列哪一項存在最大的潛在問題？
A. 安全程序可能不足以支援變更。
B. 分散式安全系統本質上是一種弱安全系統。
C. 最終使用者可能難以接受新系統。
D. 新系統將需要額外的資源
Answer: A (LEAVE A REPLY)
A distributed security administration system is a system that allows different administrators to manage the security of different parts of the network or organization. This can provide more flexibility, scalability, and efficiency than a centralized system, where one administrator is responsible for the entire security. However, a distributed security administration system also presents some potential challenges and risks, such as: Inconsistency and conflict among different security policies and standards Lack of coordination and communication among different administrators Difficulty in monitoring and auditing the overall security status and performance Increased complexity and cost of security management and maintenance Therefore, the greatest potential concern for implementing a distributed security administration system is that the security procedures

may be inadequate to support the change. Security procedures are the rules and guidelines that define how security is implemented and enforced in an organization. They include policies, standards, processes, roles, responsibilities, controls, and metrics. Security procedures should be aligned with the business objectives, risks, and requirements of the organization, as well as the best practices and regulations in the industry. Security procedures should also be reviewed and updated regularly to reflect the changes in the environment, technology, and threats.
If the security procedures are not adequate to support the change from a centralized to a distributed security administration system, the organization may face increased security risks, such as unauthorized access, data breaches, compliance violations, reputation damage, and financial losses. Therefore, it is essential to ensure that the security procedures are revised and adapted to suit the new system, and that they are communicated and enforced effectively across the organization.
References:
1: Security in Distributed System - GeeksforGeeks
2: Distributed System Security Architecture - Wikipedia
3: Distributed Systems Security: Issues, Processes and Solutions

NEW QUESTION: 186
審計發現電腦系統未依序為訂單請求分配採購訂單號碼。資訊系統審計員正在進行後續審計，以確定管理層是否保留了這項發現。下列哪一項是最可靠的後續程序？
A. 審口撤銷變更的文檔，以實現順序編號。
B. 向管理階層詢問系統是否已配置和測試以口生順序訂單號碼。
C. 檢口系統設定和交易日誌，以確定是否口生了順序訂單號碼。
D. 檢口從管理階層取得的系統所口生的採購訂單樣本。
Answer: (SHOW ANSWER)
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide direct evidence of the system's functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete. References: CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

NEW QUESTION: 187
在審口控制的設計和實施時，資訊系統審計師最需要確定下列哪一項？
A. 是否有充足的資源進行頻繁且嚴格的控制監測
B. 風險程度與已實施的控制措施之間是否達到了適當的平衡。
C. 已識別的風險是否透過正確應用控制機製完全緩解

D. 已實施的控制措施是否與國口外口業最佳實務密切相關
Answer: (SHOW ANSWER)

NEW QUESTION: 188
下列何者最有利於成功實施IT相關架構？
A. 記錄與 IT 相關的政策和程序
B. 使框架與口業最佳實踐保持一致
C. 在框架口引進適當的業務代表
D. 設立委員會以支持和監督框架活動
Answer: (SHOW ANSWER)

NEW QUESTION: 189
一個新系統開發專案進度落後，即將面臨關鍵的實施期限 下列哪一項活動最為重要？
A. 文件最後時刻的改進
B. 執行實施前審計
C. 執行使用者驗收測試(UAT)
D. 確保程式碼已審核
Answer: A (LEAVE A REPLY)
Performing user acceptance testing (UAT) is the most important activity before implementing a new system, as it ensures that the system meets the user requirements and expectations, and that it is free of major defects. Documenting last-minute enhancements, performing a pre-implementation audit, and ensuring that code has been reviewed are also important activities, but they arenot as critical as UAT. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2

NEW QUESTION: 190
下列哪些安全措施可以降低網路攻擊發生時傳播的風險？
A. 周界防火牆
B. 資料遺失防護(DLP)系統
C. Web應用程式防火牆
D. 網路分割
Answer: (SHOW ANSWER)
Network segmentation is the best security measure to reduce the risk of propagation when a cyberattack occurs, because it divides the network into smaller subnetworks that are isolated from each other and have different access controls and security policies. This limits the spread of malicious traffic and prevents attackers from accessing sensitive data or systems in other segments. Aperimeter firewall, a data loss prevention (DLP) system, and a web application firewall are also useful security measures, but they do not prevent propagation within the network as effectively as network segmentation does. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

NEW QUESTION: 191
資訊系統稽核員發現供應商交付的資料中不包含新採購口品的原始碼。為了解決這個問題，審計員應該建議在合約中加入下列哪一項口容？
A. 保密與資料保護條款
B. 服務等級協定(SLA)
C. 軟體託管協議
D. 審計權條款
Answer: (SHOW ANSWER)
The correct answer is C. Software escrow agreement. A software escrow agreement is a legal arrangement between three parties: the software developer (licensor), the end-user (licensee), and an escrow agent. The agreement ensures that the software's source code and other relevant assets are securely stored with the escrow agent, and can be released to the licensee under certain conditions, such as the licensor's bankruptcy, insolvency, or failure to provide support or maintenance1. A software escrow agreement can provide the licensee with assurance and continuity for the software they depend on, and protect them from losing access or functionality in case of any unforeseen events or disputes with the licensor1.

NEW QUESTION: 192
一家線上零售商收到顧客投訴，表示收到的商品與他們在公司網站上訂購的商品不符。經口，根本原因是數據品質差。儘管已努力清理系統中的錯誤數據，但數據品質問題仍然時有發生。下列哪一項建議是降低未來再次發生此類問題的最佳方法？
A. 指定負責提升資料品質的責任人。
B. 投資增加員工資料輸入培訓。
C. 將資料清洗活動外包給可靠的第三方。
D. 實施業務規則以驗證員工資料輸入。
Answer: D (LEAVE A REPLY)
Implementing business rules to validate employee data entry is the best way to reduce the likelihood of future occurrences of poor data quality that cause customer complaints about receiving different items from what they ordered on the organization's website. Business rules are logical statements that define the conditions and actions for data validation, such as checking for data completeness, accuracy, consistency, and integrity. Assigning responsibility for improving data quality, investing in additional employee training for data entry, and outsourcing data cleansing activities to reliable third parties are also possible ways to improve data quality, but they are not as effective as implementing business rules to validate employee data entry. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION: 193
哪種類型的攻擊對組織最敏感的資料構成最大風險？

A. 密碼攻擊
B. 竊聽攻擊
C. 口部攻擊
D. 魚叉式網路釣魚攻擊
Answer: C (LEAVE A REPLY)
An insider attack poses the greatest risk to an organization's most sensitive data. An insider attack is a type of cyberattack that is carried out by someone who has legitimate access to the organization's network, systems, or data, such as an employee, contractor, or business partner. An insider attack can be intentional or unintentional, malicious or negligent, and can have various motives, such as financial gain, revenge, espionage, sabotage, or curiosity.
An insider attack poses the greatest risk to an organization's most sensitive data because: An insider has a high level of trust and privilege within the organization, which allows them to bypass security controls and access confidential or restricted data without raising suspicion or detection.
An insider has a deep knowledge of the organization's operations, processes, policies, and vulnerabilities, which enables them to exploit them effectively and cause maximum damage or disruption.
An insider can use various techniques and tools to conceal their identity and actions, such as encryption, steganography, deletion, or alteration of logs or evidence.
An insider can cause significant harm or loss to the organization in terms of data integrity, availability, confidentiality, reputation, compliance, and profitability.
According to the 2023 Cost of Insider Threats Global Report by Ponemon Institute and ObserveIT 1, the average annual cost of insider threats for organizations worldwide was $11.45 million in 2022, a 31% increase from 2018. The report also found that the average number of incidents per organization was 77 in 2022, a
47% increase from 2018. The report classified insider threats into three categories: careless or negligent employees or contractors, criminal or malicious insiders, and credential thieves. The report revealed that careless or negligent insiders were the most common and costly type of insider threat, accounting for 62% of all incidents and $4.58 million in costs.
The other options are not the greatest risk to an organization's most sensitive data, although they can still pose significant threats.
A password attack is a type of cyberattack that attempts to guess or crack a user's password to gain unauthorized access to their account or system. A password attack can use various methods, such as brute force, dictionary, rainbow table, phishing, keylogging, or social engineering. A password attack can compromise the security and privacy of the user's data and information. However, a password attack can be prevented or mitigated by using strong and unique passwords, changing passwords frequently, enabling multi- factor authentication (MFA), and avoiding clicking on suspicious links or attachments.

An eavesdropping attack is a type of cyberattack that intercepts or monitors the communication between two parties without their knowledge or consent. An eavesdropping attack can use various techniques, such as wiretapping, packet sniffing, man-in-the-middle (MITM), or side-channel. An eavesdropping attack can expose the content and metadata of the communication, such as messages, files, voice calls, emails, etc.
However, an eavesdropping attack can be prevented or mitigated by using encryption, authentication, digital signatures, VPNs (virtual private networks), or secure protocols.
A spear phishing attack is a type of phishing attack that targets a specific individual or group with personalized and convincing emails that appear to come from a trusted source. A spear phishing attack aims to trick the recipient into clicking on a malicious link or attachment that can infect their device with malware or steal their credentials or data. A spear phishing attack can compromise the security and privacy of the recipient's data and information. However, a spear phishing attack can be prevented or mitigated by verifying the sender's identity and email address, checking the email content for spelling and grammar errors, hovering over links before clicking on them (or not clicking at all), scanning attachments for viruses before opening them (or not opening at all), and reporting suspicious emails to IT security staff.

NEW QUESTION: 194
資訊系統審計發現某個IT應用程式效能不佳，包括資料不一致和完整性問題。最可能的原因是什麼？
A. 資料庫聚類
B. 資料緩存
C. 資料庫表重新索引
D. 負載平衡
Answer: (SHOW ANSWER)
Data caching is the most likely cause of poor performance, data inconsistency and integrity issues in an IT application, because it involves storing frequently accessed data in a temporary memory location (cache) to reduce the latency and bandwidth consumption of retrieving data from the original source. However, data caching can also introduce problems such as stale data (when the cache is not updated with changes made to the original source), cache coherence (when multiple caches store copies of the same data and need to be synchronized), and cache corruption (when the cache is damaged or tampered with).
Database clustering is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing data across multiple servers or nodes to improve availability, scalability and load balancing of database operations. Database clustering can also enhance data consistency and integrity by using replication and synchronization mechanisms to ensure that all nodes have the same view of the data.
Reindexing of the database table is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves rebuilding or reorganizing indexes

on tables or views to improve query performance and reduce fragmentation of index pages. Reindexing can also improve data consistency and integrity by ensuring that indexes reflect the current state of the data in the tables or views.
Load balancing is not a likely cause of poor performance, data inconsistency and integrity issues, because it involves distributing workloads across multiple servers or resources to optimize resource utilization, throughput and response time of applications. Load balancing can also enhance data consistency and integrity by using algorithms and protocols to route requests to the most appropriate server or resource based on availability, capacity and performance.
References:
Data Caching
Database Clustering
Reindexing Database Tables in SQL Server
[Load Balancing]

NEW QUESTION: 195
下列哪一項是資訊科技指導委員會的主要職責？
A. 授權定期進行IT審計
B. 定期向業務部門報告 IT 效能
C. 促進業務與IT之間的協作
D. 確保業務部門支援 IT 目標
Answer: (SHOW ANSWER)

NEW QUESTION: 196
資訊系統審計員正在審口一家使用雲端系統進行託管的組織的營運資料庫管理。下列哪一項應該是審計員的主要關注領域？
A. 雲端供應商安全認證
B. 自動調整配置成本
C. 安全設定配置
D. 大規模資料傳輸
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed in-Depth Explanation:
The primary focus when reviewing operational database management in a cloud environment should be the security settings configuration. Cloud environments often have complex and customizable security configurations, and any misconfiguration can lead to data breaches or unauthorized access. Ensuring proper security settings helps maintain data confidentiality, integrity, and availability.
Cloud vendor security certifications (Option A) are important but do not directly address how security is configured. Auto-scaling of provisioning costs (Option B) relates to resource management rather than security. Large-scale data transfers (Option D) may be relevant, but security settings directly impact data protection.

NEW QUESTION: 197
下列哪一項能提供關於組織風險偏好和風險承受能力的最有用資訊？
A. 差距分析
B. 審計報告
C. 風險概況
D. 風險登記冊
Answer: C (LEAVE A REPLY)
The most useful information regarding an organization's risk appetite and tolerance is provided by its risk profile, as this is a document that summarizes the key risks that the organization faces, the potential impacts and likelihoods of those risks, and the acceptable levels of risk exposure for different objectives and activities.
A gap analysis is a tool that compares the current state and the desired state of a process or a system, and identifies the gaps that need to be addressed. Audit reports are documents that present the findings, conclusions, and recommendations of an audit engagement. A risk register is a tool that records and tracks the identified risks, their causes, their consequences,and their mitigation actions. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.1: IT Governance

NEW QUESTION: 198
來自位於網路外部的感測器系統的資料透過伺服器的開放連接埠接收。下列哪一項是確保從感測器系統收集的資料完整性的最佳方法？
A. 對感測器系統傳輸的資料進行雜湊處理。
B. 透過虛擬私人網路(VPN)將感測器資料傳輸到伺服器。
C. 將來自感測器系統的流量透過代理伺服器路由。
D. 在感測器系統上實現網路位址轉換。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 199
下列哪一項與最終用口計算 (EUC) 應用在財務報告方面存在的最大風險？

A. 無法快速修改和部署解決方案
B. 使用者缺乏便攜性
C. 因人工操作造成的時間損失
D. 電子表格中的計算錯誤
Answer: D (LEAVE A REPLY)
Spreadsheets, often used in EUC, are prone to manual input errors and formula mistakes. These errors can significantly compromise the accuracy and integrity of financial reporting.
References
ISACA CISA Review Manual (Current Edition) - Chapter on End-User Computing (EUC) risks Industry Research on Spreadsheet Errors: Multiple studies highlight the prevalence of errors in spreadsheets, especially those used for financial purposes.

NEW QUESTION: 200
在□部稽核流程的哪個階段會與負責審□範圍□業務流程的人員建立連結？
A. 規劃階段
B. 執行階段
C. 後續階段
D. 選擇階段
Answer: A (LEAVE A REPLY)
The planning phase is the stage of the internal audit process where contact is established with the individuals responsible for the business processes in scope for review. The planning phase involves defining the objectives, scope, and criteria of the audit, as well as identifying the key risks and controls related to the audited area. The planning phase also involves communicating with the auditee to obtain relevant information, documents, and data, as well as to schedule interviews, walkthroughs, and meetings. The planning phase aims to ensure that the audit team has a clear understanding of the audited area and its context, and that the audit plan is aligned with the expectations and needs of the auditee and other stakeholders.
The execution phase is the stage of the internal audit process where the audit team performs the audit procedures according to the audit plan. The execution phase involves testing the design and operating effectiveness of the controls, collecting and analyzing evidence, documenting the audit work and results, and identifying any issues or findings. The execution phase aims to provide sufficient and appropriate evidence to support the audit conclusions and recommendations.
The follow-up phase is the stage of the internal audit process where the audit team monitors and verifies the implementation of the corrective actions agreed upon by the auditee in response to the audit findings. The follow-up phase involves reviewing the evidence provided by the auditee, conducting additional tests or interviews if necessary, and evaluating whether the corrective actions have adequately addressed the root causes of the findings. The follow-up phase aims to ensure that the auditee has taken timely and effective actions to improve its processes and controls.

The selection phase is not a standard stage of the internal audit process, but it may refer to the process of selecting which areas or functions to audit based on a risk assessment or an annual audit plan. The selection phase involves evaluating the inherent and residual risks of each potential auditable area, considering the impact, likelihood, and frequency of those risks, as well as other factors such as regulatory requirements, stakeholder expectations, previous audit results, and available resources. The selection phase aims to prioritize and allocate the audit resources to those areas that present the highest risks or opportunities for improvement.
Therefore, option A is the correct answer.
References:
Stages and phases of internal audit - piranirisk.com
Step-by-Step Internal Audit Checklist | AuditBoard
AuditProcess | The Office of Internal Audit - University of Oregon

NEW QUESTION: 201
資訊系統審計員發現，某組織的資料遺失防護(DLP) 系統配置為使用供應商預設設定來識別違規行為。審計員的主要關注點應該是：
A. 可能會報告大量誤報違規情況。
B. 違規報告可能無法及時審核。
C. 違規行為可能無法根據組織的風險狀況進行分類。
D. 根據組織的風險狀況，違規報告可能不會保留
Answer: C (LEAVE A REPLY)

NEW QUESTION: 202
下列哪一項最有可能損害使用 RSA 加密建立的數位簽章所提供的控制權？
A. 使用摘要反轉雜湊函數
B. 修改明文訊息
C. 解密收件者的公鑰
D. 取得發送者的私鑰
Answer: D (LEAVE A REPLY)
A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document, by using a hash function and an asymmetric encryption algorithm. A hash function is a mathematical function that transforms any input data into a fixed-length output value called a digest, which is unique for each input. An asymmetric encryption algorithm uses two keys: a public key and a private key.
The public key can be shared with anyone, while the private key must be kept secret by the owner. To create a digital signature, the sender first applies a hash function to the plaintext message to generate a digest. Then, the sender encrypts the digest with their private key to produce the digital signature. To verify the digital signature, the receiver decrypts the digital signature with the sender's public key to obtain the digest. Then, the

receiver applies the same hash function to the plaintext message to generate another digest. If the two digests match, it means that the message has not been altered and that it came from the sender. The security of a digital signature depends on the secrecy of the sender's private key. If an attacker obtains the sender's private key, they can create fake digital signatures for any message they want, thus compromising the control provided by the digital signature. Reversing the hash function using the digest is not possible, as hash functions are designed to be one-way functions that cannot be inverted. Altering the plaintext message will result in a different digest after applying the hash function, which will not match with the decrypted digest from the digital signature, thus invalidating the digital signature. Deciphering the receiver's public key is not relevant, as public keys are meant to be publicly available and do not affect the security of digital signatures.

NEW QUESTION: 203
資訊系統審計員被指派對應用系統進行實施後審口。
下列哪一項會損害審計師的獨立性？
A. 審計員在系統開發過程中實施了一項具體的控制措施。
B. 審計員以專案團隊成員身分參與，但不承擔營運責任。
C. 審計員提供了有關最佳實務的建議。
D. 審計員專門為審計設計了一個嵌入式審計模組。
Answer: (SHOW ANSWER)
If an auditor implemented a control, they would later be reviewing their own work, which creates a self- review threat and compromises independence. Participating in the project without operational responsibilities (B) or providing advice (C) is acceptable as long as the auditor does not take ownership of decisions.
Designing audit modules (D) is also permissible since they are for audit use and do not affect operational processes. ISACA's Code of Professional Ethics and IS Audit Standards emphasize independence and objectivity as fundamental requirements to maintain credibility and avoid conflicts of interest.
References (ISACA): ISACA Standards for IS Audit and Assurance; ISACA Code of Professional Ethics.

NEW QUESTION: 204
下列哪一項是減輕無意中濫用授權存取權限的最有效控制措施？
A. 可接受使用保單的年度簽字確認
B. 定期監控使用者存取日誌
C. 安全意識培訓
D. 正式的紀律處分
Answer: C (LEAVE A REPLY)
The most effective control to mitigate unintentional misuse of authorized access is security awareness training. This is because security awareness training can educate users on the

proper use of their access rights, the potential consequences of misuse, and the best practices to protect the confidentiality, integrity, and availability of information systems. Security awareness training can also help users recognize and avoid common threats such as phishing, malware, and social engineering.
Annual sign-off of acceptable use policy, regular monitoring of user access logs, and formalized disciplinary action are not the most effective controls to mitigate unintentional misuse of authorized access. These controls may help deter or detect intentional misuse, but they do not address the root cause of unintentional misuse, which is often a lack of knowledge or awareness of security policies and procedures.

NEW QUESTION: 205
對於資訊系統審計師而言，下列哪一項與職責分離相關的發現最為重要？
A. 伺服器管理員也是基礎架構管理團隊的成員。
B. 測試原始碼的人員也負責批准更改。
C. 建立新使用者帳口的人也可以修改使用者存取權限等級。
D. 編輯原始碼的人也擁有生口環境的寫入權限。
Answer: (SHOW ANSWER)

NEW QUESTION: 206
參與軟體口品beta測試最重要的優勢是什麼？
A. 它提高了組織留住那些更喜歡使用新技術的員工的能力。
B. 它改善了供應商支援和培訓。
C. 它增強了安全性和保密性。
D. 它使組織能口熟悉新口品及其功能。
Answer: D (LEAVE A REPLY)
Beta testing is the process of releasing a near-final version of a software product to a group of external users, known as beta testers, who provide feedback and report bugs based on their real-world experiences. Beta testingoffers various benefits for both the developers and the users of the software product. Some of these benefits are:
It reduces product failure risk via customer validation12.
It helps to test post-launch infrastructure1.
It helps to improve product quality via customer feedback12.
It allows for thorough bug detection and issue resolution3.
It enhances usability and user experience3.
It increases customer satisfaction and loyalty3.
Based on these benefits, the most important advantage of participating in beta testing of software products is D). It enables an organization to gain familiarity with new products and their functionality. By being involved in beta testing, an organization can learn how to use the new product effectively, discover its features and benefits, and provide suggestions for improvement. This can help the organization to adopt the new product faster, easier, and

more efficiently when it is officially released. It can also give the organization a competitive edge over other users who are not familiar with the new product.

NEW QUESTION: 207
當發現低風險異常情況時，下列何者是資訊系統審計師的最佳方法？
A. 重新調整異常情況的進一步測試優先級，並將重點放在風險更高的問題上。
B. 更新審計計劃，使其包含審計過程中收集的資訊。
C. 要求受審計單位及時糾正異常狀況
D. 記錄審計工作底稿中的異常情況
Answer: D (LEAVE A REPLY)
Documenting anomalies in audit workpapers (D) is the best approach because it ensures traceability, supports findings in the audit report, and allows for future reference if similar issues arise. Even if an anomaly is low- risk, proper documentation is a fundamental audit practice.
Other options:
Reprioritizing testing (A) is a valid audit approach but does not address documentation needs.
Updating the audit plan (B) may be necessary but does not replace documentation.
Prompt remediation (C) is an operational concern but is not always the auditor's primary role.
Reference: ISACA CISA Review Manual, Audit Process

NEW QUESTION: 208
緊急斷電開關應該：
A. 可遠端存取。
B. 無法辨識。
C. 受到保護。
D. 在雙重控制之下。
Answer: C (LEAVE A REPLY)
The correct answer is C. Be protected.
An emergency power-off switch is a critical safety mechanism, but it also creates operational risk if it can be triggered accidentally or without proper safeguards. ISACA's official CISA practice material specifically treats a missing cover on an emergency power-off button as a significant concern, which supports the conclusion that the switch should be protected against accidental activation.
Option A is incorrect because remote accessibility could increase the risk of misuse or accidental shutdown.
Option B is incorrect because the switch should be identifiable in an emergency; hiding it would conflict with emergency response needs.

Option D is incorrect because dual control is not the primary requirement for an emergency switch intended for urgent use.
Therefore, the correct answer is C, because the switch should be protected, typically by a cover or similar safeguard, while still remaining available for emergency use.
References (Official ISACA):
* ISACA, CISA Practice Quiz - identifies a missing emergency power-off button cover as a significant concern.

NEW QUESTION: 209
在實施新系統的過程中，資訊系統審計師必須評估某些自動化計算是否符合監管要求。下列哪一項是獲得這種保證的最佳方法？
A. 審核簽名文件
B. 檢視與計算相關的原始碼
C. 使用審計軟體重新執行計算
D. 檢口使用者驗收測試 (UAT) 結果
Answer: C (LEAVE A REPLY)
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant. References:
CISA Review Manual (Digital Version), page 325
CISA Questions, Answers and Explanations Database, question ID 3335

NEW QUESTION: 210
下列哪一種加密方法提供最佳的無線安全性？
A. Wi-Fi Protected Access 3 (WPA3)
B. 資料加密標準(DES)
C. 有線等效加密 (WEP)
D. 安全通訊端層 (SSL)
Answer: A (LEAVE A REPLY)
Wireless security relies onstrong encryptionto prevent unauthorized access and data interception.
Option A (Correct):WPA3is thelatest and most secureWi-Fi encryption standard, offeringstronger protectionagainst brute-force attacks and improvingkey management.
Option B (Incorrect):DES is outdatedand vulnerable tomodern attacks, making it unsuitable for wireless security.
Option C (Incorrect):WEP is highly insecuredue toweak encryptionand can be cracked inminutesusing basic tools.
Option D (Incorrect):SSL secures web traffic, notwireless networks.

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

NEW QUESTION: 211
衡量一個組織安全計畫有效性的最重要指標是：
A. 與競爭對手經歷的關鍵事件進行比較。
B. 報告的新漏洞數量。
C. 事件對關鍵業務活動的不利影響。
D. 上報給高階管理層的漏洞警報數量。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 212
下列何者最有利於發生事故時口動法律程序？
A. 進行電子取證的權利
B. 法律顧問的建議
C. 維護監管鏈
D. 根本原因分析結果
Answer: C (LEAVE A REPLY)
The best way to facilitate the legal process in the event of an incident is to preserve the chain of custody of the evidence. The chain of custody is a record of who handled, accessed, or modified the evidence, when, where, how, and why. The chain of custody helps to ensure the integrity, authenticity, and admissibility of the evidence in a court of law. The chain of custody also helps to prevent tampering, alteration, or loss of evidence that could compromise the investigation or the prosecution. References:
CISAReview Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 213
下列哪一項是確定基於風險的審計計劃的關鍵領域的最佳方法？
A. 檢視同業基準測試結果。
B. 檢視近期審計報告中未解決的問題。

C. 採訪企業中的相關利害關係人。
D. 與資訊長進行風險調口。
Answer: (SHOW ANSWER)
The best answer is C. Interview relevant stakeholders in the business.
ISACA guidance on risk-based audit planning emphasizes understanding the business context, identifying risk themes, and engaging stakeholders to determine what matters most. One ISACA example describes interviewing hundreds of leaders to identify risk themes for audit planning. Stakeholder interviews give the auditor a direct view of business objectives, current risks, process changes, emerging concerns, and management priorities across the enterprise.
Option A. Review peer benchmarking results can provide context, but benchmarking does not reveal the organization's own risk drivers.
Option B. Review open issues from recent audit reports is useful input, but it is backward-looking and incomplete by itself.
Option D. Conduct a risk survey with the CIO is too narrow because risk-based audit planning should reflect the broader business, not only the CIO's perspective.
Therefore, C is the correct answer because interviewing relevant business stakeholders is the best way to identify the key areas that should shape a risk-based audit plan.
References (Official ISACA):
* ISACA Journal, Transforming the IT Audit Function-Taking the Digital Journey.
* ISACA Journal, IS Audit Basics: Risk-based Audit Planning for Beginners.
* ISACA Journal, Business Skills for the IT Audit and Assurance Professional.
* ISACA, The Future of Cybersecurity Assessments Is Here - includes stakeholder interviews as part of risk assessment.

NEW QUESTION: 214
下列哪一項最能描述數位簽章？
A. 它由接收器控制。
B. 它具備授權能力。
C. 它動態驗證資料的修改。
D. 它是使用它的發送者獨有的。
Answer: D (LEAVE A REPLY)
A digital signature is a type of electronic signature that uses cryptographic techniques to provide authentication, integrity, and non-repudiation of digital documents. A digital signature is created by applying a mathematical function (called a hash function) to the document and then encrypting the result with the sender's private key. The encrypted hash, along with the sender's public key and other information, forms the digital signature. The receiver can verify the digital signature by decrypting it with the sender's public key and comparing the hash with the one computed from the document. If they match, it

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

NEW QUESTION: 215
在採用資料虛擬化的環境中，下列哪一項提供了最佳的災難復原解決方案？
A. 本機磁碟備份系統
B. 基於磁帶的備份系統
C. 虛擬磁帶庫
D. 獨立磁碟冗餘陣列(RAID)

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

NEW QUESTION: 216
受審計單位不同意審計報告草稿中提出的糾正措施建議。
在準備最終報告時，資訊系統審計師的最佳做法是什麼？
A. 在發布最終報告之前達成一致。
B. 在最終參與報告中納入高階主管支持的立場
C. 確保被審計方的意見包含在工作底稿中。
D. 從最終專案報告中排除有爭議的建議
Answer: B (LEAVE A REPLY)
The IS auditor's best course of action when preparing the final report is to include the position supported by senior management in the final engagement report. The IS auditor should communicate the audit findings and recommendations to senior management and obtain their feedback and approval before issuing the final report. If there is a disagreement between the auditee and the IS auditor regarding a recommendation for corrective action, the IS auditor should present both sides of the argument and the supporting evidence, and seek senior management's opinion and decision. The IS auditor should respect and follow senior management' s position, and include it in the final engagement report, along with the auditee's comments if applicable. The other options arenot the best course of action, because they either do not resolve the disagreement, do

notreflect senior management's authority, or do not report the audit results accurately and completely. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.5

NEW QUESTION: 217
在電子資料交換 (EDI) 通訊中，金額欄位的校驗和用於確保金融交易的準確性：
A. 不可否認性。
B. 完整性，
C. 授權，
D. 真實性。
Answer: (SHOW ANSWER)

NEW QUESTION: 218
下列哪一項是訂定審計目標的主要依據？
A. 審計風險
B. 風險考慮
C. 先前審核的評估
D. 經營策略
Answer: B (LEAVE A REPLY)
The primary basis on which audit objectives are established is the consideration of risks12. This involves identifying and assessing the risks that could prevent the organization from achieving its objectives12. The audit objectives are then designed to address these risks and provide assurance that the organization's controls are effective in managing them12. While audit risk, assessment of prior audits, and business strategy are important factors in the audit process, they are secondary to the fundamental requirement of considering risks12.
References:
Objectives of Auditing - Primary and Secondary Objectives of Auditing | Auditing Management Notes Audit Objectives | Primary and Subsidiary Audit Objectives - EDUCBA

NEW QUESTION: 219
下列哪一個指標最能反映 Web 應用程式的效能？
A. HTTP 伺服器錯誤率
B. 伺服器執行緒數
C. 平均回應時間
D. 伺服器正常運作時間
Answer: C (LEAVE A REPLY)
The best indicator of the performance of a web application is the average response time. This metric measures how long it takes for the web server to process and deliver a request from the client. It reflects the user's perception of how fast or slow the web application is, and it affects the user's satisfaction, engagement, and conversion. A low average

response time means that the web application is responsive and efficient, while a high average response time means that the web application is sluggish and unreliable.
HTTP server error rate, server thread count, and server uptime are not as good indicators of the performance of a web application as the average response time. HTTP server error rate measures how often the web server fails to handle a request and returns an error code, such as 404 (Not Found) or 500 (Internal Server Error).
This metric indicates the reliability and availability of the web application, but it does not capture how fast or slow the web application is. Server thread count measures how many concurrent requests the web server can handle at a given time. This metric indicates the scalability and capacity of the web application, but it does not capture how long each request takes to process. Server uptime measures how long the web server has been running without interruption. This metric indicates the stability and resilience of the web application, but it does not capture how well the web application performs during that time.
References:
10 Key Application Performance Metrics and How to Measure Them - Stackify1 Measuring performance - Learn web development | MDN2 Understanding the Basics of Web Performance | BrowserStack3
14 Important Website Performance Metrics You Should Be Analyzing4
Top 8 Web Application Performance Metrics | MetricFire Blog5
Web Performance Monitoring: A How to Guide for Developers - Stackify6

NEW QUESTION: 220
口部稽核團隊正在決定是否使用位於其他國家/地區的第三方託管的稽核管理應用程式。
在託管應用程式中上傳薪資審計文件時，最重要的考慮因素是什麼？
A. 影響組織的財務法規
B. 應用程式託管所在的資料中心的實體存取控制
C. 影響組織的隱私法規
D. 託管服務提供者收取的單位儲存成本
Answer: (SHOW ANSWER)
This is because privacy regulations are laws or rules that protect the personal information of individuals from unauthorized access, use, disclosure, or transfer by third parties. Payroll audit documentation may contain sensitive and confidential data, such as employee names, salaries, benefits, taxes, deductions, and bank accounts. If the audit management application is hosted by a third party in a different country, the organization may need to comply with the privacy regulations of both its own country and the host country, as well as any international or regional agreements or frameworks that apply. Privacy regulations may impose various requirements and obligations on the organization, such as obtaining consent from the data subjects, implementing appropriate security measures, notifying data breaches, and ensuring data quality and accuracy.
Privacy regulations may also grant various rights to the data subjects, such as accessing, correcting, deleting, or transferring their data. Failing to comply with privacy regulations

may expose the organization to significant risks and consequences, such as legal actions, fines, sanctions, reputational damage, or loss of trust.
Some examples of privacy regulations affecting the organization are:
The General Data Protection Regulation (GDPR), which is a comprehensive and strict privacy regulation that applies to anyorganization that processes personal data of individuals in the European Union (EU) or offers goods or services to them, regardless ofwhere the organization or the data is located1.
The California Consumer Privacy Act (CCPA), which is a broad and influential privacy regulation that applies to any organization that collectspersonal information of California residentsand meets certain thresholds of revenue, data volume, or data sharing2.
The Health Insurance Portability and Accountability Act (HIPAA), which is a sector-specific privacy regulation that applies to any organization that handles protected health information(PHI) of individuals in the United States, such as health care providers, health plans, or health care clearinghouses3.
Therefore, before using an audit management application hosted by a third party in a different country, the internal audit team should conduct a thorough assessment of the privacy regulations affecting the organization and ensure that they have adequate policies, procedures, and controls in place to comply with them.

NEW QUESTION: 221
下列哪一項應該是災難復原計畫(DRP)的主要目標？
A. 最大限度減少資訊損失
B. 評估關鍵應用程式的風險
C. 辨識關鍵業務流程
D. 記錄所有 IT 資口
Answer: A (LEAVE A REPLY)
The primary objective of a disaster recovery plan is recovery of interrupted IT-related activities in a way that minimizes the impact of the disruption. Official ISACA definitions describe disaster recovery as activities and programs designed to return the enterprise to an acceptable condition and restore critical business functions through a DRP. ISACA's glossary defines a disaster recovery plan (DRP) as a set of human, physical, technical, and procedural resources to recover an interrupted activity within a defined time and cost.
Among the answer choices, A. Minimizing loss of information is the best match. ISACA guidance states that a DRP contains procedures for restoring systems and data, minimizing loss of information and downtime, and ensuring business continuity. This makes option A the strongest answer because it captures a direct purpose of the DRP itself.
Option B ("Assessing the risk of key applications") is an important planning activity, but it is not the primary objective of the DRP. Risk assessment is part of developing continuity capability, not the ultimate aim of the plan. ISACA continuity guidance treats assessing risks and impacts as a step in the DRP process, not the main end goal.

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

NEW QUESTION: 222
使用電子表格計算項目成本估算。然後將每個成本類別的總計資料輸入到作業成本系統中。確保資料準確輸入系統的最佳控制措施是什麼？
A. 以項目核對總金額
B. 有效性檢口，防止輸入字元資料
C. 對每種成本類型進行合理性檢口
D. 在條目之後顯示項目詳情的背面
Answer: A (LEAVE A REPLY)
Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected.
Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete.
Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data

matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human errors, but it cannot guarantee that the data is accurate or consistent with the source.
References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

NEW QUESTION: 223
下列哪一項措施最能有效提升流程改善計畫的效果？
A. 基於模型的設計符號
B. 平衡計分卡
C. 能力成熟度模型
D. 專案管理方法論
Answer: C (LEAVE A REPLY)
Capability maturity models (CMMs) are frameworks that help organizations assess and improve their processes in various domains, such as software development, project management, service delivery, and cybersecurity1. CMMs define different levels of process maturity, from initial to optimized, and describe the characteristics and best practices of each level. By using CMMs, organizations can benchmark their current processes against a common standard, identify gaps and weaknesses, and implement improvement actions to achieve higher levels of process maturity2. CMMs can also help organizations align their processes with their strategic goals, measure their performance, and increase their efficiency, quality, and customer satisfaction3.
Therefore, the use of CMMs would best enhance a process improvement program, as they provide a systematic and structured approach to evaluate and improve processes based on proven principles and practices. Option C is the correct answer.
Option A is not correct because model-based design notations are graphical or textual languages that help designers specify, visualize, and document the structure and behavior of systems4. While they can be useful for designing and communicating complex systems, they do not directly address the process improvement aspect of a program.
Option B is not correct because balanced scorecard is a strategic management tool that helps organizations translate their vision and mission into measurable objectives and indicators. While it can be useful for monitoring and evaluating the performance of a program, it does not provide specific guidance on how to improve processes.
Option D is not correct because project management methodologies are sets of principles and practices that help organizations plan, execute, and control projects. While they can be useful for managing the scope, schedule, cost, quality, and risk of a program, they do not focus on the process improvement aspect of a program.
References:
Guide to Process Maturity Models2
What is CMMI? A model for optimizing development processes1
Capability Maturity Model (CMM): A Definitive Guide3

Model-Based Design Notations4
Balanced Scorecard
Project Management Methodologies

NEW QUESTION: 224
資訊系統審計師在審計過程中發現問題並進行補救的主要職責是：
A. 向管理階層提交更新後的政策以供批准。
B. 解釋調口結果並提供一般性建議。
C. 透過提供解決方案來幫助被審計單位管理。
D. 承擔問題責任並監督補救工作。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
系統效能儀錶板顯示，多個應用程式伺服器的CPU 分配已達到設定的閾口。下列哪一項是資訊系統稽核員對 IT 部門的最佳建議？
A. 終止這些伺服器的入站和出站連接，以避免過載
B. 驗證這些伺服器的處理能力是否足以完成運算任務。
C. 通知最終用口伺服器效能下降可能導致的服務中斷。
D. 提高定義的處理閾口，以反映正常運作期間的口能消耗
Answer: B (LEAVE A REPLY)

NEW QUESTION: 226
後續審計的主要目標是：
A. 評估建議的適當性。
B. 驗證是否遵守政策。
C. 確定對建議採取的行動是否充分。
D. 評估風險狀況是否有變化。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 227

在評估組織的 IT 績效指標是否與同一口業的其他組織具有可比性時，下列何者最有助於審口？

A. IT治理框架

B. 基準調口

C. 利用率報告

D. 平衡計分卡

Answer: (SHOW ANSWER)

IT performance measures are indicators of how well an organization is achieving its IT goals and objectives.

Benchmarking surveys are useful tools for comparing an organization's IT performance measures with those of other organizations in the same industry or sector. Benchmarking surveys can provide insights into best practices, gaps, trends, and opportunities for improvement. IT governance frameworks, utilization reports, and balanced scorecards are not as helpful for comparing ITperformance measures across organizations, as they may vary in scope, methodology, and terminology. References: IT Resources | Knowledge and Insights | ISACA, CISA Review Manual (Digital Version)

NEW QUESTION: 228

某組織關注如何滿足保護資料機密性的新法規，並委託資訊系統稽核員評估其資料傳輸流程。下列哪一項最能支持組織的目標？

A. 加密哈希

B. 虛擬區域網路(VLAN)

C. 加密

D. 專用線路

Answer: C (LEAVE A REPLY)

The best option to support the organization's objectives of protecting data confidentiality while transporting data is encryption. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality of data in transit by preventing unauthorized interception,modification, or disclosure of the data. Encryption can also help comply with data privacy and security regulations, such as the GDPR and HIPAA.

The other options are not as effective as encryption in protecting data confidentiality while transporting data.

Cryptographic hashes are mathematical functions that generate a fixed-length output from an input, but they do not encrypt the data. Hashes are used to verify the integrity and authenticity of data, but they do not prevent unauthorized access to the data. Virtual local area network (VLAN) is a logical grouping of network devices that share the same broadcast domain, but they do not encrypt the data. VLANs can improve network performance and security by isolating traffic, but they do not protect the data from being intercepted or modified by external attackers. Dedicated lines are physical connections that

provide exclusive access to a network or service, but they do not encrypt the data. Dedicated lines can offer higher bandwidth and reliability, but they do not guarantee the confidentiality of the data from being compromised by physical tampering or eavesdropping.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2 Data Security and Confidentiality Guidelines - Centers for Disease Control and Prevention3 Information Security | Confidentiality - GeeksforGeeks4

NEW QUESTION: 229
對於審口網路印表機處置流程的資訊系統稽核員而言，下列何者最應受到重視？
A. 處置政策和程序執行不一致。
B. 沒有證據可以驗證印表機硬碟在處置前是否已清除資料。
C. 業務部門可直接處置印表機。
D. 無法使用的印表機存放在不安全的區域。
Answer: B (LEAVE A REPLY)
The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
387

NEW QUESTION: 230
下列哪一種生物辨識門禁系統的漏檢率最高？
A. 虹膜識別
B. 指紋掃描
C. 人臉辨識
D. 視網膜掃描
Answer: B (LEAVE A REPLY)
Among the options provided, fingerprint scanning has the highest rate of false negatives. False negatives occur when a biometric system fails to recognize an authentic individual. Factors such as skin conditions (wet, dry, greasy), finger injuries, and inadequate scanning can contribute to false negatives in fingerprint scanning1. In comparison, iris recognition23, face recognition45, and retina scanning67 generally have lower rates of false negatives.
References:
How Accurate are today's Fingerprint Scanners? - Bayometric

25 Advantages and Disadvantages of Iris Recognition - Biometric Today
Iris Recognition Technology (or, Musings While Going through Airport ...
The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist | ITIF NIST Launches Studies into Masks' Effect on Face Recognition Software Retinal scan - Wikipedia How accurate are retinal security scans - Smart Eye Technology

NEW QUESTION: 231
遭受網路攻擊的組織正在對受影響用口的電腦進行取證分析。對於審口此過程的資訊系統審計員來口，下列哪一項最口得關注？
A. 採用成像過程取得每台電腦的資料副本。
B. 法律部門尚未介入。
C. 監管鏈尚未記錄在案。
D. 審計僅在資訊擷取階段參與。
Answer: C (LEAVE A REPLY)
The chain of custody has not been documented is a finding that should be of greatest concern for an IS auditor reviewing a forensic analysis process of an organization that has suffered a cyber attack. The chain of custody is a record of who handled, accessed, or modified the evidence during a forensic investigation.
Documenting the chain of custody is essential to preserve the integrity, authenticity, and admissibility of the evidence in a court of law. The other options are less concerning findings that may not affect the validity or reliability of the forensic analysis process.
References:
CISAReview Manual (Digital Version), Chapter 7, Section 7.51
CISA Review Questions, Answers and Explanations Database, Question ID 220

NEW QUESTION: 232
資訊系統審計員正在審口新伺服器的安裝。資訊系統審計員的主要目標是確保：
A. 安全參數依照製造商的標準設定。
B. 在收購之前，已正式批准了一份詳細的商業計劃書
C. 安全參數根據組織的策略設定。
D. 此採購項目邀請了至少來自三個不同供應商的貸款方。
Answer: C (LEAVE A REPLY)
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settingsor options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in

accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:
A). Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.
B). A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
D). The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization.
References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA] , [Business Case - ISACA], [Tender - ISACA] , [Procurement Management - ISACA]

NEW QUESTION: 233
對管理行動計畫進行審計後續行動的主要目標應該是下列哪一項？
A. 驗證審計報告中列出的風險是否已妥善緩解
B. 識別組織面臨的新風險和控制措施；確保高階管理層了解審計結果；使管理行動計劃與業務需求保持一致。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 234
在評估與網路監控相關的控制設計時，資訊系統稽核員最需要檢視下列哪一項口容？
A. 事件監控服裝
B. 網際網路服務供應商服務等級協定
C. 網路流量分析報告
D. 網路拓樸圖
Answer: D (LEAVE A REPLY)
Network topology diagrams are the most important for an IS auditor to review when evaluating the design of controls related to network monitoring, because they show how the network components are connected and configured, and what security measures are in place to protect the network from unauthorized access or attacks. Incident monitoring logs,

the ISP service level agreement, and reports of network traffic analysis are useful for evaluating the effectiveness and performance of network monitoring, but not the design of controls. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.3

NEW QUESTION: 235
對於審口組織機構在辦公室之間傳輸敏感資料的方法的資訊系統審計員來口，下列哪一項應該是他們最關注的問題？
A. 此方法完全依賴公鑰基礎設施(PKI)的使用。
B. 此方法完全依賴數位簽章的使用。
C. 此方法完全依賴非對稱加密演算法的使用。
D. 此方法完全依賴 128 位元加密。
Answer: C (LEAVE A REPLY)
The greatest concern to an IS auditor reviewing an organization's method to transport sensitive data between offices is that the method relies exclusively on the use of asymmetric encryption algorithms. Asymmetric encryption algorithms, also known as public key encryption, use two different keys for encryption and decryption: a public key that is shared with anyone who wants to communicate with the sender, and a private key that is kept secret by the sender. Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, which use the same key for both encryption and decryption, but they are also slower and more computationally intensive. Therefore, relying exclusively on asymmetric encryption algorithms may not be efficient or practical for transporting large amounts of sensitive data between offices. A better method would be to use a combination of symmetric and asymmetric encryption algorithms, such as using asymmetric encryption to exchange a symmetric key and then using symmetric encryption to encrypt and decrypt the data.
The other options are not as concerning as option C. The method relying exclusively on the use of public key infrastructure (PKI) is not a concern, because PKI is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates that are based on asymmetric encryption algorithms. PKI enables secure and authenticated communication between parties who do not have a prior trust relationship. The method relying exclusively on the use of digital signatures is not a concern, because digital signatures are a way of verifying the authenticity and integrity of a message or document by using asymmetric encryption algorithms. Digital signatures ensure that the sender cannot deny sending the message or document, and that the receiver can detect any tampering or alteration of the message or document. The method relying exclusively on the use of 128-bit encryption is not a concern, because 128-bit encryption is a level of encryption that uses a 128-bit key to encrypt and decrypt data. 128-bit encryption is considered to be strong enough to resist brute-force attacks by modern computers. References: Asymmetric vs Symmetric Encryption: What are differences?, Public Key Infrastructure (PKI), Digital Signature, What is
128-bit Encryption?

NEW QUESTION: 236
哪種類型的裝置位於企業或家庭網路的邊界，取得公用IP 位址，然後在口部口生私有IP 位址？
A. 切換
B. 入侵防禦系統(IPS)
C. 網關
D. 路由器
Answer: D (LEAVE A REPLY)
A router is a type of device that sits on the perimeter of a corporate or home network, where it obtains a public IP address and then generates private IP addresses internally. A router connects two or more networks and forwards packets between them based on routing rules. A router can also provide network address translation (NAT) functionality, which allows multiple devices to share a single public IP address and access the internet. A switch is a type of device that connects multiple devices within a network and forwards packets based on MAC addresses. An intrusion prevention system (IPS) is a type of device that monitors network traffic and blocks or modifies malicious packets based on predefined rules. A gateway is a type of device that acts as an interface between different networks or protocols, such as a modem or a firewall. References: CISA Review Manual (Digital Version), [ISACA Glossary of Terms]

NEW QUESTION: 237
在使用數據分析時，資訊系統審計師最應該關注下列哪一項？
A. 審核員未擷取數據
B. 資料來源缺乏完整性
C. 資料分析軟體是開源的
D. 資料集中包含不相關字段
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
在討論審計報告草稿時，IT 管理階層提供了適當的證據，證明已針對資訊系統審計師認定為無效的控制措施實施了流程。下列哪一項是審計師的最佳行動？
A. 向IT管理階層解釋，將在後續工作中評估新的控制措施
B. 在報告中加入 IT 管理階層所採取行動的評論
C. 根據IT管理階層提供的證據修改結論
D. 在更改結論之前重新執行審計。
Answer: D (LEAVE A REPLY)
The auditor's best action is to re-perform the audit before changing the conclusion, because the auditor needs to obtain sufficient and appropriate evidence to support the audit opinion. The evidence provided by IT management may not be reliable or relevant,

and it may not reflect the actual effectiveness of the control during the audit period. Therefore, the auditor should verify the evidence independently and test the control again to ensure that it meets the audit criteria and objectives. The other options are not appropriate, because they either ignore or accept the evidence provided by IT management without verification, which may compromise the quality and integrity of the audit. References:
ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.51
ISACA, IT Audit and Assurance Standards,Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12062

NEW QUESTION: 239
在審口將機密資料備份遷移到基於雲端的解決方案的專案時，資訊系統審計員最應該關注以下哪項發現？
A. 已棄用的備份媒體缺乏監管鏈
B. 可擴充性不足
C. 對供應商進行的盡職調口不足
D. 儲存成本增加
Answer: C (LEAVE A REPLY)
The best answer is C. Insufficient due diligence performed on the vendor.
ISACA guidance on third-party and cloud risk repeatedly emphasizes the need for thorough vendor due diligence before entering or expanding a business relationship. When confidential backups are being migrated to a cloud solution, insufficient due diligence is the greatest concern because it can expose the organization to security, privacy, resilience, and compliance failures across the whole service arrangement.
Option A is relevant for retired media handling, but it is narrower than the overall third-party risk. Option B affects performance and growth, not necessarily confidentiality. Option D is a business issue, but not the greatest audit concern when confidential data is involved. Vendor due diligence is the most important control at this stage.
References (Official ISACA):
* ISACA, The Top 5 Cybersecurity Threats and How to Defend Against Them.
* ISACA Journal, The Encrypted Truth Is Already Out There.

NEW QUESTION: 240
某組織開展了一項活動，旨在測試使用者的安全意識程度。他們向用口發送一封電子郵件，郵件正文中嵌入一個鏈接，點擊該鏈接即可獲得現金獎勵。下列哪一個指標最能反映這次安全意識培訓的有效性？
A. 因郵件為釣魚郵件而將其刪除但未舉報的使用者數量
B. 點擊連結了解更多郵件寄件者資訊的使用者數量
C. 將電子郵件轉發給其業務部門經理的使用者數量
D. 向資訊安全團隊報告收到電子郵件的使用者數量
Answer: (SHOW ANSWER)

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

NEW QUESTION: 241
下列哪一項措施能最好地降低網路攻擊期間資料外洩的風險？
A. 敏感資料的雜湊處理
B. 網路存取控制(NAC)
C. 資料遺失防護(DLP)系統
D. 周界防火牆
Answer: C (LEAVE A REPLY)

NEW QUESTION: 242
資訊系統審計員正在審口外包服務台的服務管理情況。下列何者最能有效衡量服務提供者執行此項職能的效率？
A. 顧客滿意度評分
B. 通話記錄審核
C. 已完成的通話次數
D. 平均票齡
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
下列何者最能證明業務連續性計畫 (BCP) 的所有要素都在有效運作？
A. 完整運行測試結果
B. 演練測試結果
C. 桌面測試結果
D. 模擬測試結果

Answer: B (LEAVE A REPLY)

NEW QUESTION: 244
在對網路漏洞進行外部評估時，最重要的是驗證什麼？
A. 安全資訊事件管理 (SIEM) 規則更新
B. 定期檢視網路安全策略
C. 網路資口清單的完整性
D. 入侵偵測系統(IDS)的位置
Answer: (SHOW ANSWER)
An external assessment of network vulnerability is a process of identifying and evaluating the weaknesses and risks that affect the security and availability of a network froman outsider's perspective. The most important factor to verify during this process is the completeness of network asset inventory, which is a list of all the devices, systems, and software that are connected to or part of the network. A complete and accurate network asset inventory can help identify the scope and boundaries of the network, the potential attack vectors and entry points, the critical assets and dependencies, and the existing security controls and gaps. Without a complete network asset inventory, an external assessment of network vulnerability may miss some important assets or vulnerabilities, leading to inaccurate or incomplete results and recommendations.
References:
1 explains what is an external vulnerability scan and why it is important to have a complete network asset inventory.
2 provides a guide on how to conduct a full network vulnerability assessment and emphasizes the importance of knowing the network assets.
3 compares internal and external vulnerability scanning and highlights the need for a comprehensive network asset inventory for both types.

NEW QUESTION: 245
資訊系統審計員得出結論，某組織擁有高品質的安全策略。接下來最需要確定的是下列哪一項？該策略必須：
A. 所有員工都能很好地理解。
B. 基於業界標準。
C. 由流程擁有者開發。
D. 頻繁更新。
Answer: (SHOW ANSWER)
The most important thing to determine next after concluding that an organization has a quality security policy is whether the policy is well understood by all employees. A security policy is a document that defines the objectives, scope, roles, responsibilities, and rules for information security within an organization. A quality security policy is one that is clear, concise, consistent, comprehensive, and aligned with business goals and requirements.

However, a quality security policy is useless if it is not well understood by all employees who are expected to comply with it.Therefore, the IS auditor should assess the level of awareness and understanding of the security policy among employees and identify any gaps or issues that need to be addressed. The other options are not as important as ensuring that the security policy is well understood by all employees, as they do not directly affect the implementation and effectiveness of the security policy. References: CISA Review Manual, 27th Edition, page 317

NEW QUESTION: 246
下列何者是判斷第三方供應商是否遵守組織要求的控制措施的最佳指標？
A. 供應商維護的認證
B. 對供應商系統的日誌文件進行實質審口
C. 審核供應商提交的每月績效報告
D. 對供應商進行定期獨立評估
Answer: (SHOW ANSWER)

NEW QUESTION: 247
資訊系統審計員發現，為了提升效能,Web應用程式中的驗證控制已從伺服器端移至瀏覽器端。這極有可能透過以下方式增加攻擊成功的風險：
A. 結構化口詢語言(SQL)注入
B. 緩衝區溢位。
C. 拒口服務(DoS)。
D. 網路釣魚。
Answer: A (LEAVE A REPLY)
Validation controls are used to check the input data from the user before processing it on the server. If the validation controls are moved from the server side to the browser, it means that the user can modify or bypass them using tools such as browser developer tools, JavaScript console, or proxy tools. This would increase the risk of a successful attack by structured query language (SQL) injection, which is a technique that exploits a security vulnerability in an application's software layer that allows an attacker to execute arbitrary SQL commands on the underlying database. SQL injection can result in data theft, data corruption, or unauthorized access to the system.
Buffer overflow, denial of service (DoS), and phishing are not directly related to the validation controls in a web application. Buffer overflow is a type of attack that exploits a memory management flaw in an application or system that allows an attacker to write data beyond the allocated buffer size and overwrite adjacent memory locations. DoS is a type of attack that prevents legitimate users from accessing a service or resource by overwhelming it with requests or traffic. Phishing is a type of attack that uses fraudulent emails or websites to trick users into revealing sensitive information or installing malware.
References:
Client-side form validation - Learn web development | MDN

JavaScript: client-side vs. server-side validation - Stack Overflow
SQL Injection - OWASP

NEW QUESTION: 248
下列哪一項屬於矯正性控制措施？
A. 分離設備開發測試與生口
B. 驗證資料處理中的重複計算
C. 審口使用者存取權限以實現隔離
D. 執行緊急應變計劃
Answer: D (LEAVE A REPLY)
A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions.
Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems.
Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles. References: ISACA, CISA Review Manual,
27th Edition, 2018, page 64

NEW QUESTION: 249
在實施資料分類程序時，下列何者最為重要？
A. 理解資料分類級別
B. 正式確定資料所有權
C. 制定隱私權政策
D. 規劃安全儲存容量
Answer: B (LEAVE A REPLY)
Data classification is the process of organizing data into categories based on its sensitivity, value, and risk to the organization. Data classification helps to ensure that data is protected according to its importance and regulatory requirements. Data classification also enables data owners to make informed decisions about data access, retention, and disposal.
To implement a data classification program, it is most important to formalize data ownership. Data owners are the individuals or business units that have the authority and responsibility for the data they create or use. Data owners should be involved in defining the data classification levels, assigning the appropriate classification to their data, and ensuring that the data is handled according to the established policies and procedures. Data owners should also review and update the data classification periodically or when there are changes in the data or its usage.

The other options are not as important as formalizing data ownership when implementing a data classification program. Understanding the data classification levels is necessary, but it is not sufficient without identifying the data owners who will apply them. Developing a privacy policy is a good practice, but it is not specific to data classification. Planning for secure storage capacity is a technical consideration, but it does not address the business and legal aspects of data classification.
References:
ISACA, CISA Review Manual, 27th Edition, 2020, page 247
Data Classification: What It Is and Howto Implement It

NEW QUESTION: 250
在組織口部設立資訊系統稽核職能的最大優勢是什麼？
A. 全年提高資訊系統審計人員的可見度和可用性
B. 與管理階層協商建議的能力
C. 更了解業務和流程
D. 提高建議的獨立性和公正性
Answer: C (LEAVE A REPLY)

NEW QUESTION: 251
資訊系統審計員已確認某組織的 IT 部門運行多個低優先順序的自動化任務。下列哪一項是自動化作業計畫的最佳建議？
A. 應避免執行低優先權任務。
B. 低優先權任務應包括主要功能。
C. 低優先權作業應獲得最佳資源。
D. 低優先權作業應根據資源可用性進行排程。
Answer: (SHOW ANSWER)
Low-priority jobs typically involve non-critical processes or tasks that do not immediately impact business operations. The best approach to handling such jobs is to schedule them subject to resource availability. This ensures that high-priority tasks can access resources when needed without being affected by the execution of low-priority tasks.
Avoiding Low-Priority Jobs (Option A)is not feasible because even low-priority tasks may be necessary for maintenance or support activities.
Including Major Functions in Low-Priority Jobs (Option B)contradicts the classification of " low-priority " because major functions are usually critical.
Allocating Optimal Resources to Low-Priority Jobs (Option C)is inefficient as resources should primarily be allocated to high-priority tasks.
Scheduling based on resource availability optimizes the use of resources, avoids unnecessary delays in high- priority activities, and ensures that low-priority tasks are executed without disrupting overall operations. This aligns with best practices in IT resource management and scheduling.

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

NEW QUESTION: 252
在一次外部評審中，資訊系統審計師發現組織口部對系統關鍵性進行分類的方法並不一致。下列哪一項應被推薦為確定係統關鍵性的首要因素？
A. 復原點目標(RPO)
B. 最大允許停機時間(MAD)
C. 平均恢復時間(MTTR)
D. 關鍵績效指標(KPI)
Answer: (SHOW ANSWER)
The primary factor to determine system criticality is the maximum allowable downtime (MAD), which is the maximum period of time that a system can be unavailable before causing significant damage or risk to the organization. TheMAD reflects the business impact and the recovery requirements of the system, and it can be used to prioritize the systems and allocate the resources for disaster recovery planning. The other options are not as important as the MAD, and they may vary depending on the system characteristics and the recovery strategy. The recovery point objective (RPO) is the maximum amount of data loss that is acceptable for a system. The mean time to restore (MTTR) is the average time required to restore a system after a failure. The key performance indicators (KPIs) are metrics that measure the performance and effectiveness of a system. References: CISA Review Manual (Digital Version) 1, page 468-469.

NEW QUESTION: 253
下列何者能為資訊系統審計專業人員提供執行審計職能的最佳指引？
A. 審計章程
B. IT指導委員會
C. 資訊安全政策
D. 審計最佳實踐
Answer: A (LEAVE A REPLY)
The audit charter is the document that defines the purpose, authority and responsibility of the IS audit function. It provides IS audit professionals with the best source of direction for performing audit functions, as it establishes the scope, objectives, reporting lines, independence, accountability and resources of the IS audit function. The IT steering committee is a governance body that oversees the strategic alignment, prioritization and direction of IT initiatives, but it does not provide specific guidance for IS audit functions. The information security policy is a document that defines the rules and principles for protecting information assets in the organization, but it does not cover all aspects of IS audit functions. Audit best practices are general guidelines and recommendations for conducting effective and efficient audits, but they are not binding or authoritative sources of

direction for IS audit functions. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.1: Audit Charter.

NEW QUESTION: 254
資訊系統審計員正在審□一家即將從瀑布式開發方法轉向敏捷開發方法的組織的系統開發實踐。由於此次轉變，下列哪一項對審計員來□最為重要？
A. 發布管理
B. 程式碼文檔
C. □能規劃
D. 安全代碼審□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 255
在審計計畫階段，資訊系統審計經理正在考慮是否將對企業認為風險較低的實體的審計納入預算。在這種情況下，下列哪一項是最佳做法？
A. 將低風險審計外包給外部審計服務提供者。
B. 對低風險商業實體進行有限範圍的審計。
C. 驗證低風險實體評級並運用專業判斷。
D. 質疑風險評級，並將低風險實體納入計畫
Answer: C (LEAVE A REPLY)
Audit planning is the process of developing an overall strategy and approach for conducting an audit. Audit planning involves identifying the objectives, scope, criteria, and methodology of the audit, as well as the resources, schedule, and reporting requirements. Audit planning also involves performing a risk assessment to identify and prioritize the areas of highest risk and significance for the audit1.
Risk assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. Risk assessment involves identifying the sources and causes of risk, analyzing the likelihood and impact of risk, and determining the level of risk and the appropriate response2.
During audit planning, the IS audit manager is considering whether to budget for audits of entities regarded by the business as having low risk. The best course of action in this situation is C. Validate the low-risk entity ratings and apply professional judgment.
This is because validating the low-risk entity ratings can help to ensure that the risk assessment is accurate, reliable, and consistent with the business objectives and expectations. Validating the low-risk entity ratings can also help to identify any changes or developments that may affect the risk profile of the entities since the last assessment.
Applying professional judgment can help to determine whether the low-risk entities should be included or excluded from the audit plan, based on factors such as materiality, relevance, significance, and assurance needs3.

NEW QUESTION: 256
下列哪一項是確定檔案伺服器所需資料保護等級的最佳資訊來源？
A. 資料分類政策與程序
B. 類似檔案伺服器的存取權限
C. 以往資料外洩事件報告
D. 可接受使用政策與隱私權聲明
Answer: A (LEAVE A REPLY)
The best source of information to determine the required level of data protection on a file server is the data classification policy and procedures, which define the criteria and methods for classifying data according to its sensitivity, value, and criticality, and specify the appropriate security measures and controls for each data category. Data classification policy and procedures help to ensure that data is protected in proportion to its importance and risk exposure. Access rights of similar file servers, previous data breach incident reports,and acceptable use policy and privacy statements are not sufficient or reliable sources of information to determine the required level of data protection on a file server, as they do not provide clear and consistent guidance on how to classify and protectdata. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Information Asset Security Framework

NEW QUESTION: 257
當一個國際組織計劃推出全球資料隱私政策時，資訊系統審計師最應該關注下列哪一項？
A. 要求可能變得不合理。
B. 該政策可能與現有的應用程式要求相衝突。
C. 地方法規可能與政策相抵觸。
D. 當地管理階層可能不接受該政策。
Answer: C (LEAVE A REPLY)
The greatest concern for an IS auditor when an international organization intends to roll out a global data privacy policy is that local regulations may contradict the policy. Data privacy regulations vary across different countries and regions, and they may impose different or conflicting requirements on how personal data can be collected, processed, stored, transferred, and disclosed. The organization should ensure that its global data privacy policy complies with the applicable local regulations in each jurisdiction where it operates,

or risk facing legal sanctions or reputational damage. Requirements may become unreasonable, but this is not a major concern for an IS auditor, as it is a business decision that should be based on a cost-benefit analysis. The policy may conflict with existing application requirements, but this is not a serious concern for an IS auditor, as it can be resolved by modifying or updating the applications to align with the policy. Local management may not accept the policy, but this is not a critical concern for an IS auditor, as it can be mitigated by providing adequate training and awareness on the policy and its benefits. References:
CISA Review Manual, 27th Edition, pages 406-4071
CISA Review Questions, Answers and ExplanationsDatabase, Question ID: 2592

NEW QUESTION: 258
資料庫安全審計中發現的下列哪一項結果會帶來最大的嚴重安全風險？
A. 歷史資料尚未清除。
B. 管理者帳號密碼未設定為過期。
C. 預設設定未更改。
D. 資料庫活動日誌記錄不完整。
Answer: B (LEAVE A REPLY)
Admin accounts typically have the highest level of privileges and access to sensitive data. If the passwords for these accounts are not set to expire, it increases the risk of unauthorized access and potential security breaches. This is especially true if an admin's credentials are compromised, as the attacker could have ongoing access to critical systems and data1.
References:
Database Auditing - Satori

NEW QUESTION: 259
下列哪一項是組織資料分類過程中最令人擔憂的問題？
A. 用於管理資料分類過程的系統不同步。
B. 資料分類流程在過去一年沒有更新。
C. 資料分類過程不符合業界標準。
D. 負責管理記錄的使用者不了解資料分類過程。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
創建資料分類程序的第一步是什麼？
A. 對資料進行分類和優先排序。
B. 開發資料流程圖。
C. 依所有者將資訊分類。
D. 制定政策。

Answer: D (LEAVE A REPLY)
The first step when creating a data classification program is to develop a policy (D). A data classification policy is a document that defines the purpose, scope, objectives, roles, responsibilities, and procedures of the data classification program. A data classification policy is essential for establishing the governance framework, standards, and guidelines for the data classification process. A data classification policy also helps to communicate the expectations and benefits of the data classification program to the stakeholders, such as data owners, users, custodians, and auditors12.
Categorizing and prioritizing data (A) is not the first step when creating a data classification program, but the third step. Categorizing and prioritizing data involves defining and applying the criteria and labels for classifying data based on its sensitivity, value, and risk. For example, data can be categorized into public, internal, confidential, or restricted levels. Categorizing and prioritizing data helps to identify and protect the most critical and sensitive data assets of the organization12.
Developing data process maps (B) is not the first step when creating a data classification program, but the fourth step. Developing data process maps involves documenting and analyzing the flow and lifecycle of data within the organization. Data process maps show how data is created, collected, stored, processed, transmitted, used, shared, archived, and disposed of. Developing data process maps helps to understand the context and dependencies of data, as well as to identify and mitigate any potential risks or issues related to data quality, security, or compliance12.
Categorizing information by owner is not the first step when creating a data classification program, but the second step. Categorizing information by owner involves assigning roles and responsibilities for each type of data based on its ownership and stewardship. Data owners are the individuals or entities that have the authority and accountability for the data. Data stewards are the individuals or entities that have the operational responsibility for managing and maintaining the data. Data custodians are the individuals or entities that have the technical responsibility for implementing and enforcing the security and access controls for the data12.
References:
7 Steps to Effective Data Classification | CDW
Data Classification: The Basics and a 6-Step Checklist - NetApp

NEW QUESTION: 261
下列哪一步是 IS 審計員在隱私權審計中最重要的一步？
A. 評估現有的資料管理控制措施。
B. 確定是否對員工進行隱私訓練。
C. 審口第三方協定以確保有足口的個人識別資訊 (PII) 保護措施。
D. 分析個人識別資訊 (PII) 資料生命週期的所有階段以識別潛在風險。
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation:

The most important step in a privacy audit is to ensure that all risks associated with PII handling are identified. This requires analyzing the entire PII data life cycle-from collection, processing, storage, and transfer to retention and destruction.
Option A: Reviewing data management controls is part of the audit but is narrower than life cycle coverage.
Option B: Privacy training is necessary, but training alone doesn't ensure compliance.
Option C: Reviewing third-party agreements is important but only covers outsourced risks.
Option D: Provides comprehensive coverage of privacy risks across all stages.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on data privacy, data life cycle, and PII risks.

NEW QUESTION: 262
在決定IT投資是否為企業帶來價口時，資訊系統審計師最應該檢視下列哪一項口容？
A. 投資報酬率(ROI)
B. 商業策略
C. 商業案例
D. 總擁有成本(TCO)
Answer: B (LEAVE A REPLY)
The answer B is correct because the most important thing for an IS auditor to review when determining whether IT investments are providing value to the business is the business strategy. The business strategy is the plan or direction that guides the organization's decisions and actions to achieve its goals and objectives.
The business strategy defines the organization's vision, mission, values, competitive advantage, target market, value proposition, and key performance indicators (KPIs).
IT investments are the expenditures or costs incurred by the organization to acquire, develop, maintain, or improve its IT assets, such as hardware, software, network, data, or services. IT investments can help the organization to support its business processes, operations, functions, and capabilities. IT investments can also help the organization to create or enhance its products, services, or solutions for its customers or stakeholders.
To determine whether IT investments are providing value to the business, an IS auditor needs to review how well the IT investments align with and contribute to the business strategy. Alignment means that the IT investments are consistent and compatible with the business strategy, and that they support and enable the achievement of the strategic goals and objectives. Contribution meansthat the IT investments are effective and efficient in delivering the expected outcomes and benefits for the business, and that they generate a positive return on investment (ROI) or value for money.
An IS auditor can use various methods or frameworks to review the alignment and contribution of IT investments to the business strategy, such as:
Balanced scorecard: A balanced scorecard is a tool that measures and monitors the performance of an organization across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help an IS auditor to evaluate

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

NEW QUESTION: 263
下列哪一項能□最大程度地保證用於從多個銷售交易資料庫編譯資料以進行預測的中間件應用程式有效運作？
A. 持續審計
B. 人工檢□
C. 異常報告
D. 自動對帳

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

NEW QUESTION: 264
在評估組織口部的資訊安全治理時，資訊安全審計員最應該關注下列哪項發現？
A. 資安部門難以填補空缺職位
B. 過去一年口未進行資訊安全治理審計。
C. 資料中心經理對安全專案擁有最終簽字權
D. 資訊安全策略每年更新。
Answer: C (LEAVE A REPLY)
The finding that should be of most concern to an IS auditor when evaluating information security governance within an organization is that the data center manager has final sign-off on security projects. This indicates a lack of segregation of duties and a potential conflict of interest between the operational and security roles. The data center manager may have access to sensitive information or systems that should be protected by security controls, or may influence or override security decisions that are not in the best interest of the organization.
This finding also suggests that there is no clear accountability or authority for information security governance at a higher level, such as senior management or board of directors. The other findings are not as concerning as this one, although they may indicate some areas for improvement or monitoring. References:
ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.11
ISACA, IT Governance Using COBIT and Val IT: Student Booklet - 2nd Edition4

NEW QUESTION: 265
在災難復原審計過程中，資訊系統審計員發現尚未進行業務影響分析(BIA)。審計員首先該做什麼？
A. 進行業務影響分析(BIA)。
B. 向管理階層提交中期報告。
C. 評估對目前災難復原能力的影響。
D. 進行額外的合規性測試。

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

NEW QUESTION: 266
在審計框架中，資訊系統審計員會檢口員工是否被允許將個人設備連接到公司電腦 審計員如何才能最好地驗證是否已採取適當的安全控制措施來防止資料遺失？
A. 進行現場巡視，口看員工插入設備傳輸機密資料的結果
B. 檢視資料遺失合規性和適用的行動裝置使用者驗收政策。
C. 驗證組織是否已正確配置資料遺失防護 (DLP) 工具。
D. 核實員工是否已接受適當的行動裝置安全意識培訓。
Answer: B (LEAVE A REPLY)
The best way to validate that appropriate security controls are in place to prevent data loss is to review compliance with data loss and applicable mobile device user acceptance policies. This will ensure that the organization has established clear rules and guidelines for employees to follow when connecting their personal devices to company-owned computers. A walk-through, a DLP tool configuration, and a security awareness training are not sufficient to validate the effectiveness of the controls, as they may not cover all possible scenarios and risks. References: IT Audit Fundamentals Certificate Resources

NEW QUESTION: 267
在製定有效的安全意識計畫時，下列何者最重要？
A. 培訓人員是資訊安全專業人員。
B. 已製定該專案的成果指標。

C. 程式口容中包含安全威脅場景。
D. 網路釣魚演練在訓練後進行。
Answer: (SHOW ANSWER)
The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization1. Outcome metrics can help ensure the effectiveness of the security awareness program by:
Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate1.
Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency1.
Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program1.

NEW QUESTION: 268
下列哪一個是影子IT的例子？
A. 員工未經IT部門批准使用基於雲端的訂單管理工具
B. 員工使用公司提供的筆記型電腦存取個人銀行訊息
C. 員工未經IT部門批准，使用個人信箱與客口溝通
D. 員工在工作時間使用公司提供的平板電腦存取社群媒體。
Answer: A (LEAVE A REPLY)
Shadow IT refers to the use of IT systems, devices, software, or services without explicit organizational approval. This often occurs when employees or departments adopt tools that bypass official IT governance structures.
Using a Cloud-Based Order Management Tool Without Approval (Option A)is a clear example of shadow IT because the employee is circumventing established IT policies to implement a solution independently.
Accessing Personal Banking Information on a Company-Provided Laptop (Option B)is a potential misuse of resources but does not qualify as shadow IT since it does not involve unauthorized technology.
Using Personal Email for Client Communication (Option C)may violate communication policies but is not related to the adoption of unapproved IT systems.
Accessing Social Media on a Company-Provided Tablet (Option D)is improper use of a company asset but does not involve unauthorized IT tools.

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

NEW QUESTION: 269
當預期總體中誤差相對較少時，下列哪一種抽樣方法是最佳選擇？
A. 變數抽樣
B. 判斷抽樣
C. 停止或繼續取樣
D. 發現性抽樣
Answer: D (LEAVE A REPLY)
Discovery sampling is a type of statistical sampling that's used when the expected error rate in the population is very low1. This method is designed to discover at least one instance of an attribute or condition in a population1. It's often used in auditing to uncover fraud or noncompliance with rules and regulations1.
References:
What are sampling methods and how do you choose the best one?

NEW QUESTION: 270
下列哪一項對於IT治理中的有效風險管理是必要的？
A. 本地管理人員全權負責風險評估。
B. IT風險管理與企業風險管理是分開的。
C. 風險管理策略已獲審計委員會批准。
D. 風險評估已融入管理流程。
Answer: D (LEAVE A REPLY)
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and ExplanationsDatabase

NEW QUESTION: 271
下列哪些口容必須作為年度審計計畫流程的一部分完成？

A. 業務連續性分析
B. 口業標竿分析
C. 風險評估
D. 風險控制矩陣
Answer: C (LEAVE A REPLY)
A risk assessment must be completed as part of annual audit planning. ISACA's ITAF-based guidance states that the IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for effective allocation of audit resources.
Option C is correct because audit planning is fundamentally risk-based under ISACA guidance. Annual planning requires identifying and prioritizing risk areas so the audit plan focuses on the areas of greatest significance. ISACA also notes that, before creating the annual audit plan, the organizationwide risk register should be reviewed thoroughly to prioritize risk areas.
Option A may inform audit planning in some organizations, but it is not a universal required planning step.
Option B can be useful, but it is optional and supplementary, not mandatory.
Option D is typically developed at the engagement level for specific audits rather than as a mandatory organizationwide annual planning deliverable.
Therefore, C is the best answer because risk assessment is the required foundation of the annual audit plan under ISACA guidance.
References (Official ISACA):
* ISACA Journal, Developing the IT Audit Plan Using COBIT 2019 - ITAF requires an appropriate risk assessment approach to develop the overall IS audit plan.
* ISACA Journal, Auditing and Digital Transformation Are at a Crossroads - before creating the annual audit plan, the organizationwide risk register should be reviewed thoroughly.
* ISACA, Certification Exam Candidate Guide - includes evaluation of audit processes and quality programs, supporting structured audit planning.

NEW QUESTION: 272
一項以資料防洩漏 (DLP) 為重點的安全審口發現，該組織無法口看儲存在雲端的資料 資訊系統審計員針對此問題提出的最佳建議是什麼？

A. 增強網路邊界的防火牆。
B. 實作檔案系統掃描器以發現儲存在雲端的資料。
C. 採用雲端存取安全代理程式(CASB)。
D. 利用桌面上的 DLP 工具監控使用者活動。
Answer: C (LEAVE A REPLY)
Here ' s the breakdown, considering
the need for DLP visibility in the cloud:
Verified Answer
C). Employ a cloud access security broker (CASB).
Very Short Explanation
CASBs are specifically designed to enhance visibility and control over cloud-based data. They can monitor data flows, enforce security policies, and often have DLP capabilities built-in, making them the ideal solution in this scenario.
References
ISACA Resources (Glossary): Definitions of Cloud Access Security Broker (CASB) highlight their role in cloud security and governance.
Industry Research (Gartner, etc.): Research on CASB tools emphasizes their ability to address visibility and control challenges for cloud data.

NEW QUESTION: 273
對一款複雜的作業排程工具的部署進行了實施後審計。下列哪一項觀察結果最令人擔憂？
A. IT 團隊透過通用帳口存取排程器管理面板。
B. 整個專案耗時比計畫的要長。
C. IT 人員在未獲得提供者批准的情況下學習自訂工具設定。
D. 調度工具中未口用資料加密設定。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 274
下列何者最能幫助組織實現其 IT 基礎架構的標準化，使其與業務目標一致？
A. 營運技術
B. 機器人流程自動化(RPA)
C. 資料架構
D. 企業架構(EA)
Answer: (SHOW ANSWER)

NEW QUESTION: 275
下列哪一項是資料遺失預防 (DLP) 機制的主要目標？
A. 增強系統效能，同時防止資料遺失
B. 自動化資料遺失復原程序，以最大限度地減少事故發生時的停機時間
C. 防止未經授權的傳輸或洩漏敏感數據

D. 確保遵守資料保護的監管要求

Answer: C (LEAVE A REPLY)

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

References (ISACA): COBIT 2019, DSS05 Managed Security Services.

NEW QUESTION: 276

當安全代碼審口作為部署程序的一部分進行時，實施了哪種類型的控制？

A. 偵探

B. 修正

C. 監控

D. 威懾

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

Secure code reviews identify security flaws or vulnerabilities in code before deployment. This makes them detective controls, since they help find issues but do not directly prevent or correct them.

Option A: Correct - they detect flaws.

Option B: Corrective controls are applied after issues are detected.

Option C: Monitoring is ongoing observation, not review-based.

Option D: Deterrent controls discourage actions (e.g., policies, warnings), not detect issues.

ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on software development controls and code review practices.

NEW QUESTION: 277

由於技術和電子記錄的進步，資訊系統審計師僅透過電子郵件完成了一項審計工作。下列哪一項資訊系統審計師可能因此受到損害？

A. 熟練度

B. 應有的專業護理

C. 充分的證據

D. 報告

Answer: (SHOW ANSWER)

Due professional care is the obligation of an IS auditor to exercise the appropriate level of skill, competence, and diligence in performing an audit. It also requires the IS auditor to comply with the relevant standards, guidelines, and ethical principles of the profession.

Completing an engagement by email only may compromise due professional care, as it may limit the IS auditor's ability to obtain sufficient and appropriate evidence, to communicate effectively with the auditee and other stakeholders, and to perform adequate quality assurance and review procedures. The other options are not as relevant as due professional care, as they relate to specific aspects of an audit, such as proficiency (the knowledge and skills of the IS auditor), sufficient evidence (the quantity and quality of the audit evidence), and reporting (the presentation and communication of the audit results). References: CISA Review Manual (Digital Version), Domain 1: The Process of Auditing Information Systems, Section 1.2 ISACA IT Audit and Assurance Standards

NEW QUESTION: 278
資訊系統審計師將透過對所有交易進行資料分析來測試應付帳款控制。在取得總體資料時，審計師最需要確認下列哪一項？
A. 數據直接取自系統。
B. 資料中不包含任何隱私資訊。
C. 可以及時取得數據。
D. 資料分析工具最近已更新。
Answer: A (LEAVE A REPLY)
The most important thing for the auditor to confirm when sourcing the population data for testing accounts payable controls by performing data analytics is that the data is taken directly from the system. Taking the data directly from the system can help ensure that the data is authentic, complete, and accurate, and that it has not been manipulated or modified by any intermediary sources or processes. The other options are not as important as taking the data directly from the system, as they do not affect the validity or reliability of the data. There is no privacy information in the data is a privacy concern that can help protect the confidentiality and integrity of personal or sensitive data, but it does not affect the accuracy or completeness of the data. The data can be obtained in a timely manner is a logistical concern that can help facilitate the efficiency and effectiveness of the data analytics process, but it does not affect the authenticity or accuracy of the data. The data analysis tools have been recently updated is a technical concern that can helpenhance the functionality and performance of the data analytics tools, but it does not affect the validity or reliability of the data. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 279
在審口組織的 IT 容量管理流程時，IS 審計師最應該關注的是容量規劃是否符合以下要求：
A. 在過去六個月口曾被審核過一次。
B. 省略了關鍵業務系統的變更。
C. 缺乏系統管理員的輸入。
D. 僅基於 IT 服務管理的輸入。

Answer: B (LEAVE A REPLY)
Capacity management must consider business changes to ensure IT resources can meet future demand. If changes to critical systems are omitted from planning, capacity forecasts will be inaccurate, leading to risks of downtime, bottlenecks, and unplanned outages. A six-month review (A) might be acceptable depending on system dynamics. Lack of administrator input (C) and reliance on service management (D) reduce planning quality but are less critical than missing major business drivers. COBIT DSS01 (Managed Operations) and APO02 (Managed Strategy) emphasize alignment between IT capacity and business requirements.
References (ISACA): COBIT 2019, DSS01 Managed Operations; APO02 Managed Strategy.

NEW QUESTION: 280
下列何者最能反映對 IT 基礎架構的有效治理？
A. 提供持續、可靠度能的能力
B. 年度安全意識計畫的要求
C. IT 基礎設施伺服器數量的增加
D. 資訊安全事件數量減少
Answer: (SHOW ANSWER)
Effective governance over IT infrastructure is indicated by the ability to deliver continuous, reliable performance12. This is because good governance ensures that IT investments support business objectives and produce measurable results towards achieving their strategies2. It involves implementing management and internal controls, strengthening security, financial controls, risk mitigation, and inspection and compliance obligations3. While security awareness programs, the number of servers, and the number of security incidents can be aspects of IT governance, they are not the best indicators of its effectiveness.
References:
The Value of IT Governance - ISACA
What is IT governance? A formal way to align IT and business strategy | CIO Robust Governance - KPMG Global

NEW QUESTION: 281
某組織希望根據其資料分類方案對資料庫表進行分類。從資訊系統審計員的角度來看，表應基於以下幾點進行分類：
A. 表的更新頻率。
B. 每個表格的具體功能口容。
C. 有權存取該表的最終使用者數量。
D. 表中列名稱的描述。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 282
在下列哪一種抽樣方法中，如果發現一個錯誤，則整個樣本都被認為是不規則的？
A. 發現性抽樣
B. 變數抽樣
C. 停止或繼續取樣
D. 判斷抽樣
Answer: A (LEAVE A REPLY)
The sampling method in which the entire sample is considered to be irregular if a single error is found is discovery sampling. Discovery sampling is a type of statistical sampling that is used to test for the existence of at least one occurrence of a specific characteristic or condition in a population. Discovery sampling is often used when the auditor expects the characteristic or condition to be very rare or nonexistent, and when any occurrence would have a significant impact on the audit objective. For example, discovery sampling can be used to test for fraud, noncompliance, or material misstatement.
Discovery sampling works by setting a very low tolerable error rate (the maximum rate of occurrence of the characteristic or condition that the auditor is willing to accept) and a high confidence level (the degree of assurance that the auditor wants to obtain). The auditor then selects a sample from the population using a random or systematic method, and examines each item in the sample for the presence or absence of the characteristic or condition. If no error is found in the sample, the auditor can conclude with a high level of confidence that the characteristic or condition does not exist or is very rare in the population. However, if one or more errors are found in the sample, the auditor cannot draw any conclusion about the population and must either expand the sample size or perform alternative procedures.
Discovery sampling differs from other sampling methods in that it does not allow for any errors in the sample.
Other sampling methods, such as variable sampling, stop-or-go sampling, or judgmental sampling, can tolerate some errors in the sample and use them to estimate the error rate or amount in the population.
However, discovery sampling is designed to test for zero-tolerance situations, where any error would be unacceptable or material. Therefore, discovery sampling considers the entire sample to be irregular if a single error is found.
References:
Audit Sampling - Overview, Purpose, Importance, and Types1
Audit Sampling - What Is It, Methods, Example, Advantage, Reason2
ISA 530: Audit sampling | ICAEW3
Audit Sampling - AICPA4

NEW QUESTION: 283
下列何者最能確保審計分析中所使用的測試程序的品質和完整性？

A. 向審計團隊開發並傳達測試流程最佳實踐
B. 開發和實施審計資料儲存庫
C. 分散程序並實施定期同儕審口
D. 集中化流程並實施變更控制
Answer: D (LEAVE A REPLY)
The best way to ensure the quality and integrity of test procedures used in audit analytics is to centralize procedures and implement change control. Centralizing procedures means storing themin a common repository that can be accessed and updated by authorized users. Change control means implementing a process for tracking, reviewing, approving, and documenting any changes made to the procedures. This ensures that the procedures are consistent, accurate, reliable, and secure. References: CISA Review Manual, 27th Edition, page 401

NEW QUESTION: 284
下列哪一項是與虛擬化相關的擔憂？
A. 伺服器在資料中心口的實體佔地面積可能會減少。
B. 主機效能問題可能會影響客口作業系統。
C. 處理能力可以在多個作業系統之間共用。
D. 一台主機可以有多個相同作業系統的版本。
Answer: B (LEAVE A REPLY)
A concern associated with virtualization is that performance issues with the host could impact the guest operating systems, which are the operating systems that run on virtual machines within the host. For example, if the host has insufficient memory, CPU, disk space, or network bandwidth, it could affect the performance and availability of the guest operating systems and the applications running on them. The physical footprint of servers could decrease within the datacenter, processingcapacity may be shared across multiple operating systems, and one host may have multiple versions of the same operating system are not concerns associated with virtualization, but rather benefits or features of virtualization that can help reduce costs, improve efficiency, and enhance flexibility. References: CISA Review Manual (Digital Version), Chapter 4:
Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support

NEW QUESTION: 285
雲端存取安全代理 (CASB) 代表客口組織管理軟體即服務 (SaaS) 的使用者存取權限。在對該服務進行審計時，資訊系統審計員最需要確認下列哪一項？
A. CASB 在授予存取權限之前，會驗證來自指定客口聯絡人的存取請求。
B. CASB 定期對存取請求進行審計，以確保符合客口政策。
C. CASB 將存取請求記錄為服務記錄，並在授予存取權限後進行審核。
D. CASB 管理對 SaaS 應用程式所使用的聯合目錄服務的安全存取。

Answer: D (LEAVE A REPLY)

NEW QUESTION: 286
下列哪一項出現在組織的可接受使用政策中的敘述最能反映其與資訊資口保護相關的資料分類標準的一致性？
A. 任何透過公共網路傳輸的資訊資口都必須經過高階主管的批准。
B. 所有資訊資口在組織系統中儲存時必須加密。
C. 資訊資口只能由有正當理由的人員存取。
D. 所有資訊資口將被分配一個明確定義的級別，以便於員工妥善處理
Answer: B (LEAVE A REPLY)
The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively12.
References:
1. IFRC. "Information Security: Acceptable Use Policy."
1(https://www.ifrc.org/sites/default/files/2021-11
/IFRC-Information-Security-Acceptable-Use-Policy.pdf)
2. UNSW Sydney. "Data Classification Standard."
2(https://www.unsw.edu.au/content/dam/pdfs/governance
/policy/2022-01-policies/datastandard.pdf)
3. Digital Guardian. "What is a Data Classification Policy?"
3(https://www.digitalguardian.com/blog/what- data-classification-policy)
4. Microsoft Service Trust Portal. "Data classification and sensitivity label taxonomy."
4(https://learn.
microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-labels)
5. Clark University ITS Policies. "Data Classification - Data Security Policies."
5(https://www2.clarku.edu
/offices/its/policies/data_classification.cfm)

NEW QUESTION: 287
為了提出有意義的建議或發現問題，資訊系統審計師需要確定並瞭解下列哪一項最為重要？
A. 根本原因
B. 責任方
C. 影響
D. 標準
Answer: (SHOW ANSWER)
Root cause is the most important thing for an IS auditor to determine and understand to develop meaningful recommendations for findings. A root cause is the underlying factor or condition that leads to a problem or issue. A finding is a statement that describes a problem or issue identified during an audit. A recommendation is a suggestion or advice that aims to address or resolve a finding. To develop meaningful recommendations for findings, an IS auditor should determine and understand the root cause of each finding, as this can help to identify the most effective and appropriate actions to prevent or correct the problem or issue. The other options are not as important as determining and understanding the root cause, as they do not directly address or resolve the finding.
References: CISA Review Manual, 27th Edition, page 434

NEW QUESTION: 288
在審口IT戰略計劃時，資訊系統審計員應考慮該計劃是否明確指出：
A. IT人員分配。
B. 使用的專案管理方法。
C. 重大 IT 計劃。
D. 連結到作戰戰術計畫。
Answer: C (LEAVE A REPLY)
In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the major IT initiatives that are aligned with the organization's vision, mission, and objectives, and that support the business strategy and priorities12. The major IT initiatives should also be realistic, measurable, and achievable, and should have clear timelines, budgets, and responsibilities34.
References
1: IT Strategy Template for a Successful Strategic Plan | Gartner2 2: IT Strategy Template for a Successful Strategic Plan | Gartner4 3: Conduct a Strategic Plan Review and Assessment - Governance3 4: Time To Conduct A Strategy Review? Here's How To Get Started1

NEW QUESTION: 289

一位經理發現了一些屬於已離職員工的活躍特權帳口。在這種情況下，下列哪一項是威脅行為者？

A. 已離職員工

B. 未經授權的訪問

C. 已刪除日誌數據

D. 駭客行動主義者

Answer: A (LEAVE A REPLY)

A threat actor is an entity or individual that poses a potential harm or danger to an organization's information systems or data. Terminated staff are the threat actors in this scenario, as they are former employees who may still have active privileged accounts that grant them access to sensitive or critical information or resources of the organization. Terminated staff may abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of the information systems or data, either intentionally or unintentionally. Unauthorized access is a threat event or action that occurs when an unauthorized entity or individual gains access to an organization's information systems or data without permission or authorization.

Unauthorized access is not a threat actor, but rather a result of a threat actor's activity. Deleted log data is a threat consequence or impact that occurs when log data, which are records of events or activities that occur on an information system or network, are erased or corrupted by a threat actor. Deleted log data can affect the auditability, accountability, and visibility of the information system or network, and prevent detection or investigation of security incidents. Deleted log data is not a threat actor, but rather a result of a threat actor's activity. Hacktivists are threat actors who use hacking techniques to promote a political or social cause or agenda. Hacktivists are not the threat actors in this scenario, as there is no indication that they are involved in this case.

NEW QUESTION: 290

資訊系統審計員已完成網路安全審口的現場工作階段，正在準備初步報告，下列哪些發現應被列為最高風險？

A. 未執行網路滲透測試。

B. 網路防火牆策略尚未獲得資安官的批准。

C. 網路防火牆規則尚未記錄。

D. 網路設備清單不完整。

Answer: (SHOW ANSWER)

The finding that should be ranked as the highest risk is that network penetration tests are not performed.

Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices.

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

NEW QUESTION: 291
下列哪一項是實體存取預防控制措施的例子？
A. 記錄所有建築物訪客的資料。
B. 為建築物實施基於指紋的門禁系統
C. 在所有出入口安裝閉路電視(CCTV)攝影機
D. 實施集中式日誌伺服器，以記錄員工登入工作站的實例
Answer: B (LEAVE A REPLY)
A preventive control is a control that aims to deter or prevent undesirable events from occurring. A fingerprint-based access control system for the building is an example of a preventive control for physical access, as it restricts unauthorized persons from entering the premises. Keeping log entries for all visitors to the building, installing CCTV cameras for all ingress and egress points, and implementing a centralized logging server to record instances of staff logging into workstations are examples of detective controls, which are controls that aim to discover or detect undesirable events that have already occurred. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 292
在實施新應用程式系統期間，審計人員在審口資料轉換和遷移時，下列哪一項最應引起他們的注意？
A. 變更管理流程沒有正式的文件記錄。
B. 舊系統和資料的備份無法在線上取得。
C. 轉換過程中發生了未經授權的資料修改，
D. 資料轉換採人工方式完成。
Answer: (SHOW ANSWER)
The finding that should be of greatest concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system is that unauthorized data modificationsoccurred during conversion. Data conversion and migration is a process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. Unauthorized data modifications during conversion

can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Unauthorized data modifications can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The IS auditor should verify that adequate controls are in place to prevent, detect, and correct unauthorized data modifications during conversion, such as access control, data validation, reconciliation, audit trail, and backup and recovery. The other findings (A, B and D) are less concerning, as they can be mitigated by documenting the change management process, restoring the backups of the old system and data from offline storage, or automating the data conversion process. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.4:
System Implementation

NEW QUESTION: 293
審口資料庫安全性的資訊系統審計師最應該關注的是資料庫管理員 (DBA) 是否符合以下情況：
A. 執行恢復程序。
B. 解決資料庫鎖定。
C. 評估資料庫效能。
D. 核准存取角色。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 294
在製定基於風險的審計策略時，資訊系統審計師最應該關注的領域是什麼？
A. 關鍵業務應用程式
B. 業務流程
C. 現有IT控制
D. 近期審計結果
Answer: (SHOW ANSWER)
This is because the business processes are the core activities and functions that enable the organization to achieve its objectives and create value for its stakeholders. The business processes are also the sources and drivers of various risks that may affect the organization's performance, compliance, and reputation. Therefore, the IS auditor should focus on understanding, assessing, and prioritizing the business processes that are most critical, complex, or vulnerable to the organization's success, and align the audit objectives, scope, and resources accordingly12.
Critical business applications (A) are not the most important area of focus for an IS auditor when developing a risk-based audit strategy, but rather a specific aspect of the business processes that may require attention.
Critical business applications are the software systems that support the execution and automation of the business processes, such as enterprise resource planning (ERP),

customer relationship management (CRM), or accounting systems. Critical business applications may pose significant risks to the organization if they are not reliable, secure, or efficient. Therefore, the IS auditor should consider the criticality, functionality, and dependency of the business applications when planning the audit, but not as the primary focus12.
Existing IT controls are not the most important area of focus for an IS auditor when developing a risk- based audit strategy, but rather an outcome or output of the risk assessment process. Existing IT controls are the policies, procedures, practices, and technologies that are implemented to manage and mitigate the IT- related risks that may affect the organization's business processes and objectives. Existing IT controls may vary in their design, effectiveness, and maturity. Therefore, the IS auditor should evaluate and testthe existing IT controls as part of the audit execution and reporting process, but not as the main focus12.
Recent audit results (D) are not the most important area of focus for an IS auditor when developing a risk- based audit strategy, but rather an input or source of information for the risk assessment process. Recent audit results are the findings, recommendations, and opinions of previous audits that may provide insights or feedback on the organization's business processes, risks, and controls. Recent audit results may also indicate any changes or trends in the organization's risk profile or environment. Therefore, the IS auditor should review and consider the recent audit results as part of the audit planning and scoping process, but not as the main focus12.

NEW QUESTION: 295
誰是設計 IT 控制措施以實現控制目標的主要責任人？
A. 口部稽核員
B. 企業管理
C. ITC經理
D. 風險管理
Answer: C (LEAVE A REPLY)

NEW QUESTION: 296
實施資訊科技治理架構要求組織的董事會：
A. 解決技術性 IT 問題。
B. 了解所有 IT 措施。
C. 成立一個IT策略委員會。
D. 批准 IT 策略。
Answer: (SHOW ANSWER)
IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. The board of directors of an organization is ultimately accountable for IT governance and has the authority to approve the IT strategy. The board of directors does not need to address technical IT issues, be informed of all IT

initiatives, or have an IT strategy committee, as these tasks can be delegated to other stakeholders or committees within the organization.

NEW QUESTION: 297
資訊系統審計員在審口組織對新隱私立法的回應時，首先應該評估什麼？
A. 限制收集個人資訊的實施計劃
B. 其他國家的隱私法例可能包含類似要求
C. 實現遵守法律法規的營運計劃
D. 包含隱私組件的系統分析
Answer: D (LEAVE A REPLY)
The first thing that an IS auditor should evaluate when reviewing an organization's response to new privacy legislation is the analysis of systems that contain privacy components. Privacy components are elements of a system that collect, process, store, or transmit personal information that is subject to privacy legislation. An analysis of systems that contain privacy components should identify what types of personal information are involved, where they are located, how they are used, who has access to them, and what risks or threats they face. An analysis of systems that contain privacy components is essential for determining the scope and impact of the new privacy legislation on the organization's systems and processes.
The other options are not as important as option D. An implementation plan for restricting the collection of personal information is a possible action, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An implementation plan for restricting the collection of personal information is a document that outlines how an organization will comply with the principle of data minimization, which states that personal information should be collected only for specific and legitimate purposes and only to the extent necessary for those purposes. An implementation plan for restricting the collection of personal information should be based on an analysis of systems that contain privacy components.
Privacy legislation in other countries that may contain similar requirements is a possible source of reference, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation.
Privacy legislation in other countries that may contain similar requirements is a set of laws or regulations that governs the protection of personal information in other jurisdictions that may have comparable or compatible standards or expectations as the new privacy legislation. Privacy legislation in other countries that may contain similar requirements may provide guidance or best practices for complying with the new privacy legislation. However, privacy legislation in other countries that may contain similar requirements should not be used as a substitute foran analysis of systems that contain privacy components. An operational plan for achieving compliance with the legislation is a possible deliverable, but not the first thing to evaluate, when reviewing an organization's response to new privacy legislation. An operational plan for achieving compliance with the legislation is a document

that describes how an organization will implement and maintain the necessary policies, procedures, controls, and measures to comply with the new privacy legislation. An operational plan for achieving compliance with the legislation should be derived from an analysis of systems that contain privacy components. References: Privacy law - Wikipedia, Data Protection and Privacy Legislation Worldwide | UNCTAD, Data minimization - Wikipedia

NEW QUESTION: 298
在審口硬碟利用率報告時，資訊系統審計員發現利用率通常高於95%。
下列哪一項應該是資訊系統審計師最該關注的問題？
A. 拒口服務 (DoS) 攻擊
B. 資料安全
C. 可用性
D. 一致性
Answer: (SHOW ANSWER)

NEW QUESTION: 299
某組織的安全團隊創造了一個包含多個存在漏洞應用程式的模擬生口環境。創造這樣一個環境的主要目的是什麼？
A. 收集網路攻擊的數位證據
B. 吸引攻擊者以便研究其行為
C. 為安全經理提供培訓
D. 測試入侵偵測系統(IDS)
Answer: B (LEAVE A REPLY)
The primary purpose of creating a simulated production environment with multiple vulnerable applications is to attract attackers in order to study their behavior. This is a technique known as honeypotting, which is a form of deception security that lures attackers into a fake system or network that mimics the real one, but is isolated and monitored1. Honeypotting can help security teams to learn about the attackers' methods, tools, motives, and targets, and to collect valuable intelligence that can be used to improve the security posture of the organization1. Honeypotting can also help to divert the attackers' attention from the real assets and to waste their time and resources2.
The other options are not the primary purpose of creating a simulated production environment with multiple vulnerable applications. To collect digital evidence of cyberattacks, security teams would need to use forensic tools and techniques that can preserve and analyze the data from the compromised systems or networks3. To provide training to security managers, security teams would need to use simulation tools and scenarios that can test and enhance their skills and knowledge in responding to cyber incidents4. To test the intrusion detection system (IDS), security teams would need to use penetration testing tools and methods that can evaluate the effectiveness and performance of the IDS in detecting and preventing malicious activities5.

References:
What is a Honeypot? | Imperva
Honeypots: A sweet solution for identifying intruders | CSO Online
Digital Forensics - an overview | ScienceDirect Topics
Cybersecurity Training and Exercises - Homeland Security
What is Penetration Testing? | Types and Stages | Imperva

NEW QUESTION: 300
在評估控制措施的有效性時，下列何者對資訊系統審計師最有幫助？
A. 控制自我評估(CSA)
B. 控制測試結果
C. 管理階層訪談
D. 控制矩陣
Answer: B (LEAVE A REPLY)
The most helpful thing for an IS auditor when assessing the effectiveness of controls is the results of control testing, as this provides objective and reliable evidence of how well the controls are designed and operating in practice. A control self-assessment (CSA) is a technique that involves the participation of process owners and stakeholders in evaluating the effectiveness of controls, but it may not be as rigorous or independent as control testing. Interviews with management are useful for gaining an understanding of the control environment and culture, but they may not reflect the actual performance of controls. A control matrix is a tool that maps the controls to the objectives, risks, and requirements, but it does not measure the effectiveness of controls. References: CISA Review Manual (Digital Version),Chapter 1: Information Systems Auditing Process, Section 1.3: IT Audit Process

NEW QUESTION: 301
下列哪一種測試方法最適合評估系統在進行變更後是否保持了完整性？
A. 迴歸測試
B. 單元測試
C. 整合測試
D. 驗收測試
Answer: A (LEAVE A REPLY)
Regression testing is the most appropriate testing method for assessing whether system integrity has been maintained after changes have been made. Regression testing is a type of software testing that ensures that previously developed and tested software still performs as expected after a change1 Regression testing helps to detectany defects or errors that may have been introduced or uncovered due to the change2 Regression testing can be performed at different levels of testing, such as unit, integration, system, and acceptance3 Unit testing is a type of software testing that verifies the functionality of individual components or units of code. Unit testing is usually performed by developers

before integrating the code with other components. Unit testing helps to identify and fix errors at an early stage of development, but it does not ensure that the system as a whole works as expected after a change.
Integration testing is a type of software testing that verifies the functionality, performance, and reliability of the interactions between different components or units of code. Integration testing is usually performed after unit testing and before system testing. Integration testing helps to identify and fix errors that may occur when different components are integrated, but it does not ensure that the system as a whole works as expected after a change.
Acceptance testing is a type of software testing that verifies whether the system meets the user requirements and expectations. Acceptance testing is usually performed by end-users or customersafter system testing and before deploying the system to production. Acceptance testing helps to ensure that the system delivers the desired value and quality to the users, but it does not ensure that the system as a whole works as expected after a change.
References: 1: What is Regression Testing? Test Cases (Example) - Guru99 2: What is Regression Testing? Definition, Tools, Examples - Katalon 3: Regression testing - Wikipedia : What is Unit Testing?
Definition, Types, Tools and Examples - Guru99 : What is Integration Testing? Definition, Types, Tools and Examples - Guru99 : What is Acceptance Testing? Definition, Types, Tools and Examples - Guru99

NEW QUESTION: 302
資訊系統審計員建議管理階層在將新系統投入生口環境之前進行測試。管理層制定測試計劃的最佳方法是使用以下處理參數：
A. 由測試口生器隨機選擇。
B. 由應用程式供應商提供。
C. 由使用者隨機選擇。
D. 由生口實體和客口模擬。
Answer: D (LEAVE A REPLY)
The best approach for management in developing a test plan is to use processing parameters that are simulated by production entities and customers. This is because using realistic data and scenarios can help to evaluate the functionality, performance, reliability,

and security of the new system under actual operating conditions and expectations. Using processing parameters that are randomly selected by a test generator, provided by the vendor of the application, or randomly selected by the user may not be sufficient or representative of the production environment and may not reveal all the potential issues or defects of the new system. References: [ISACA CISA Review Manual 27th Edition], page 266.

NEW QUESTION: 303
下列何者最能及時辨識風險暴露？
A. 外部審計審□
B. □部稽核審□
C. 控制自我評估(CSA)
D. 壓力測試
Answer: C (LEAVE A REPLY)
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not have as much insight into the business operations and environment. References: ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION: 304
審計章程包含下列哪些□容？
A. 制定年度審計計劃的過程
B. 賦予稽核功能的權限
C. 審計人員所需培訓
D. 審計目標與範圍
Answer: B (LEAVE A REPLY)
The authority given to the audit function is one of the components that is found in an audit charter. According to the IIA, the audit charter is a formal document that defines internal audit's purpose, authority, responsibility and position within the organization1. The authority given to the audit function includes the scope of its activities, the access to records, personnel and physical properties relevant to its work, and the independence and objectivity of its staff2. The authority given to the audit function helps to ensure that internal auditors can perform their duties effectively and efficiently, and that they can provide assurance and consulting services that add value and improve the organization's operations3.

The other options are not found in an audit charter. The process of developing the annual audit plan is not part of the audit charter, but rather a separate document that outlines the methodology, criteria and resources for selecting and prioritizing audit engagements based on a risk assessment4. Required training for audit staff is not part of the audit charter, but rather a component of the quality assurance and improvement program that evaluates the competence and performance of internal auditors and provides them with opportunities for professional development5. Audit objectives and scope are not part of the audit charter, but rather specific elements of each individual audit engagement that define the expected outcomes and the boundaries of the audit work.

NEW QUESTION: 305
下列哪一項是確保應用程式依照其規範運作的最佳方法？
A. 單元測試
B. 試點測試
C. 系統測試
D. 整合測試
Answer: D (LEAVE A REPLY)
Integration testing is the best way to ensure that an application is performing according to its specifications, because it tests the interaction and compatibility of different modules or components of the application. Unit testing, pilot testing and system testing are also important, but they do not cover the whole functionality and integration of the application as well as integration testing does. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION: 306
資訊系統審計員想要確定誰負責監督執行特定任務的員工，並參考了組織的RACI 矩陣圖。矩陣圖中的下列哪個角色可以提供此資訊？
A. 已諮詢
B. 知情
C. 負責
D. 負責
Answer: (SHOW ANSWER)
The role within the RACI chart that would provide information on who has oversight of staff performing a specific task is accountable. A RACI chart is a matrix that defines and assigns the roles and responsibilities of different stakeholders for a project, process, or activity. RACI stands for responsible, accountable, consulted, and informed. Accountable is the role that has the authority and oversight to approve or reject the work done by the responsible role. The other options are not the roles that provide information on who has oversight of staff performing a specific task, as they have different meanings and functions. Consulted is the role that provides input or advice to the responsible or accountable roles. Informed is the role that receives updates or reports from the responsible or accountable

roles. Responsible is the role that performs or executes the work or task. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 307
在審口組織的安全資訊和事件管理 (SIEM) 解決方案時，下列哪一項最令人關注？
A. SIEM 報告是可自訂的。
B. SIEM 配置每年審核一次
C. SIEM 是去中心化的。
D. SIEM 報告是臨時性的。
Answer: C (LEAVE A REPLY)
The greatest concern that the IS auditor should have when reviewing an organization's security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization. The other findings are not as concerning as a decentralized SIEM, because they can be addressedby implementing best practices and standards for SIEM reporting and configuration. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 308
在容易出現電力意外激增的地區，下列哪一項措施能最有效保護電力系統？
A. 斷路器
B. 穩壓器
C. 備用電源線
D. 生成器
Answer: B (LEAVE A REPLY)

NEW QUESTION: 309
在向管理階層傳達資訊系統審計問題時，下列哪一項應是重點？
A. 組織因該問題而面臨的風險
B. 解決此問題的詳細方案
C. 後續審計跟進的性質、範圍和時間安排
D. 問題是如何發現的以及誰應為此負責
Answer: A (LEAVE A REPLY)

NEW QUESTION: 310
下列哪一項應作為確定 IT 專案和計畫優先順序的主要依據？
A. 可用資源
B. 風險降低程度
C. 預期業務價口
D. 預計成本和時間
Answer: C (LEAVE A REPLY)

NEW QUESTION: 311
在安排後續審計時，下列何者最重要？
A. 與新審計師進行獨立核口所需的工作量
B. 如果不採取糾正措施，其影響將是什麼？
C. 受審計單位同意與審計人員共處的時間量
D. 與觀測相關的控制與偵測風險
Answer: (SHOW ANSWER)
The impact if corrective actions are not taken is the most important factor to consider when scheduling follow- up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:
CISA Review Manual(Digital Version), Chapter 2, Section 2.5.31
CISA Review Questions, Answers and Explanations Database, Question ID 207

NEW QUESTION: 312
為了確認雜湊訊息的完整性，接收方應使用：
A. 使用與發送方相同的雜湊演算法來建立檔案的二進位影像。
B. 使用與發送方不同的雜湊演算法來建立檔案的二進位影像。
C. 使用與發送方相同的雜湊演算法來建立檔案的數口表示。
D. 與發送方不同的雜湊演算法，用於建立檔案的數口表示。
Answer: C (LEAVE A REPLY)
To confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender' s to create a binary image of the file. A hashing algorithm is a mathematical function that transforms an input data into a fixed-length output value, called a hash or a digest. A hashing algorithm has two main properties:
it is one-way, meaning that it is easy to compute the hash from the input, but hard to recover the input from the hash; and it is collision-resistant, meaning that it is very unlikely to find two different inputs that produce the same hash. These properties make hashing algorithms useful for verifying the integrity of data, as any change in the input data will result in a different hash value. Therefore, to confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender's to create a binary image

of the file, which is a representation of the file in bits (0s and 1s). The receiver should then compare this binary image with the hash value sent by the sender. If they match, then the message has not been altered in transit.
If they do not match, then the message has been corrupted or tampered with.
References:
Ensuring Data Integrity with Hash Codes
Message Integrity

NEW QUESTION: 313
下列哪一項是確保新的 IT 實施符合企業架構 (EA) 原則和要求的最佳方法？
A. 將安全性檢視記錄為企業架構的一部分。
B. 在定義企業架構時，應考慮利害關係人的關切
C. 對IT實施進行強制性實施後審口
D. 作為變革諮詢委員會的一部分，進行企業架構審口
Answer: (SHOW ANSWER)
The best way to help ensure new IT implementations align with enterprise architecture (EA) principles and requirements is to conduct EA reviews as part of the change advisory board (CAB). A CAB is a committee that evaluates and authorizes changes to IT services, such as new IT implementations. By conducting EA reviews as part of the CAB process, the organization can ensure that the proposed changes are consistent with the EA vision, goals, standards, and guidelines. This can help avoid potential conflicts, risks, or inefficiencies that may arise from misaligned IT implementations. Additionally, EA reviews can help identify opportunities for improvement, optimization, or innovation in the IT services.
The other options are not the best ways to help ensure new IT implementations align with EA principles and requirements. Documenting the security view as part of the EA is important, but it does not guarantee that new IT implementations will follow the security requirements or best practices. Considering stakeholder concerns when defining the EA is also essential, but it does not ensure that new IT implementations will meet the stakeholder expectations or needs. Performing mandatory post-implementation reviews of IT implementations is a good practice, but it does not prevent potential issues or problems that may arise from misaligned IT implementations.
References:
5: Change Advisory Board Best Practices: 15+ Industry Leaders Weigh In
6: What Does the Change Advisory Board (CAB) Do?
7: How do I set up an effective change advisory board? - ServiceNow
8: ITIL Change Management - The Role of the Change Advisory Board

NEW QUESTION: 314
有效實施適當的資料分類的主要好處是什麼？
A. 滿足業務需求的能力

B. 提高敏感資料的準確性
C. 敏感資料業務風險管理
D. 確保敏感資料加密。
Answer: (SHOW ANSWER)

NEW QUESTION: 315
資訊系統審計員正在審口最近發生的一起安全事件，並尋求有關最近對資料庫系統安全設定進行修改的批准資訊。審計員最有可能在哪裡找到這些資訊？
A. 系統事件關聯報告
B. 資料庫日誌
C. 變更日誌
D. 安全事件與事件管理 (SIEM) 報告
Answer: (SHOW ANSWER)
A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system's security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

NEW QUESTION: 316
下列哪一個群體主要負責建立有利於有效和有效率的口部控制系統的文化？
A. 人力資源
B. 高階管理層
C. 直線管理
D. 口部稽核
Answer: (SHOW ANSWER)
The best answer is B. Senior management.
The culture that supports an effective internal control system is set from the top. ISACA's governance and culture guidance consistently treats culture as a management and leadership responsibility. Senior leadership establishes tone, values, expectations, accountability, and behavioral norms that shape how controls are designed, followed, and enforced across the enterprise. A strong control culture depends on visible commitment from leadership, not just procedural ownership by operational teams.
Option A. HR supports the culture through hiring, training, and policy reinforcement, but HR does not have primary accountability for the overall control environment.
Option C. Line management plays an important role in day-to-day control execution, but enterprise culture is primarily driven by senior leadership.

Option D. Internal audit evaluates and provides assurance over the control system; it does not own or establish the control culture because doing so would impair independence. Therefore, B is the correct answer because senior management is primarily accountable for establishing the tone and culture that enable an effective and efficient internal control system.
References (Official ISACA):
* ISACA Journal, Auditing Your Organizational Culture.
* ISACA Now Blog, Culture as a Corporate Asset.
* ISACA Digital Video/Podcast, Understanding and Assessing Organization Culture.
* ISACA Journal, Auditing Culture.

NEW QUESTION: 317
在對網路設備管理進行審計時，資訊系統審計員最需要驗證下列哪一項？
A. 無法透過服務帳口存取裝置。
B. 備份策略包含裝置設定檔。
C. 所有裝置均已評估目前安全性修補程式。
D. 所有裝置均位於受保護的網路段口。
Answer: C (LEAVE A REPLY)
The most important thing for an IS auditor to validate when auditing network device management is that all devices have current security patches assessed. This is because security patches are essential for fixing known vulnerabilities and preventing unauthorized access, data breaches, or denial-of-service attacks on the network devices. If the network devices are not patched regularly, they may expose the network to various cyber threats and compromise the confidentiality, integrity, and availability of the network services and data12.
Devices cannot be accessed through service accounts is not the most important thing to validate because service accounts are typically used for automated tasks or processes that require privileged access to network devices. Service accounts can be secured by using strong passwords, limiting their permissions, and monitoring their activities. However, service accounts alone do not protect the network devices from external or internal attacks that exploit unpatched vulnerabilities3.

Backup policies include device configuration files is not the most important thing to validate because backup policies are mainly used for restoring the network devices in case of failure, disaster, or corruption. Backup policies can help with recovering the network functionality and data, but they do not prevent the network devices from being compromised or attacked in the first place. Backup policies should be complemented by security policies that ensure the network devices are patched and protected4.
All devices are located within a protected network segment is not the most important thing to validate because network segmentation is a technique that divides the network into smaller subnets or zones based on different criteria, such as function, security level, or access control. Network segmentation can help isolate and contain the impact of a potential attack on a network device, but it does not prevent the attack from happening. Network segmentation should be combined with security patching and other security measures to ensure the network devices are secure.

NEW QUESTION: 318
資訊系統審計員發現，為了提高效能,Web應用程式的驗證控制已從伺服器端移至瀏覽器端。這極有可能增加遭受攻擊成功的風險。
A. 網路釣魚。
B. 拒口服務(DoS)
C. 結構化口詢語言(SQL)注入
D. 緩衝區溢位
Answer: (SHOW ANSWER)
Moving validation controls from the server side into the browser would most likely increase the risk of a successful attack by structured query language (SQL) injection. SQL injection is a technique that exploits a security vulnerability in an application's database layer by inserting malicious SQL statements into user input fields. Validation controls are used to check and filter user input before sending it to the database. If these controls are moved to the browser, they can be easily bypassed or modified by an attacker, who can then execute arbitrary SQL commands on the database. References: CISA Review Manual, 27th Edition, page 361

NEW QUESTION: 319
為大型組織開發資料遺失防護 (DLP) 解決方案時，下列哪一項應該是第一步？
A. 進行資料清點與分類工作。
B. 識別企業範圍口已核准的資料工作流程
C. 對敏感資料使用進行威脅分析。
D. 建立 DLP 策略和模板
Answer: A (LEAVE A REPLY)
The first step when developing a DLP solution for a large organization is to conduct a data inventory and classification exercise. This step involves identifying and locating all the data

assets that the organization owns, generates, or handles, and assigning them to different categories based on their sensitivity, value, and regulatory requirements1. Data inventory and classification is essential for DLP because it helps to determine the scope and objectives of the DLP solution, as well as the appropriate level of protection and monitoring for each data category2. Data inventory and classification also enables the organization to prioritize its DLP efforts based on the risk and impact of data loss or leakage3.
Option B is not correct because identifying approved data workflows across the enterprise is a subsequent step after conducting data inventory and classification. Data workflows are the processes and channels through which data are created, stored, accessed, shared, or transmitted within or outside the organization4. Identifying approved data workflows helps to define the normal and legitimate use of data, as well as to detect and prevent unauthorized or anomalous data activities5. However, before identifying approved data workflows, the organization needs to know what data it has and how it should be classified.
Option C is not correct because conducting a threat analysis against sensitive data usage is another subsequent step after conducting data inventory and classification. Threat analysis is the process of identifying and assessing the potential sources, methods, and impacts of data loss or leakage incidents. Threat analysis helps to design and implement effective DLP controls and countermeasures based on the risk profile of each data category. However, before conducting threat analysis, the organization needs to know what data it has and how it should be classified.
Option D is not correct because creating the DLP policies and templates is the final step after conducting data inventory and classification, identifying approved data workflows, and conducting threat analysis. DLP policies and templates are the rules and configurations that specify how the DLP solution should monitor, detect, report, and respond to data loss or leakage events. DLP policies and templates should be aligned with the organization's business needs, regulatory obligations, and risk appetite. However, before creating the DLP policies and templates, the organization needs to know what data it has, how it should be classified, how it should be used, and what threats it faces.
References:
Data Inventory and Classification: The First Step in Data Protection1
Data Classification: What It Is And Why You Need It2
How to Prioritize Your Data Loss Prevention Strategy in 20203
What Is Data Workflow? Definition and Examples4
How to Identify Data Workflows for Your Business5
Threat Analysis: A Comprehensive Guide for Beginners
How to Conduct a Threat Assessment for Your Business
What Is Data Loss Prevention (DLP)? Definition and Examples
How to Create Effective Data Loss Prevention Policies

NEW QUESTION: 320
對於評估組織設計的資訊系統審計師而言，下列何者最為重要？

的事件管理流程？
A. 未遵循服務管理標準。
B. 未指定解決事件的預期時間。
C. 指標不會向高階主管報告。
D. 優先權標準未定義。
Answer: (SHOW ANSWER)
he design of an incident management process should include prioritization criteria to ensure that incidents are handled according to their impact and urgency. Without prioritization criteria, the organization may not be able to allocate resources effectively and respond to incidents in a timely manner. Expected time to resolve incidents, service management standards, and metrics reporting are important aspects of incident management, but they are not as critical as prioritization criteria for the design of the process. References: ISACA Journal Article: Incident Management: A Practical Approach

NEW QUESTION: 321
為了確保組織能□集中管理行動裝置以防止資料洩露，對於IS 審計師來□最重要的是確定：
A. 存在行動安全意識培訓計畫。
B. 定期提供管理階層事件統計資料。
C. 在行動裝置上□用了遠端清除功能。
D. 可以遠端定位遺失的行動裝置。
Answer: (SHOW ANSWER)
The primary risk is data exposure if a mobile device is lost or stolen. A centrally enforced mobile device management (MDM) solution with remote wipe ensures sensitive data can be erased quickly, effectively mitigating disclosure risk. While training and reporting provide value, they are not preventative. Locating devices is helpful but does not protect data if recovery fails.
References (ISACA): COBIT 2019, DSS05 (Managed Security Services).

NEW QUESTION: 322
資訊系統審計員正在重新部署一套新的自動化系統。下列哪一項發現代表了最重大的風險？
A. 新系統導致多名經驗豐富的關鍵人員被裁員。
B. 使用者尚未接受新系統的訓練。
C. 舊系統中的資料未正確遷移到新系統。
D. 新系統並非平台無關的
Answer: C (LEAVE A REPLY)
The finding that presents the most significant risk when reviewing the deployment of a new automated system is that data from the legacy system is not migrated correctly to the new system. Data migration is a critical process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. If data migration is not performed correctly, it can result in data loss, corruption, inconsistency, or duplication,

which can affect the functionality, performance, reliability, and security of the new system. Data migration errors can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The other findings (A, B and D) are less significant risks, as they can be mitigated by rehiring or retraining personnel, providing user training, or adapting the system to different platforms.

NEW QUESTION: 323
在規劃為客口進行口部和外部滲透測試時，應先執行下列哪項操作？
A. 確定測試時間。
B. 確定里程碑。
C. 確定測試報告
D. 建立交戰規則。
Answer: (SHOW ANSWER)
The rules of engagement define the scope, objectives, methodology, deliverables, and limitations of the penetration testing. They also specify the legal and ethical boundaries, communication channels, and escalation procedures. Establishing the rules of engagement is the first step when planning to conduct penetration testing for a client, as it ensures that both parties agree on the expectations and outcomes of the testing. The other options are important steps, but they should be done after the rules of engagement are established. References: CISA Review Manual (Digital Version) 1, page 381.

NEW QUESTION: 324
下列哪一種方法能最有效地為實體存取提供正向身分驗證？
A. 感應卡
B. 視網膜掃描
C. 數位鍵盤與監視器
D. 一張智慧卡和一個保安
Answer: (SHOW ANSWER)
The most effective method for positive authentication for physical access is a retina scan because it uses a biometric characteristic that is strongly tied to the individual and difficult to share, transfer, or replicate compared with cards, codes, or visual checks. ISACA materials discussing physical access and identity verification recognize biometrics such as retina scans as a high-assurance authentication mechanism.
Option B is correct because positive authentication means reliably confirming that the person presenting for access is truly the claimed individual. A retina scan verifies "something you are," which is generally stronger than "something you have" or "something you know" for physical access authentication.
Option A is weaker because a proximity card is only possession-based authentication. It can be lost, borrowed, stolen, or shared, so it does not positively verify identity to the same degree as biometrics. This makes it less effective than a retina scan.

Option C is also weaker. A numeric keypad depends on a code that can be disclosed or observed, and a surveillance camera is more detective than authentication-focused. Together they do not provide the same strong identity binding as biometrics.
Option D improves assurance somewhat, but a smart card is still possession-based and a security guard's judgment can be fallible. Human verification helps, but it does not usually match the direct individual-specific certainty of biometric authentication.
Therefore, B is the best answer because a retina scan most effectively provides positive authentication by directly verifying an individual's unique biometric characteristic.
References (Official ISACA):
* ISACA Journal, Against the Quantum Threat: Selective Compatibility - references retina and palm print scans being confirmed at each use to prevent identity theft.
* ISACA News and Trends biometric authentication resources index.

NEW QUESTION: 325
在審口使用者帳口策略時，資訊系統審計員最應該關注下列哪一項？
A. 公司沒有規定在員工離職時撤銷其係統存取權限。
B. 目前沒有持續安全意識訓練的政策。
C. 沒有政策要求員工簽署保密協議(NDA)。
D. 沒有政策規定員工更換角色時撤銷先前的存取權限。
Answer: (SHOW ANSWER)
Failure torevoke access upon terminationposes the greatest security risk, as ex-employees could still access sensitive data or systems.
No Policy to Revoke Access (Correct Answer - A)
A terminated employee retaining access can lead todata breaches or insider threats.
Example:A former employee misuses active credentials to access financial systems.
Lack of Security Awareness Training (Incorrect - B)
Important but does not pose an immediate security risk like an active ex-employee account.
No NDAs (Incorrect - C)
Protects intellectual property but is not as critical as system access.
No Access Revocation for Role Changes (Incorrect - D)
Still a concern, but ex-employees with active access are ahigherrisk.
References:
ISACA CISA Review Manual
NIST 800-53 (Access Control)

NEW QUESTION: 326
在審口組織的架構(EA)時，資訊系統稽核員最有可能在EA文件中發現下列哪一項口容？
A. IT部門關鍵資源的聯絡訊息
B. 詳細的加密標準
C. 展示從當前狀態到未來狀態演變的路線圖

D. 用於系統間通訊的協定

Answer: C (LEAVE A REPLY)

Enterprise Architecture (EA) documentation primarily includes strategic and operational blueprints outlining the evolution of IT infrastructure to align with business goals. Roadmaps showing the evolution from current state to future state (C) are essential for understanding how the organization's IT environment will change over time to support business strategy.

Other options:

Contact information for key resources (A) is more of an operational or administrative document rather than an EA component.

Detailed encryption standards (B) would typically be found in security policies or system-specific documentation rather than in EA documentation.

Protocols used to communicate between systems (D) are typically documented within network or system architecture diagrams rather than high-level EA documentation.

Reference: ISACA CISA Review Manual, IT Governance and Management of IT

NEW QUESTION: 327

資訊系統審計員應確保應用程式的審計追蹤：

A. 具有足口的安全性。

B. 記錄所有資料庫記錄。

C. 可在線訪問

D. 不影響營運效率

Answer: A (LEAVE A REPLY)

An application's audit trail is a record of all actions or events that occur within or affect an application, such as user activities, system operations, data changes, errors, exceptions, etc. An audit trail can provide evidence and accountability for an application's functionality and performance, and support auditing, monitoring, troubleshooting, and investigation purposes. An IS auditor should ensure that an application's audit trail has adequate security, which means that it is protected from unauthorized access, modification, deletion, or disclosure. Adequate security can help ensure that an audit trail maintains its integrity, reliability, and availability, and prevents tampering or manipulation by attackers or insiders who want to hide their tracks or evidence of their actions. Logs all database records is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as logging all database records may not be necessary or feasible for some applications, and may generate excessive or irrelevant data that can affect the storage or analysis of the audit trail. Is accessible online is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as online accessibility may not be required or desirable for some applications, and may introduce security or privacy risks for the audit trail. Does not impact operational efficiency is a desirable outcome of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as operational efficiency may not be the primary objective or

concern of an application's audit trail, and may depend on other factors or trade-offs such as storage capacity, performance speed, or data quality.

NEW QUESTION: 328
資訊系統審計員發現，為多個業務部門服務的IT組織對所有項目賦予相同的優先級，這可能導致專案資金的獲取出現延誤。下列哪一項最有助於以支援業務目標的方式，將專案和服務需求與可用資源相匹配？
A. 專案管理
B. 風險評估結果
C. IT治理框架
D. 投資組合管理
Answer: D (LEAVE A REPLY)
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:
CISA Review Manual, 27th Edition, page 721
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 329
某□部稽核部門最近建立了一個品質保證(QA)專案。下列哪一項活動對於QA專案的要求最為重要？
A. 長期□部稽核資源規劃
B. 持續監測審計活動
C. 業務線用□滿意度報告分析
D. □部稽核人員的回饋
Answer: B (LEAVE A REPLY)
Ongoing monitoring of the audit activities is the most important activity to include as part of the quality assurance (QA) program requirements for an internal audit department. An IS auditor should perform regular reviews and evaluations of the audit processes, methods, standards, and outcomes to ensure that they comply with the QA program objectives and criteria. This will help to maintain and improve the quality and consistency of the audit services and deliverables. The other options are less important activities to include as part of the QA program requirements, as they may involve long-term resource planning, user satisfaction reports, or feedback from internal audit staff. References:
CISA Review Manual (Digital Version), Chapter 2, Section2.61

CISA Review Questions, Answers and Explanations Database, Question ID 224

NEW QUESTION: 330
某組織最近在其口部會計軟體系統中採用敏捷模型部署自訂程式碼。在檢視生口程式碼部署流程時，下列哪一項是需要解決的最重要的安全問題？
A. 軟體漏洞掃描是暫時進行的。
B. 變更控制不包括品質保證(QA)的測試和批准。
C. 生口程式碼部署不是自動化的。
D. 目前的 DevSecOps 流程尚未經過獨立驗證。
Answer: B (LEAVE A REPLY)
Change control is the process of managing and documenting changes to an information system or its components. Change control aims to ensure that changes are authorized, tested, approved, implemented, and reviewed in a controlled and consistent manner. Change control is an essential part of ensuring the security, reliability, and quality of an information system.
One of the key elements of change control is testing and approval from quality assurance (QA). QA is the function that verifies that the changes meet the requirements and specifications, comply with the standards and policies, and do not introduce any errors or vulnerabilities. QA testing and approval provide assurance that the changes are fit for purpose, function as expected, and do not compromise the security or performance of the system.
An organization that has recently moved to an agile model for deploying custom code to its in-house accounting software system should still follow change control procedures, including QA testing and approval.
Agile development methods emphasize flexibility, speed, and collaboration, but they do not eliminate the need for quality and security checks. In fact, agile methods can facilitate change control by enabling frequent and iterative testing and feedback throughout the development cycle.
However, if change control does not include testing and approval from QA, this poses a significant security concern for the organization. Without QA testing and approval, the changes may not be properly validated, verified, or evaluated before being deployed to production. This could result in introducing bugs, defects, or vulnerabilities that could affect the functionality, availability, integrity, or confidentiality of the accounting software system. For example, a change could cause data corruption, performance degradation, unauthorized access, or data leakage. These risks could have serious consequences for the organization's financial operations, compliance obligations, reputation, or legal liabilities.
Therefore, change control that does not include testing and approval from QA is the most significant security concern to address when reviewing the procedures in place for production code deployment in an agile model.
References:

Change Control - ISACA
Quality Assurance - ISACA
Agile Development - ISACA
10 Agile Software Development Security Concerns You Need to Know

NEW QUESTION: 331
在檢視專案風險管理實務時，下列哪一項發現最令人擔憂？
A. 未正式追蹤的未解決問題。
B. 未使用專案管理軟體。
C. 定性風險分析尚未更新。
D. 沒有正式的里程碑驗收。
Answer: C (LEAVE A REPLY)
The best answer is C. Qualitative risk analyses have not been updated.
ISACA guidance describes the risk register as a living document that should be regularly reviewed and amended so management has an up-to-date picture of risk when making decisions. If qualitative risk analyses are not updated, the project may be working from outdated assumptions about probability, impact, and priority, which undermines the entire risk management process.
Option A is a concern, but issue tracking is not as central to project risk management as keeping risk analysis current. Option B is not inherently a weakness because effective risk management does not depend on a specific software tool. Option D is a governance concern, but stale risk analysis more directly damages the organization's ability to identify, assess, prioritize, and respond to project risk.
References (Official ISACA):
* ISACA Journal, Mitigating Technical Vulnerabilities With Risk Assessment - the risk register is a living document that should be regularly reviewed and amended.
* ISACA, Making Risk Management for Agile Projects Effective - risk registers are updated throughout the project lifecycle.

NEW QUESTION: 332
資訊系統審計師在審計過程中何時最需要應用重要性概念？
A. 在規劃審計業務時

B. 在收集田野調口資料時
C. 當發現違反監理要求時
D. 在評估被審計單位的陳述時
Answer: (SHOW ANSWER)
The concept of materiality is most important for an IS auditor to apply when planning an audit engagement, because it helps the auditor to determine the scope, objectives, procedures and resources of the audit.
Materiality is the degree to which an omission or misstatement of information could affect the users' decisions or the achievement of the audit objectives. By applying the concept of materiality, the auditor can focus on the most significant and relevant areas of the audit and avoid wasting time and effort on trivial or immaterial matters. The other options are not as important as planning an audit engagement, because they are either based on or affected by the materiality assessment done during the planning phase. References:
ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.31
ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques forIS Audit and Assurance Professionals, section 12022

NEW QUESTION: 333
當被審計方在後續審計時仍無法完成所有審計建議時，資訊系統審計師的最佳做法是什麼？
A. 確保未解決的問題保留在審計結果中。
B. 由於未解決的問題，終止後續跟進。
C. 建議對未決問題進行補償控制。
D. 評估未決問題造成的剩餘風險。
Answer: D (LEAVE A REPLY)
The best course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit is to evaluate the residual risk due to open issues. Residual risk is the risk that remains after the implementation of controls or mitigating actions. Evaluating the residual risk due to open issues can help the IS auditor assess the impact and likelihood of the potential threats and vulnerabilities that have not been addressed by the auditee, as well as the adequacy and effectiveness of the existing controls or mitigating actions. Evaluating the residual risk due to open issues can also help the IS auditor prioritize and communicate the open issues to the auditee and other stakeholders, such as senior management or audit committee, and recommend appropriate actions or escalation procedures.
Ensuring the open issues are retained in the audit results is a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but it is not the best one. Ensuring the open issues are retained in the audit results can help the IS auditor document and report the status and progress of the audit recommendations, as well as provide a basis for future follow-up audits.

However, ensuring the open issues are retained in the audit results does not provide an analysis or evaluation of the residual risk due to open issues, which is more important for informing decision-making and action- taking.
Terminating the follow-up because open issues are not resolved is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a consequence or outcome of it. Terminating the follow-up because open issues are not resolved may indicate that the auditee has failed to comply with the agreed-upon actions or deadlines, or that the IS auditor has encountered significant obstacles or resistance from the auditee. Terminating the follow-up because open issues are not resolved may also trigger further actions or sanctions from the IS auditor or other authorities, such as issuing a qualified or adverse opinion, withholding certification, or imposing penalties.
Recommending compensating controls for open issues is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a possible outcome or result of it. Compensating controls are alternative or additional controls that are implemented to reduce or eliminate the risk associated with a weakness or deficiency in another control. Recommending compensating controls for open issues may be appropriate when the auditee is unable to implement the original audit recommendations due to technical, operational,financial, or other constraints, and when the compensating controls can provide a similar or equivalent level of assurance. However, recommending compensating controls for open issues requires a prior evaluation of the residual risk due to open issues, which is more important for determining whether compensating controls are necessary and feasible.
References:
Follow-up Audits - Canadian Audit and Accountability Foundation 1
Conducting The Audit Follow-Up: When To Verify - TheAuditor 2
Internal Audit Follow Ups: Are They Really Worth The Effort

NEW QUESTION: 334
當員工使用公共社群網站時，下列哪一項對組織構成最大的風險？
A. 跨站口本攻擊(XSS)
B. 版權侵權
C. 社會工程
D. 關於該組織的負面帖子
Answer: (SHOW ANSWER)
Social engineering is the manipulation of people to perform actions or divulge confidential information. It is a common technique used by attackers to gain unauthorized access to systems or data. Employees who use public social networking sites may be vulnerable to social engineering attacks, such as phishing, baiting, or pretexting, which pose the greatest risk to the organization's security. The other options are not as serious as social engineering, as they relate to web application vulnerabilities, intellectual property rights,

and reputation management, which are less likely to compromise the organization's assets or operations. References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.3 Security Awareness Training1

NEW QUESTION: 335
資訊系統審計員發現日誌管理系統充斥著大量誤報。審計員的最佳建議是：
A. 建立警報審口標準。
B. 招募更多監控人員。
C. 減少防火牆規則。
D. 微調入侵偵測系統(IDS)。
Answer: (SHOW ANSWER)
Fine tuning the intrusion detection system (IDS) is the best recommendation to reduce the number of false positive alerts that overwhelm the log management system, because it can help adjust the sensitivity and accuracy of the IDS rules and signatures to match the network environment and traffic patterns. Establishing criteria for reviewing alerts, recruiting more monitoring personnel, and reducing thefirewall rules are not effective solutions to address theroot cause of the false positive alerts, but rather ways to cope with the consequences. References: CISA Review Manual (Digital Version), Chapter 5, Section5.4.3

NEW QUESTION: 336
對於執行重大系統升級後實施審口的資訊系統審計師而言，下列哪一項應該是最需要關注的問題？
A. 開發人員可以存取測試環境。
B. 變更核准沒有正式的文件記錄。
C. 開發團隊將變更提交至生口環境。
D. 開發群組可以存取目標程式碼。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 337
在組織實施資料遺失防護 (DLP) 解決方案時，下列哪些活動應該先完成？
A. 設定報表
B. 配置規則集
C. 口用檢測點
D. 建立異常工作流程
Answer: D (LEAVE A REPLY)
Configuring rule sets is the first activity that should be completed during the implementation of a DLP solution, because rule sets define the criteria and actions for identifying, monitoring, and preventingdata loss incidents12. Rule sets are based on the organization's data classification, policies, and requirements, and they help to ensure that

the DLP solution is aligned with the business objectives and risk appetite34. Configuring rule sets before enabling detection points, establishing exceptions workflow, or configuring reports helps to avoid false positives, false negatives, or unnecessary alerts5.
References
1: 3.13: Deploy a Data Loss Prevention Solution - Read the Docs
2: Plan and implement data loss prevention (DLP) [Guided] - NICCS
3: CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM DATA PROTECTION ... - CISA
4: Continuous Diagnostics and Mitigation Program Technical ... - CISA
5: Data Loss Prevention Best Practices - ISACA Journal

NEW QUESTION: 338
下列哪一項與系統介面相關的因素對組織構成最大風險？
A. 部分資料傳輸過程是手動執行的。
B. 透過介面進行的資料傳輸通知不會被保留。
C. 沒有可靠的系統介面清單。
D. 某些系統介面沒有流程文件。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 339
資訊系統審計員發現，開發人員使用相同金鑰授予多個呼叫應用程式介面(API) 的應用程式存取權。下列哪一項是解決此問題的最佳建議？
A. 授權 API 金鑰，允許所有應用程式進行唯讀存取。
B. 將 API 金鑰替換為授予最小權限存取權限的有時限令牌。
C. 實作一個流程，使API 金鑰在預先約定的時間段後過期。
D. 與所有受影響的應用程式擁有者協調 API 金鑰輪換工作。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 340
系統出現多個重複出現的處理錯誤。下列哪一項是資訊系統審計員的首要關注點？
A. 事件管理效率低下
B. 缺乏問題管理
C. 缺乏變革管理
D. 專案管理效率低下
Answer: B (LEAVE A REPLY)
The primary concern is lack of problem management. Recurring processing errors indicate that incidents may be getting handled repeatedly without identifying and eliminating the underlying root cause. ISACA guidance ties problem management to root cause analysis and distinguishes it from incident management, which is primarily focused on restoring service quickly.

Option B is correct because repeated errors usually mean the organization is not effectively analyzing and resolving the underlying cause. ISACA explicitly notes that root cause analysis is essential for both incident and problem-related processes, particularly DSS02 Manage service requests and incidents and DSS03 Manage problems. Repeated issues are a classic sign that problem management is weak or absent.
Option A is not the best answer because incident management is about handling and restoring service for individual events. Even efficient incident response can coexist with recurring incidents if root causes are not addressed. That points more directly to weak problem management than to incident handling alone.
Option C could be relevant if the errors stem from poorly controlled changes, but the question does not mention recent changes. The strongest direct inference from recurring errors is failure to resolve the root cause, which is the purpose of problem management.
Option D is the weakest answer because project management is not the most direct operational control area implicated by recurring production processing errors.
Therefore, B is the best answer because recurring processing errors most strongly suggest that underlying root causes are not being identified and eliminated through effective problem management.
References (Official ISACA):
* ISACA, Root Cause Analysis - root cause analysis is used in DSS02 Manage service requests and incidents and DSS03 Manage problems.
* ISACA, Issue Management Confidential: Tools and Best Practices for Improving IT Issue Management
- issue management prioritizes and resolves issues based on impact and likelihood.
* ISACA, A Fresh Look at Modern Auditing - repeated cyber/operational issues can indicate missing accountability and issue tracking.

NEW QUESTION: 341
在進行實施後評估時，確定下列何者最為重要？
A. 解決方案架構是否符合 IT 標準
B. 是否已達到成功標準
C. 專案是否在核准的預算口完成
D. 團隊合作的經驗教訓是否已被記錄
Answer: B (LEAVE A REPLY)
The most important thing to determine when conducting a post-implementation review is whether success criteria have been achieved. A post-implementation review is a process of evaluating the results and outcomes of a project or initiative after it has been completed and implemented. The success criteria are the measurable indicators that define what constitutes a successful project or initiative in terms of its objectives, benefits, quality, performance, and stakeholder satisfaction. The IS auditor should verify whether the success criteria have been achieved by comparing the actual results and outcomes with the expected or planned ones, and by assessing whether they meet or exceed the

expectations and requirements of the stakeholders. The IS auditor should also identify any gaps, issues, or risks that may affect the sustainability or scalability of the project or initiative, and provide recommendations for improvement or remediation. The other options are not as important as determining whether success criteria have been achieved when conducting a post- implementation review, because they either focus on specific aspects or components of the project or initiative rather than theoverall value proposition, or they are part of the pre-implementation or implementation phases rather than the post-implementation phase. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION: 342
資訊系統審計員發現有違規行為，但被審計單位的管理階層選擇忽視這些違規行為。
如果需要向外部機構報告，下列哪一項是資訊系統審計員應採取的最佳行動？
A. 取得審計和被審計管理階層的批准才能發布報告。
B. 取得被審計單位管理階層的批准，方可發布報告。
C. 立即向相關監管機構提交報告。
D. 在獲得審計管理層的批准後提交報告。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 343
下列哪一項控制措施對於確保系統介面的完整性最為重要？
A. 定期審計
B. 檔案計數
C. 檔案校驗和
D. IT操作員監控
Answer: C (LEAVE A REPLY)
File checksums are values that are calculated from the contents of a file and can detect any changes or corruption in the file. They are used to verify that the files that are transferred or processed through system interfaces are not altered in any way. File checksums are more effective than periodic audits, file counts, or IT operator monitoring, which are other types of controls that can help ensure the integrity of system interfaces, but they are not as reliable or timely as file checksums.

NEW QUESTION: 344
資訊系統審計師擔心有人可能透過搭便車或尾隨的方式未經授權存取高度敏感的資料中心。下列哪一項是最佳建議？ (請從CISA認證－資訊系統審計師官方教材中選出正確答案並加以解釋)
A. 生物辨識技術
B. 訪客護送程序
C. 氣閘入口

D. 入侵警報

Answer: C (LEAVE A REPLY)

The best recommendation to prevent unauthorized access to a highly sensitive data center by piggybacking or tailgating is to use an airlock entrance. An airlock entrance is a type of access control system that consists of two doors that are interlocked, so that only one door can be opened at a time. This prevents an unauthorized person from following an authorized person into the data center without being detected. An airlock entrance can also be integrated with other security measures, such as biometrics, card readers, or PIN pads, to verify the identity and authorization of each person entering the data center.

Biometrics (option A) is a method of verifying the identity of a person based on their physical or behavioral characteristics, such as fingerprints, iris scans, or voice recognition. Biometrics can provide a high level of security, but they are not sufficient to prevent piggybacking or tailgating, as an unauthorized person can still follow an authorized person who has been authenticated by the biometric system.

Procedures for escorting visitors (option B) is a policy that requires all visitors to the data center to be accompanied by an authorized employee at all times. This can help prevent unauthorized access by visitors, but it does not address the risk of piggybacking or tailgating by other employees or contractors who may have legitimate access to the building but not to the data center.

Intruder alarms (option D) are devices that detect and alert when an unauthorized person enters a restricted area. Intruder alarms can provide a deterrent and a response mechanism for unauthorized access, but they are not effective in preventing piggybacking or tailgating, as they rely on the detection of the intruder after they have already entered the data center.

References: 1: CISA Certification | Certified Information Systems Auditor | ISACA 2: CISA Certified Information Systems Auditor Study Guide, 4th Edition 3: CISA - Certified Information Systems Auditor Study Guide [Book]

NEW QUESTION: 345

下列哪一項是口部稽核在協助建立組織隱私保護計畫中應發揮的適當作用？

A. 分析新規則帶來的風險

B. 制定監控個人資料使用的程序

C. 定義組織口與隱私相關的角色

D. 設計控制措施以保護個人數據

Answer: A (LEAVE A REPLY)

An appropriate role of internal audit in helping to establish an organization's privacy program is analyzing risks posed by new regulations. A privacy program is a set of policies, procedures, and controls that aim to protect the personal data of individuals from unauthorized or unlawful collection, use, disclosure, or disposal.

A privacy program should comply with the applicable laws and regulations that govern the privacy rights and obligations of individuals and organizations, such as the General Data

Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). New regulations may introduce new requirements or changes that affect the organization's privacy program and expose it to potential compliance risks or penalties. Therefore, internal audit can help to establish an organization's privacy program by analyzing the risks posed by new regulations and providingassurance, advice, or recommendations on how to address them1. The other options are less appropriate or incorrect because:
B). Developing procedures to monitor the use of personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role.
Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the effectiveness and efficiency of the organization's privacy program, but not create or execute it2.
C). Defining roles within the organization related to privacy is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a governance or strategic role. Internal audit should not be involved in setting or approving the organization's privacy strategy, objectives, or policies, as it would compromise its independence and objectivity. Internal audit should provide assurance on the alignment and compliance ofthe organization's privacy program with its strategy, objectives, and policies, but not define or approve them2.
D). Designing controls to protect personal data is not an appropriate role of internal audit in helping to establish an organization's privacy program, as it is more of a management or operational role. Internal audit should not be involved in designing or implementing the organization's privacy program, as it would compromise its independence and objectivity. Internal audit should provide assurance on the adequacy and effectiveness of the organization's privacy program, but not design or implement it2. References: ISACA Introduces New Audit Programs for Business Continuity/Disaster ..., Best Practices for Privacy Audits - ISACA, ISACA Produces New Audit and Assurance Programs for Data Privacy and ...

NEW QUESTION: 346
對於評估財務系統應付帳款模組存取控制的資訊系統審計師而言，下列哪項觀察結果最應引起重視？
A. 資訊系統稽核員被授予建立採購訂單的權限。
B. 應付帳款人員有權更新供應商銀行帳口詳細資料。
C. 配置的委派限制與組織的委派策略不一致。
D. 付款文件在處理之前以可寫格式儲存在共用磁碟機上。
Answer: (SHOW ANSWER)

NEW QUESTION: 347
下列哪一項是確定防火牆配置是否符合組織安全策略的最佳審計程序？
A. 檢口參數設定
B. 口看系統日誌
C. 訪談防火牆管理員
D. 檢討實際程序
Answer: (SHOW ANSWER)
The best audit procedure to determine whether a firewall is configured in compliance with the organization's security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization's security policy, which is a document that outlines the security objectives, requirements, and guidelines for an organization's information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts, etc., and may not indicate whether they comply with the organization's security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possibleaudit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization's security policy.

NEW QUESTION: 348
業務應用程式的資料庫會在幾分鐘口複製到複製伺服器。下列哪些在工作時間口進行的流程最能受益於這種架構？
A. 生口伺服器故障時交易向前捲動
B. 涉及資料庫的硬體更換工作

C. 應用效能下降分析
D. 來自複製伺服器的臨時批次報告作業
Answer: D (LEAVE A REPLY)

NEW QUESTION: 349
下列哪一項反映了數據分析在貸款發放過程中的應用？
A. 評估貸款記錄是否包含在批次文件中，並已通過服務系統的驗證。
B. 將發起系統中輸入的貸款群體與服務系統中記錄的貸款進行比較
C. 驗證兩個系統之間是否已執行資料核對，並調口差異。
D. 檢視錯誤處理控制措施，以便在發生傳輸故障時通知相關人員
Answer: (SHOW ANSWER)
Data analytics can be used to compare data from different sources and identify any discrepancies or anomalies. In this case, comparing a population of loans input in the origination system to loans booked on the servicing system can help detect any errors or frauds in the loan origination process. The other options are not examples of data analytics, but rather controls for data integrity, reconciliation, and error handling.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.2

NEW QUESTION: 350
資訊系統審計師在審計任務的初步階段對業務流程進行功能演練的主要原因是：
A. 辨識業務流程中的控制缺陷。
B. 優化業務流程。
C. 了解關鍵領域。
D. 了解資源需求。
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed in-Depth Explanation:
During the preliminary phase, the auditor ' s goal is to understand the key areas of the business process to identify potential risks and areas that need deeper examination. This understanding helps in planning the audit effectively.
Identifying weaknesses (Option A) occurs later, while optimization (Option B) and resource understanding (Option D) are not primary objectives at this stage.
ISACA CISA Reference: Domain 1 - Information System Auditing Process

NEW QUESTION: 351
下列哪一項是加強智慧型設備安全性以防止資料外洩的最佳方法？
A. 及時審口對組織敏感資料的存取日誌。
B. 在自帶裝置 (BYOD) 安全程序中加入使用限制。
C. 在智慧型裝置上強制執行嚴格的安全設定。
D. 請員工正式確認安全程序。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 352
當組織取得新的 IT 系統來支援其業務策略時，下列何者是口部IS 稽核師的主要職能？
A. 辨識重大 IT 錯誤和詐欺
B. 評估系統開發生命週期 (SDLC) 控制
C. 評估 IT 風險與控制
D. 實施風險與控制差距緩解
Answer: (SHOW ANSWER)

NEW QUESTION: 353
對於使用雲端服務供應商處理客口資料的組織而言，下列何者是最重要的隱私考量？
A. 未經客口同意，不得將任何個人資訊轉移給服務提供者。
B. 資料隱私必須按照行業標準和最佳實踐進行監控。
C. 傳輸給服務提供者的客口資料必須向監管機構報告。
D. 資料隱私必須依照適用於該組織的法規進行管理。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
在準備審計業務時，記錄審計目標的主要目的是什麼？
A. 為了因應正在審口的活動相關的整體風險。
B. 辨識物質問題機率發生相對較高的區域
C. 為了確保在審計過程中最大限度地利用審計資源
D. 協助決定受審計方會議的優先順序和時間安排
Answer: B (LEAVE A REPLY)
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with relatively high probability of material problems that may affect the achievement of audit goals or business objectives.
Addressing the overall risk associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems. References:
CISA Review Manual, 27th Edition, page 1111
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 355

資訊系統審計員受命對擬議的新電腦硬體採購項目進行審計。審計員的主要關注點是：
A. 實施方案滿足使用者需求。
B. 將包含完整的、可見的審計追蹤。
C. 已確立一個合理的商業理由。
D. 新硬體符合既定的安全標準
Answer: C (LEAVE A REPLY)
The IS auditor's primary concern when auditing the proposed acquisition of new computer hardware is that a clear business case has been established. A business case is a document that justifies the need, feasibility, and benefits of a proposed project or investment. A clear business case can help to ensure that the acquisition of new computer hardware is aligned with the organization's goals, objectives, and requirements, and that it provides value for money and return on investment. The other options are not as important as establishing a clear business case, as they do not address the rationale or justification for acquiring new computer hardware. References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION: 356
在製定後續計劃時，資訊系統審計員從營運管理層獲悉，近期組織架構的調整已解決了先前識別出的風險，因此無需再實施行動計劃。審計員下一步該怎麼做？
A. 報告稱，這些變化使得確定風險是否已解決變得不切實際。
B. 接受管理階層的口法，並報告風險已解決。
C. 確定這些變更是否引入了需要解決的新風險。
D. 審口變更並確定風險是否已解決。
Answer: B (LEAVE A REPLY)
When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence1. References:
1(https://www.isaca.org/resources/isaca-journal/issues
/2016/volume-6/enhancing-the-audit-follow-up-process-using-cobit-5)

NEW QUESTION: 357
對於審口IT策略文件的IS審計師而言，下列何者最為重要？
A. 上一年的IT策略目標沒有實現。
B. 目標架構是在技術層面上定義的。
C. 新舉措的財務估算已在文件中揭露。
D. 策略 IT 目標完全源自於最新的市場趨勢。

Answer: (SHOW ANSWER)
AnIT strategymust bealigned with business objectives, not solely based onmarket trends.
Strategic IT Goals Derived Solely from Market Trends (Correct Answer - D) IT strategy should supportorganizational goals, not justfollow industry trends.
Example:A company investing inAIjust because it'strendy, without considering business needs.
Previous Year's IT Goals Not Achieved (Incorrect - A)
A concern, butdoes not indicate a fundamental strategy flaw.
Target Architecture Defined at a Technical Level (Incorrect - B)
Technical details are important for implementation.
Financial Estimates Included (Incorrect - C)
Cost transparency is agood practice.
References:
ISACA CISA Review Manual
COBIT 2019 (IT Governance)

NEW QUESTION: 358
在組織的資訊分類過程中，資訊系統審計員的主要職責是什麼？
A. 根據分配的分類保護資訊資口。
B. 驗證資口是否根據分配的分類受到保護
C. 確保分類等級與監理指南保持一致
D. 定義組織口資訊資口的分類級別
Answer: B (LEAVE A REPLY)
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization's information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:
CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
CISA Review Questions, Answers and Explanations Database, Question ID 206

NEW QUESTION: 359
使用行動裝置時，下列何者是維護網路完整性最有效的方法？
A. 實施網路存取控制。
B. 實施出站防火牆規則。
C. 執行網路審口。
D. 審口存取控制清單。
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 360
下列哪一項能□最好地保證新的資料庫管理系統(DBMS)符合當地隱私法規的要求？
A. 合規性審計
B. 行政審計
C. 一般資訊科技控制審□
D. 法務審計
Answer: A (LEAVE A REPLY)
The best assurance that a new DBMS meets local privacy regulations is provided by a compliance audit.
ISACA defines privacy compliance as adherence to relevant data protection laws, regulations, standards, and policies. A compliance-focused review is therefore the most direct way to determine whether the DBMS design, configuration, and operation satisfy applicable privacy requirements.
Option A is correct because the question is specifically about meeting local privacy regulations. A compliance audit is designed to assess conformance with external legal and regulatory obligations as well as applicable internal requirements. ISACA's privacy risk guidance also notes that privacy assessments determine whether an enterprise is in compliance with applicable laws and regulations.
Option B is incorrect because an administrative audit is broader and does not specifically target legal and regulatory privacy compliance.

Option C is incorrect because a general IT controls review may assess access, change management, backup, and operations controls, but it does not directly assure compliance with privacy laws.
Option D is incorrect because a forensic audit is typically used to investigate incidents or evidence after suspected wrongdoing, not to assess upfront regulatory compliance. ISACA's digital forensics guidance is centered on identifying, preserving, analyzing, and presenting evidence.
Therefore, A is the best answer because a compliance audit most directly evaluates whether the DBMS meets local privacy regulatory requirements.
References (Official ISACA):
* ISACA, Privacy Compliance - adherence to relevant data protection laws, regulations, standards, and policies.
* ISACA Journal, Privacy Risk Management - privacy risk assessment determines compliance with applicable laws and regulations.
* ISACA Journal, What Is Your Privacy and Data Protection Strategy? - privacy strategy should ensure compliance with privacy standards, rules, and laws.
* ISACA, Overview of Digital Forensics - clarifies why forensic audit is not the best fit for regulatory assurance.

NEW QUESTION: 361
IT平衡計分卡是監控最有效的手段：
A. 企業 IT 治理。
B. 控制效果。
C. 投資報酬率(ROI)。
D. 變革管理成效。
Answer: A (LEAVE A REPLY)
An IT balanced scorecard is a strategic management tool that aligns IT objectives with business goals and measures the performance of IT processes using key performance indicators (KPIs). It is the most effective means of monitoring governance of enterprise IT, which is the process of ensuring that IT supports the organization's strategy and objectives. Governance of enterprise IT covers aspects such as IT value delivery, IT risk management, IT resource management, and IT performance measurement. An IT balanced scorecard can help monitor these aspects and provide feedback to improve IT governance. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

NEW QUESTION: 362
在規劃滲透測試時，下列哪一項應先執行？
A. 簽署保密協議(NDA)。
B. 確定漏洞報告要求。
C. 定義測試範圍。
D. 取得管理階層對測試的同意。
Answer: D (LEAVE A REPLY)
The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against theorganization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when planning a penetration test, but they are not the first step.
These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

NEW QUESTION: 363
在評估包含多個巨集的電子表格的準確性時，資訊系統審計員最需要審□下列哪一項□容？
A. 電子表格加密
B. 版本歷史記錄
C. 巨集中的公式
D. 關鍵計算的核對
Answer: C (LEAVE A REPLY)
The most important thing for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros is the formulas within macros. Macros are sequences of commands or instructions that can automate tasks or calculations in a spreadsheet. Formulas are expressions that perform calculations on values or data in a spreadsheet. The accuracy of a spreadsheet depends largely on whether the formulas within macros are correct, consistent, and complete. The IS auditor should review the formulas within macros to verify that they produce the expected results and do not contain

any errors or inconsistencies. The other options are not as important as formulas within macros, as they do not directly affect the accuracy of a spreadsheet. Encryption of the spreadsheet is a security control that can protect the confidentiality and integrity of the spreadsheet, but it does not ensure its accuracy. Version history is a document control feature that can track and manage changes to the spreadsheet, but it does not verify its accuracy. Reconciliation of key calculations is a validation technique that can compare and confirm the results of calculations with other sources, but it does not evaluate the accuracy of formulas within macros. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 364
下列哪一項是確保線上訂單完整性的最適當控制措施？
A. 資料加密標準(DES)
B. 數位簽名
C. 公鑰加密
D. 多因素身份驗證
Answer: B (LEAVE A REPLY)
A digital signature is the most appropriate control to ensure integrity of online orders because it provides a way to verify the authenticity and integrity of the data sent by the sender. A digital signature is created by applying a cryptographic algorithm to the data and attaching the result to the data. The receiver can then use the sender's public key to verify that the data has not been altered or tampered with during transmission. A digital signature also provides non-repudiation, which means that the sender cannot deny sending the data.
Data Encryption Standard (DES) is a symmetric encryption algorithm that can provide confidentiality of online orders, but not integrity. DES uses the same key to encrypt and decrypt the data, which means that anyone who has the key can modify the data without detection.
Public key encryption is an asymmetric encryption algorithm that can also provide confidentiality of online orders, but not integrity. Public key encryption uses a pair of keys: a public key and a private key. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their own private key.
However, public key encryption does not prevent anyone from modifying the encrypted data.
Multi-factor authentication is a control that can provide authentication and authorization of online orders, but not integrity. Multi-factor authentication requires the user to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Multi-factor authentication can prevent unauthorized access to online orders, but it does not protect the data from being modified after being sent.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 281 1

ISACA, CISA Review Questions, Answers and Explanations Database - 12 MonthSubscription 2

NEW QUESTION: 365
下列哪一項是管理階層在批准大量 IT 策略例外時最令人擔憂的問題？
A. 這些例外情況可能會無限期地持續下去。
B. 例外情況可能導致不合規。
C. 例外情況可能會增加營運風險。
D. 例外情況可能會對流程效率口生負面影響。
Answer: B (LEAVE A REPLY)
The greatest concern associated with a high number of IT policy exceptions approved by management is that the exceptions may result in noncompliance. IT policy exceptions are deviations from the established IT policies that are granted by management for specific reasons and circumstances. However, if there are too many exceptions, it may indicate that the IT policies are not aligned with the business needs, regulatory requirements, or best practices. This may expose the organization to legal, contractual, or reputational risks due to noncompliance. The other options are not as concerning as noncompliance, as they do not have the same potential impact or consequences. The exceptions are likely to continue indefinitely is a possible outcome of a high number of exceptions, but it does not necessarily imply a negative effect on the organization. The exceptions may elevate the level of operational risk is a valid concern, but it can be mitigated by implementing compensating controls or monitoring mechanisms. The exceptions may negatively impact process efficiency is a minor concern, as it does not affect the effectiveness or reliability of the IT processes. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 366
下列哪一項措施能最有效確保網路傳輸資料的完整性？
A. 訊息加密
B. 憑證授權單位(CA)
C. 隱寫術
D. 訊息摘要
Answer: D (LEAVE A REPLY)
The most effective way to ensure the integrity of data transmitted over a network is to use a message digest. A message digest is a cryptographic function that generates a unique and fixed-length value (also known as a hash or checksum) from any input data. The message digest can be used to verify that the data has not been altered or corrupted during transmission by comparing it with the message digest generated at the destination. Message encryption is a method of protecting the confidentiality of data transmitted over a network by transforming it into an unreadable format using a secret key. Message encryption does not ensure the integrity of data, as it does not prevent or detect

unauthorized modifications. Certificate authority (CA) is an entity that issues and manages digital certificates that bind public keys to identities. CA does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Steganography is a technique of hiding data within other data, such as images or audio files. Steganography does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. References:
CISA Review Manual, 27th Edition, pages 383-3841
CISA Review Questions, Answers and Explanations Database, Question ID: 258

NEW QUESTION: 367
資訊系統審計員正在準備審口與製造工廠實施工業物聯網 (IoT) 基礎設施相關的控制措施。下列哪一項漏洞會為組織帶來最大的安全風險？
A. 低電位有效設備周圍的實體安全措施不足，無法有效防止竊盜
B. 物聯網設備中開源軟體元件的使用
C. 物聯網設備韌體儲存空間中用於程式碼升級的限制
D. 不使用無線網路連接的物聯網設備
Answer: (SHOW ANSWER)
The use of open-source software components in IoT devices presents the greatest security risk due to potential vulnerabilities that may exist within the software. These vulnerabilities can be exploited if patches are not applied promptly, and the organization might not have direct control over the software ' s maintenance and security updates. This risk is amplified in critical manufacturing environments where compromised IoT devices can lead to operational disruptions.
Physical Security (Option A):While important, theft of IoT devices generally poses less risk compared to a system-wide compromise due to software vulnerabilities.
Firmware Storage Constraints (Option C):While a limitation, this is a secondary concern compared to exploitable software.
Devices Not Using Wireless Connectivity (Option D):Wired devices are generally more secure, reducing this as a significant concern.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 368
屬性抽樣最適合用來估計：
A. 符合已核准程序的程度
B. 總體誤差總量。
C. 平均口的標準差。
D. 人口的真實貨幣價口。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 369
供應商需要對關鍵業務應用程式擁有特權存取權限。下列哪一項是降低資料外洩風險的最佳建議？
A. 為特權角色實現即時活動監控
B. 在供應商合約中加入審計權條款
C. 對特權角色和職責進行審口
D. 要求供應商對特權角色實施輪調制度
Answer: (SHOW ANSWER)
A vendor requires privileged access to a key business application. The best recommendation to reduce the risk of data leakage is to implement real-time activity monitoring for privileged roles. This is because real-time activity monitoring can provide visibility and accountability for the actions performed by the vendor with privileged access, such as creating, modifying, deleting, or copying data. Real-time activity monitoring can also enable timely detection and response to any unauthorized or suspicious activities that may indicate data leakage. Including the right-to-audit in the vendor contract is a good practice, but it may not be sufficient to prevent or detect data leakage in a timely manner, as audits are usually performed periodically or on-demand.
Performing a review of privileged roles and responsibilities is also a good practice, but it may not address the specific risk of data leakage by the vendor with privileged access. Requiring the vendor to implement job rotation for privileged roles may reduce the risk of collusion or fraud, but it may not prevent or detect data leakage by any individual with privileged access. References: CISA Review Manual (Digital Version),
[ISACA Privacy Principles and Program Management Guide]

NEW QUESTION: 370
下列哪一項是組織預防資料遺失最有效的方法？
A. 限制員工上網。
B. 實施資料分類程序。
C. 檢口防火牆日誌是否有異常。
D. 定期進行安全意識培訓。
Answer: D (LEAVE A REPLY)
Data loss can occur due to various reasons, such as accidental deletion, hardware failure, malware infection, theft, or unauthorized access. Data classification procedures can help to identify and protect sensitive data, but they are not sufficient to prevent data loss. The most effective way to protect against data loss is to conduct periodic security awareness training for employees, which can educate them on the importance of data security, the best practices for data handling and storage, and the common threats and risks to data.

NEW QUESTION: 371
下列哪一項指標最有助於評估問題管理實務的有效性？

A. 導致停機的重複事件數量
B. 偵測並確定事件優先順序所需的平均時間
C. 在服務等級協定 (SLA) 範圍口解決的事件百分比
D. 已調口和診斷的事件數量
Answer: A (LEAVE A REPLY)

NEW QUESTION: 372
下列哪一項是最大限度降低公司遺失的行動裝置被未經授權存取風險的最佳控制措施？
A. 密碼/PIN碼保護
B. 裝置追蹤軟體
C. 裝置加密
D. 定期備份
Answer: C (LEAVE A REPLY)
The best control to minimize the risk of unauthorized access to lost company-owned mobile devices is device encryption. Device encryption is a process that transforms data on a device into an unreadable format using a cryptographic key. Device encryption protects the data stored on the device from being accessed by unauthorized parties, even if they bypass the password or PIN protection. Device encryption can also prevent data leakage if the device is disposed of or recycled without proper data sanitization. Password or PIN protection is a basic control that prevents unauthorized access to the device by requiring a secret code or pattern to unlock it. However, password or PIN protection can be easily compromised by brute force attacks, shoulder surfing, or social engineering. Device trackingsoftware is a tool that allows the device owner or administrator to locate, lock, or wipe the device remotely in case of loss or theft. However, device tracking software depends on the device's network connectivity and GPS functionality, which may not be available or reliable in some situations. Periodic backup is a process that copies the data from the device to another storage location for recovery purposes. Periodic backup can help restore the data in case of loss or damage of the device, but it does not prevent unauthorized access to the data on the device itself. References: CISA ReviewManual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Mobile Devices

NEW QUESTION: 373
為提高獲利能力，某組織已做出策略決策，將業務拆分為多個獨立的營運實體
然而，各實體之間仍共享IT基礎設施。下列哪一項措施最有助於確保資訊系統稽核在其年度計畫中仍涵蓋IT環境中的關鍵風險領域？
A. 提高每個業務實體基於風險的資訊系統審計頻率
B. 制定基於風險的計劃，並考慮每個實體的業務流程
C. 對新引入的IT政策和程序進行審計
D. 修訂資訊系統審計計劃，重點關注分拆後引入的資訊技術變更
Answer: (SHOW ANSWER)

Developing a risk-based plan considering each entity's business processes would best help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan. A risk-based plan is a plan that prioritizes the audit activities based on the level of risk associated with each area or process. A risk- based plan can help to allocate the audit resources more efficiently and effectively, and provide more assurance and value to the stakeholders1.
By considering each entity's business processes, the IS audit can identify and assess the specific risks and controls that affect the IT environment of each entity, and tailor the audit objectives, scope,and procedures accordingly. This can help to address the unique needs and expectations of eachentity, and ensure that the IS audit covers the key risk areas that are relevant and significant to each entity's operations, performance, and compliance2.
The other options are not as effective as developing a risk-based plan considering each entity's business processes in ensuring that IS audit still covers key risk areas within the IT environment as part of its annual plan. Option A, increasing the frequency of risk-based IS audits for each business entity, is not a feasible or efficient solution, as it may increase the audit costs and workload, and create duplication or overlap of audit efforts. Option C, conducting an audit of newly introduced IT policies and procedures, is a limited and narrow approach, as it may not cover all the aspects or dimensions of the IT environment that may have changed or been affected by the split. Option D, revising IS audit plans to focus on IT changes introduced after the split, is a reactive and short-term approach, as it may not reflect the current or future state of the IT environment or the business objectives of each entity.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription Risk-Based Audit Planning: A Guide for Internal Audit1 Risk-Based Audit Approach: Definition and Example

NEW QUESTION: 374
下列哪些口容在資訊系統審計報告中最為重要？
A. 針對每項審計發現的具體技術解決方案
B. 由於證據不足，觀察結果未報告為調口結果
C. 因應各種風險領域的路線圖
D. 未緩解風險的程度及其對業務的影響
Answer: D (LEAVE A REPLY)

NEW QUESTION: 375
在自備設備 (BYOD) 計畫實施情況進行審計的規劃階段，下列何者能提供最重要的資訊？
A. 以往審計結果
B. 風險評估結果
C. 待連結到企業網路的個人裝置清單

D. 包括 BYOD 可接受使用者聲明在口的政策

Answer: (SHOW ANSWER)

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

NEW QUESTION: 376

下列何者最能有效偵測口部網路中是否存在未經授權的無線存取點？

A. 持續網路監控

B. 定期網路漏洞評估

C. 電子訪問日誌審口

D. 實體安全審口

Answer: A (LEAVE A REPLY)

The most effective method for detecting the presence of an unauthorized wireless access point on an internal network is A. Continuous network monitoring. This is because continuous network monitoring can capture and analyze all the wireless traffic in the network and identify any rogue or spoofed devices that may be connected to the network without authorization. Continuous network monitoring can also alert the system administrator of any suspicious or anomalous activities on the network and help to locate and remove the unauthorized wireless access point quickly.

Periodic network vulnerability assessments (B) can also help to detect unauthorized wireless access points, but they are not as effective as continuous network monitoring, because they are performed at fixed intervals and may miss some devices that are added or removed between the assessments. Review of electronic access logs can provide some information about the devices that access the network, but they may not be able to detect devices that use fake or stolen credentials or devices that do not generate any logs.

Physical security reviews (D) can help to prevent unauthorized physical access to the network ports or devices, but they may not be able to detect wireless access points that are hidden or disguised as legitimate devices.

NEW QUESTION: 377
在災難復原計畫 (DRP) 中，下列哪一項定義最為重要？
A. 業務連續性計劃(BCP)
B. 備份資料復原測試結果
C. 災難復原方案和優先順序的綜合列表
D. 恢復團隊成員的角色與職責
Answer: D (LEAVE A REPLY)
The most important thing to define within a disaster recovery plan (DRP) is the roles and responsibilities for recovery team members, as this ensures that everyone knows what to do, who to report to, and how to communicate in the event of a disaster. A business continuity plan (BCP) is a broader document that covers the overall strategy and objectives for maintaining or resuming business operations after a disaster. Test results for backup data restoration are important to verify the integrity and availability of backup data, but they are not part of the DRP itself. A comprehensive list of disaster recovery scenarios and priorities is useful to identify the potential risks and impacts of different types of disasters, but it is not as critical as defining the roles and responsibilities for recovery team members. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.3: Disaster Recovery Planning1

NEW QUESTION: 378
下列哪一項是確定災難復原計畫 (DRP) 測試是否成功的最佳方法？
A. 分析是否達到預定的測試目標。
B. 在備份資料中心執行測試。
C. 評估關鍵人員的參與。
D. 測試異地備份檔案。
Answer: A (LEAVE A REPLY)
The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated. Test objectives should be

aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

NEW QUESTION: 379
透過正確設定網路防火牆可以降低下列哪些安全風險？
A. SQL 注入攻擊
B. 拒口服務 (DoS) 攻擊
C. 網路釣魚攻擊
D. 口部攻擊
Answer: B (LEAVE A REPLY)
A network firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A network firewall can help reduce the risk of denial of service (DoS) attacks, which are attempts to overwhelm a system or network with excessive requests or traffic, by filtering or blocking unwanted or malicious packets. A SQL injection attack is a type of code injection attack that exploits a vulnerability in a web application's database query, by inserting malicious SQL statements into the input fields. A phishing attack is a type of social engineering attack that attempts to trick users into revealing sensitive information or installing malware, by sending fraudulent emails or messages that impersonate legitimate entities. An insider attack is a type of malicious activity that originates from within an organization, such as employees, contractors, or partners, who abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of information systems or data. A network firewall cannot prevent these types of attacks, as they rely on exploiting human or application weaknesses rather than network vulnerabilities.

NEW QUESTION: 380
下列哪一種技術能最好地降低普遍存在的網路攻擊風險？
A. 加密
B. 配置評估
C. 非軍事區(DMZ)
D. 分割
Answer: D (LEAVE A REPLY)

NEW QUESTION: 381
資訊系統品質保證(OA)小組負責：
A. 確保程序變更符合既定標準。
B. 設計程式以保護資料免於意外外洩。

C. 確保從系統處理接收的輸出完整。
D. 監控電腦處理任務的執行情形。
Answer: A (LEAVE A REPLY)
The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect dataagainst accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

NEW QUESTION: 382
下列哪一項最適合防止未經授權的人取得儲存在業務應用系統中的機密資訊？
A. 應用單一登入進行存取控制
B. 實施職責分離。
C. 執行口部資料存取策略。
D. 強制使用數位簽章。
Answer: C (LEAVE A REPLY)
The most appropriate control to prevent unauthorized retrieval of confidential information stored in a business application system is to enforce an internal data access policy. A data access policy defines who can access what data, under what conditions and for what purposes. It also specifies the roles and responsibilities of data owners, custodians and users, as well as the security measures and controls to protect data confidentiality, integrity and availability. By enforcing a data access policy, the organization can ensure that only authorized personnel can retrieve confidential informationfrom the business application system. Applying single sign-on for access control, implementing segregation of duties and enforcing the use of digital signatures are also useful controls, but they are not sufficient to prevent unauthorized data retrieval without a clear and comprehensive data access policy.
References:
CISA Review Manual, 27th Edition, page 2301
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2

NEW QUESTION: 383
一項網路安全審口發現，使用者在網路服務供應商(ISP) 處擁有個人使用者帳口，並使用這些帳口下載業務資料。該組織希望確保僅使用公司網路。組織首先應該：
A. 使用代理伺服器過濾掉不應該造訪的網路網站。
B. 手動記錄網路存取狀況。

C. 監控遠端存取活動。
D. 在其安全性策略中包含有關網路使用的聲明。
Answer: D (LEAVE A REPLY)
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personalaccounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.
References:
ISACA CISA Review Manual 27th Edition (2019), page 247
What is a Security Policy? Definition, Elements, and Examples - Varonis1

NEW QUESTION: 384
下列哪一項措施能為管理階層提供最合理的保證，確保新的資料倉儲能滿足組織的需求？
A. 將資料需求整合到系統開發生命週期(SDLC)中
B. 任命資料管理員以提供有效的資料治理
C. 根據資料品質問題對組織的影響程度進行分類
D. 促進管理階層和開發人員之間的有效溝通
Answer: (SHOW ANSWER)
A data warehouse is a centralized repository of data that is collected from various sources and organized for analysis and reporting purposes. A data warehouse can help an organization gain insights into its business performance, trends, and opportunities. However, building a data warehouse requires careful planning, design, and implementation to ensure that it meets the needs of the organization.
One of the best practices that would provide management with the most reasonable assurance that a new data warehouse will meet the needs of the organization is A. Integrating data requirements into the system development life cycle (SDLC). The SDLC is

a framework that defines the phases and activities involved in developing a software system, such as planning, analysis, design, testing, deployment, and maintenance1. By integrating data requirements into the SDLC, an organization can ensure that the data warehouse is aligned with the business objectives and expectations, and that it delivers value to the end users.
Some of the benefits of integrating data requirements into the SDLC are:
It helps to identify and prioritize the key business questions and metrics that the data warehouse should support2.
It helps to define and validate the data sources, models, structures, and quality standards that the data warehouse should follow3.
It helps to design and implement the data integration, transformation, and loading processes that the data warehouse should use4.
It helps to test and verify the functionality, performance, and accuracy of the data warehouse before deploying it to production.
It helps to monitor and maintain the data warehouse after deployment and incorporate feedback and changes as needed.

NEW QUESTION: 385
在執行後續活動時，資訊系統審計師發現管理階層實施的糾正措施與最初與審計部門討論並達成一致的措施有所不同。為了解決這種情況，資訊系統審計師的最佳做法是：
A. 將原問題重新列為高風險問題，並上報給高階管理層
B. 在下一個審計週期安排後續審計。
C. 延後後續活動，並將替代控制措施回報給高階審計管理階層
D. 確定替代控制措施是否足以降低風險。
Answer: D (LEAVE A REPLY)
The IS auditor's best course of action in this situation is to determine whether the alternative controls sufficiently mitigate the risk. Alternative controls are different from those originally discussed and agreed with the audit function, but they may still achieve the same objective of addressing the audit issue or reducing the risk to an acceptable level. The IS auditor should evaluate whether the alternative controls are appropriate, effective, and sustainable before closing the audit finding or escalating it to senior management. The other options are not appropriate for resolving this situation, as they do not consider whether the alternative controls are adequate or reasonable. Re-prioritizing the original issue as high risk and escalating to senior management is a drastic step that may undermine the relationship between the auditor and management, and it should be done only after exhausting other means of resolving the issue. Scheduling a follow-up audit in the next audit cycle is unnecessary, as follow-up activities should be performed as soon as possible after management has implemented corrective actions. Postponing follow-up activities and escalating the alternative controls to senior audit management is premature, as follow-up activities should be completed before reporting any findings or

recommendations to senior audit management. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 386
資訊系統審計員注意到，由於第三方供應商提供的硬體不足，上一年的災難復原測試未能按計畫時間完成。下列哪一項最能證明目前已分配足口的資源來成功恢復系統？
A. 服務等級協定(SLA)
B. 硬體變更管理策略
C. 供應商備忘錄，顯示問題已解決
D. 最新的 RACI 圖表
Answer: (SHOW ANSWER)
The best evidence that adequate resources are now allocated to successfully recover the systems is a service level agreement (SLA). An SLA is a contract between a service provider and a customer that defines the scope, quality, and terms of the service delivery. An SLA should include measurable and verifiable indicators of the service performance, such as availability, reliability, capacity, security, and recovery. An SLA should also specify the roles, responsibilities, and expectations of both parties, as well as the remedies and penalties for non-compliance. An SLA can help to ensure that the third-party vendor has allocated sufficient hardware and other resources to meet the recovery objectives and requirements of the organization. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 387
資訊系統審計員正在審口某組織的商業智慧基礎設施。幫助該組織達到合理數據品質水準的最佳建議是：
A. 根據資料分類標準審口資料。
B. 將資料清洗外包給專業服務提供者。
C. 將儲存在不同資料庫中的資料合併到一個資料倉儲中。
D. 根據預先定義的規格分析資料。
Answer: D (LEAVE A REPLY)
This is because analyzing the data against predefined specifications is a method of data quality assessment that can help the organization achieve a reasonable level of data quality. Data quality assessment is the process of measuring and evaluating the accuracy, completeness, consistency, timeliness, validity, and usability of the data. Predefined specifications are the criteria or standards that define the expected or desired quality of the data. By comparing the actual data with the predefined specifications, the organization can identify and quantify any gaps, errors, or deviations in the data quality, and take corrective actions accordingly12.

Reviewing data against data classification standards (A) is not the best answer, because it is not a method of data quality assessment, but rather a method of data security management. Data classification standards are the rules or guidelines that define the level of sensitivity and confidentiality of the data, and determine the appropriate security and access controls for the data. For example, data can be classified into public, internal, confidential, or restricted categories. Reviewing data against data classification standards can help the organization protect the data from unauthorized or inappropriate use or disclosure, but it does not directly improve the data quality3.
Outsourcing data cleansing to skilled service providers (B) is not the best answer, because it is not a recommendation to help the organization achieve a reasonable level of data quality, but rather a decision to delegate or transfer the responsibility of data quality management to external parties. Data cleansing is the process of detecting and correcting any errors, inconsistencies, or anomalies in the data. Skilled service providers are third-partyvendors or contractors that have the expertise and resources to perform data cleansing tasks. Outsourcing data cleansing to skilled service providers may have some benefits, such as cost savings, efficiency, or scalability, but it also has some risks, such as loss of control, dependency, or liability4.
Consolidating data stored across separate databases into a warehouse is not the best answer, because it is not a method of data quality assessment, but rather a method of data integration and storage. Data integration is the process of combining and transforming data from different sources and formats into a unified and consistent view. Data warehouse is a centralized repository that stores integrated and historical data for analytical purposes. Consolidating data stored across separate databases into a warehouse can help the organization improve the availability and accessibility of the data, but it does not necessarily improve the data quality.

NEW QUESTION: 388
下列何者是參與資料中心改造專案的IS審計員最適合的職責？
A. 對參與專案的責任方進行獨立審口
B. 篩選翻新工程供應商
C. 確保專案按計畫推進並達成里程碑
D. 實施資料中心營運控制
Answer: A (LEAVE A REPLY)
IS auditors primarily provide assurance and oversight. In this context, independent reviews ensure that those responsible for the renovation project are meeting their obligations, following best practices, and managing risks appropriately.
References:
ISACA ' s Code of Professional Ethics: Emphasizes the IS Auditor ' s duty to be independent and objective.
The Role of IS Audit: IS Auditors are not project managers but provide objective assessment and guidance regarding controls and risk mitigation within projects.

CISA Review Manual (27th Edition): May have sections discussing the role of IS auditors in infrastructure projects or similar initiatives.

NEW QUESTION: 389
下列哪一項措施最能確保建立適當的截止時間，以便將交易和記錄恢復到電腦系統故障之前的狀態？
A. 異地輪替備份交易文件副本
B. 使用資料庫管理系統(DBMS)動態回溯部分處理的事務
C. 以電子形式維護系統控制台日誌
D. 確保所有輸電線路具備雙向同步能力
Answer: B (LEAVE A REPLY)
The best way to ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure is to use a database management system (DBMS) to dynamically back-out partially processed transactions. A DBMS is a software system that manages the creation, manipulation, retrieval, and security of data stored in a database. A DBMS can provide features such as transaction management, concurrency control, recovery management, and integrity management. A DBMS can dynamically back-out partially processed transactions by using mechanisms such as rollback segments, undo logs, or write-ahead logs. These mechanisms allow the DBMS to restore the database to a consistent state before the failure occurred.
References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 390
資訊系統審計員正在審口遠距辦公使用者的密碼重置流程。為了了解此流程所需的詳細步驟，應要求提供哪種類型的文件？
A. 標準
B. 程序
C. 指南
D. 政策
Answer: B (LEAVE A REPLY)

NEW QUESTION: 391
在審口IT戰略計劃時，最令人擔憂的問題是：
A. 尚未成立資訊科技策略委員會。
B. 此計劃不支持相關的組織目標。
C. 沒有關鍵績效指標(KPI)。
D. 該計劃未經董事會正式批准。
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 392
當組織的文件伺服器需要對外部使用者開放時，下列哪一項是資訊系統稽核員為保護組織免受攻擊而提出的最佳建議？
A. 強制建立安全隧道連線。
B. 增強口部防火牆。
C. 設立非軍事區(DMZ)。
D. 實現安全協定。
Answer: C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a network segment that is separated from the internal network and the external network, such as the internet, by firewalls or other security devices. A DMZ provides an extra layer of security for the organization's internal network by isolating the servers and services that need to be accessible to external users, such as a file server, from the rest of the network. A DMZ also prevents external users from accessing the internal network directly, as they have to go through two firewalls to reach it. Therefore, setting up a DMZ is an IS auditor's best recommendation to protect anorganization from attacks when its file server needs to be accessible to external users12.
The other possible options are:
Enforce a secure tunnel connection: This means that the organization requires external users to establish a secure and encrypted connection, such as a virtual private network

(VPN), to access its file server. This can provide some level of security and privacy for the data transmission, but it does not protect the file server or the internal network from attacks if the connection is compromised or if the external users are malicious. Therefore, enforcing asecuretunnel connection is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users3.
Enhance internal firewalls: This means that the organization improves the security and performance of its internal firewalls, which are devices that filter and control the network traffic between different segments of the network. This can provide some level of protection for the internal network from unauthorized or malicious access, but it does not protect the file server or the external network from attacks if the file server is exposed to the internet or if the external network is compromised. Therefore, enhancing internal firewalls is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users4.
Implement a secure protocol: This means that the organization uses a secure and standardized protocol, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), to transfer files between its file server and external users. This can provide some level of security and integrity for the data transmission, but it does not protect the file server or the internal network from attacks if the protocol is exploited or if the external users are malicious. Therefore, implementing a secure protocol is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users5. References: 1: What Is a DMZ Network and Why Would You Use It? | Fortinet 2: Demilitarised zone (DMZ) | Cyber.gov.au 3: What Is VPN Tunneling? | Fortinet 4: Firewall - Wikipedia 5: Secure Shell - Wikipedia

NEW QUESTION: 393
資訊系統審計員正在審□應用程式變更的相關文件。下列哪一項發現最令人擔憂？
A. 測試文件以紙本形式保存。
B. 測試文件在使用者驗收測試 (UAT) 完成之前獲得批准。
C. 測試文件的日期比系統實施日期早三週。
D. 測試文件未顯示經理批准。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 394
為了幫助確定是否應該採用依賴控制的方法對公司的財務系統進行審計，哪種資訊系統審計工作的順序最適合？
A. 對財務交易進行詳細審□，然後審核總帳
B. 對主要財務應用進行審□，隨後審□IT 治理流程。
C. 對應用程式控制進行審□，然後測試關鍵業務流程控制
D. 先檢視一般資訊系統控制，然後檢討應用控制
Answer: (SHOW ANSWER)

NEW QUESTION: 395
對於審口組織業務連續性計畫 (BCP) 的資訊系統審計師而言，下列何者最應引起重視？
A. BCP 的聯絡資訊需要更新
B. 業務連續性計劃 (BCP) 沒有版本控制。
C. 業務連續性計畫尚未獲得高階主管的批准。
D. 業務連續性計劃自首次發布以來尚未經過測試。
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor reviewing an organization's business continuity plan (BCP) is that the BCP has not been tested since it was first issued. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include information such as roles and responsibilities, recovery strategies, resources,procedures, communication plans, and backup arrangements3. Testing the BCP is a vital step in ensuring its validity, effectiveness, and readiness. Testing the BCP involves simulating various scenarios and executing the BCP to verify whether it meets its objectives and requirements. Testing the BCP can also help to identify and correct any gaps, errors, or weaknesses in the BCP before they become issues during a real incident4. Therefore, an IS auditor should be concerned if the BCP has not been tested since it was first issued, as it may indicate that the BCP is outdated, inaccurate, incomplete, or ineffective. The other options are less concerning or incorrect because:
A). The BCP's contact information needs to be updated is not a great concern for an IS auditor reviewing an organization's BCP, as it is a minor issue that can be easily fixed. Contact information refers to the names, phone numbers, email addresses, or other details of the people involved in the BCP execution or communication. Contact information needs to be updated regularly to reflect any changes in personnel or roles. While having outdated contact information may cause some delays or confusion during a BCP activation, it does not affect the overall validity or effectiveness of the BCP.
B). The BCP is not version controlled is not a great concern for an IS auditor reviewing an organization's BCP, as it is a moderate issue that can be improved. Version control refers to the process of tracking and managing changes made to the BCP over time. Version control helps to ensure that only authorized changes are made to the BCP and that there is a clear record of who made what changes when and why. Version control also helps to avoid conflicts or inconsistencies among different versions of the BCP. While having no version control may cause some difficulties or risks in maintaining and updating the BCP, it does not affect the overall validity or effectiveness of the BCP.
C). The BCP has not been approved by senior management is not a great concern for an IS auditor reviewing an organization's BCP, as it is a high-level issue that can be resolved. Approval by senior management refers to the formal endorsement and support of the BCP by the top executives or leaders of the organization.

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

NEW QUESTION: 396
資訊系統審計員發現，一個仍在正常使用的軟體系統已經過時多年且不再受支援。受審計方表示，需要六個月的時間才能將軟體升級到最新版本。下列哪一項是降低使用不受支援的軟體版本所帶來的直接風險的最佳方法？
A. 驗證所有修補程式是否已應用於軟體系統的過時版本。
B. 關閉過時軟體系統上所有未使用的連接埠。
C. 監控嘗試存取過時軟體系統的網路流量。
D. 將過時的軟體系統與主網路隔離。
Answer: D (LEAVE A REPLY)
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. This will limit the exposure of the system to potential attacks and prevent it from compromising other systems on the network. Segregating the system will also reduce the impact of any security incidents that may occur on the system.
Monitoring network traffic attempting to reach the outdated software system (option C) is not the best way to reduce the risk, as it will not prevent or stop any attacks on the system. It will only provide visibility into the network activity and alert the auditee of any suspicious or malicious traffic.
Verifying all patches have been applied to the software system's outdated version (option A) and closing all unused ports on the outdated software system (option B) are also not the best ways to reduce the risk, as they will not address the underlying issue of using an unsupported version of the software. Patches and ports may still have vulnerabilities that are not fixed by the vendor, and attackers may exploit them to gain access to the system. Therefore, option D is the correct answer.
References:
Introduction (Part 1 of 7: Mitigating Risks of Unsupported Operating Systems) Summary (Part 7of 7: Mitigating Risks of Unsupported Operating Systems) Upgrade, Retire, or Replace Unsupported Software (Part 4 of 7: Mitigating Risks of Unsupported Operating Systems)

NEW QUESTION: 397
對 IS 審計師來口，在進行法務調口時，下列何者是確保資訊保存的最有效方法？
A. 強化電腦硬體和軟體。
B. 影像殘留資料和已刪除的檔案。
C. 對系統日誌和入侵偵測系統 (IDS) 日誌進行編碼。
D. 記錄與第三方的所有應用程式介面 (API) 連線。
Answer: B (LEAVE A REPLY)
The forensic principle is to preserve evidence in its original state. Imaging-including capturing residual and deleted data-ensures that the full contents of a storage device are preserved for analysis while maintaining the chain of custody. Hardening (A) may alter system state. Encoding logs (C) is not preservation but transformation. Documenting APIs (D) helps investigation scope but does not preserve evidence. ISACA guidance on digital forensics stresses the importance of bit-level imaging and ensuring evidence integrity through hashing and proper custody documentation.
References (ISACA): ISACA Incident Response and Forensics Guidance; ISACA Journal - Forensic Readiness.

NEW QUESTION: 398
下列哪一項審計證據蒐集程序最可靠？
A. 檢口從獨立第三方取得的紙本文件
B. 檢口控制所有者提供的系統口生證據
C. 審口從受審計單位收到的關鍵數據
D. 獨立於控制所有者執行手動程序
Answer: D (LEAVE A REPLY)
The most reliable evidence is evidence obtained directly by the auditor through independent performance of procedures. ISACA guidance notes that higher-assurance audit work is achieved when evidence is produced directly by auditors, or at least strictly under their control, rather than being supplied by the entity being audited.
Option D is correct because independently performing manual procedures gives the auditor direct control over the evidence-gathering process and reduces reliance on the auditee or control owner. In audit theory and in ISACA-aligned practice, evidence obtained directly by the auditor is generally more reliable than evidence merely provided by the auditee.
Option A is strong evidence because it comes from an independent third party, but it is still inspected rather than generated directly by the auditor. It is generally very reliable, but not as strong as auditor-generated evidence through independent reperformance.
Option B is less reliable because system-generated evidence provided by a control owner still depends on the completeness and integrity of what was selected and presented by the auditee.

Option C is the least reliable among the plausible choices because critical data received from an auditee is subject to the greatest dependence on management representation and auditee-controlled extraction.
Therefore, D is the best answer because evidence generated through procedures performed independently by the auditor is the most reliable.
References (Official ISACA):
* ISACA Journal, Capability Maturity Model and Risk Register Integration - "evidence is produced directly by the auditors or, if strictly under the auditors' control, by the entity's staff."
* ISACA Journal, A Factory Model Approach to Technology Control Testing - emphasizes gathering evidence, analyzing it, and substantiating results within a governed testing process.
* ISACA, ITAF update announcement - confirms ITAF as ISACA's professional framework for audit standards and guidance.

NEW QUESTION: 399
資訊資□分類的主要好處在於：
A. 防止資□損失。
B. 有助於協調組織目標。
C. 有助於預算的準確性。
D. 支援風險管理決策。
Answer: D (LEAVE A REPLY)
The primary benefit of information asset classification is that it enables risk management decisions.
Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

NEW QUESTION: 400
對於涉及資料傳輸的作業排程過程，下列何者是最佳的偵測控制措施？
A. 每月作業失敗量指標由高階管理層報告和審□。
B. 作業按計畫每天完成，資料使用安全文件傳輸協定(SFTP) 傳輸。
C. 作業已安排，並且此活動的日誌將保留以供後續審□。
D. 作業失敗警報會自動□生並傳送給支援人員。
Answer: D (LEAVE A REPLY)

The best detective control for a job scheduling process involving data transmission is job failure alerts that are automatically generated and routed to support personnel. Job failure alerts are notifications that indicate when a scheduled job or task fails to execute or complete successfully, such as due to errors, interruptions, or delays. Job failure alerts can help detect and correct any issues or anomalies in the job scheduling process involving data transmission by informing and alerting the support personnel who can investigate and resolve the problem. The other options are not as effective as job failure alerts in detecting issues or anomalies in the job scheduling process involving data transmission, as they do not provide timely or specific information or feedback. Metrics denoting the volume of monthly job failures are reported and reviewed by senior management is a reporting technique that can help measure and improve the performance and reliability of the job scheduling process, but it does not provide immediate or detailed information on individual job failures.
Jobs are scheduled to be completed daily and data is transmitted using a Secure File Transfer Protocol (SFTP) is a preventive control that can help ensure the timeliness and security of the job scheduling process involving data transmission, but it does not detect any issues or anomalies that may occur during the process. Jobs are scheduled and a log of this activity is retained for subsequent review is a logging technique that can help record and track the status and results of the job scheduling process involving data transmission, but it does not provide real-time or proactive information on job failures. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 401
下列哪一項措施能提供最有效的防護，抵禦新出現的威脅？
A. 非軍事區(DMZ)
B. 口發式入侵偵測系統(IDS)
C. 防毒軟體的即時更新
D. 基於特徵的入侵偵測系統(IDS)
Answer: (SHOW ANSWER)
A heuristic intrusion detection system (IDS) provides the most protection against emerging threats, as it uses behavioral analysis and anomaly detection to identify unknown or zero-day attacks. A heuristic IDS can adapt to changing patterns and learn from previous incidents, making it more effective than a signature-based IDS, which relies on predefined rules and signatures to detect known attacks. A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, and it can provide some protection against external threats, but not against internal or emerging threats. Real-time updating of antivirus software is important to protect against malware, but it may not be sufficient to prevent new or sophisticated attacks that exploit unknown vulnerabilities. References: CISA Review Manual (Digital Version) 1, page 452-453.

NEW QUESTION: 402

用於企業連接外部資源的網路代理伺服器可以透過以下方式降低組織風險：
A. 透過更改 IP 位址匿名化使用者。
B. 提供多因素身份驗證以增強安全性。
C. 提供比直接存取更快的回應速度。
D. 負載平衡流量以最佳化資料路徑。
Answer: A (LEAVE A REPLY)
A web proxy server for corporate connections to external resources reduces organizational risk by anonymizing users through changed IP addresses. A web proxy server is an intermediarybetween the web and client devices, that can provide proxy services to a client or a group of clients1. One of the main benefits of using a web proxy server is that it allows users to change their IP address andlocation, circumventing geoblocking and hiding their identity from the target website2.
Anonymizing internal IP addresses is important for online security, as it helps protect the organization from several threats. If an attacker controls a server that employees connect to, the outgoing IP address of the organization's router is logged on the server. This IP address can be used by the attacker to launch a denial-of- service (DoS) attack or to create more targeted attacks such as phishing2. With a web proxy server, the IP shown in web logs is the web proxy's, which means an attacker would not have access to theorganization's router outgoing IP address2.
Anonymizing outgoing IP addresses is also important when carrying out sensitive actions online, such as law enforcement investigations or competitive intelligence. A web proxy server can help users avoid exposing their internal IP address that leads back to their organization, and instead use a third-party web proxy that provides more anonymity2.
The other options are not directly related to reducing organizational risk by using a web proxy server. Providing multi-factor authentication for additional security (option B) is a benefit of some web proxy servers, but it is not the main purpose of using a web proxy server3. Providing faster response than direct access(option C) is a benefit of some web proxy servers that cache content forbetter data transfer speeds and less bandwidth usage, but it is not directly related to reducing organizational risk1. Load balancing traffic to optimize data pathways (option D) is a benefit of some web proxy servers that distribute traffic across multiple servers, but it is not directly related to reducing organizational risk4.
References: 1: Proxy servers and tunneling 2: Multi-factor authentication: How to enable 2FA and boost your security 3: What Is Multi-factor Authentication (MFA) Security? 4: How it works: Microsoft Entra multifactor authentication

NEW QUESTION: 403
下列哪一項最能描述創建數位信封的過程？
A. 使用對稱加密對訊息進行編碼後，加密金鑰被壓縮在資料夾中。
B. 使用對稱加密對訊息進行編碼，然後使用公鑰加密保護加密金鑰。
C. 訊息被雜湊，並且散列總數使用對稱加密發送。

D. 使用非對稱加密對訊息摘要進行加密，並使用非對稱加密發送加密金鑰
Answer: B (LEAVE A REPLY)
A digital envelope combines the strengths of symmetric and asymmetric cryptography. The message itself is encrypted using a fast symmetric algorithm. The session key used for symmetric encryption is then encrypted using the recipient's public key. This ensures efficiency (large data encrypted quickly with symmetric keys) and security (session key securely transmitted using asymmetric encryption). Options A, C, and D describe other cryptographic processes (compression, hashing, or digital signatures) but do not correctly represent a digital envelope. ISACA training materials and CISA manuals highlight this hybrid approach as the standard method for secure data transmission.
References (ISACA): CISA Review Manual - Cryptography Concepts; ISACA Glossary.

NEW QUESTION: 404
下列哪一項是組織確保資訊系統審計中商定的行動計畫得到實施的最有效方法？
A. 確保分配充足的審計資源，
B. 向全組織傳達審計結果。
C. 確保已分配所有權。
D. 測試完成後所採取的矯正措施。
Answer: (SHOW ANSWER)
The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management. This will ensure accountability, commitment, and follow-up for the audit recommendations34. References: 3: CISA ReviewManual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 41 4: CISA Online Review Course, Module 1:
The Process of Auditing Information Systems, Lesson 1.6: Reporting

NEW QUESTION: 405
下列哪一項存取權限授予系統開發團隊的新成員時風險最大？
A. 對生口程式庫的寫入權限
B. 對開發資料庫的寫入權限
C. 執行對生口程序庫的訪問
D. 執行對開發程式庫的訪問
Answer: A (LEAVE A REPLY)
Write access to production program libraries presents the greatest risk when granted to a new member of the system development staff. Production program libraries contain executable code that runs on live systems and supports critical business functions. Write access allows a user to modify or delete existing programs, or add new programs to the library. If a user were to make unauthorized or erroneous changes to production programs,

it could cause serious disruptions, errors, or security breaches in the organization's operations.
Therefore, writeaccess to production program libraries should be restricted to authorized personnel only, and subject to strict change management controls.

NEW QUESTION: 406
某組織計劃實施居家辦公政策，允許使用者根據需要遠端辦公 下列哪一項是確保安全遠端存取公司資源的最佳解決方案？
A. 附加防火牆規則
B. 多因素身份驗證
C. 虛擬私人網路(VPN)
D. 虛擬桌面
Answer: C (LEAVE A REPLY)
The best solution for ensuring secure remote access to corporate resources is to use a virtual private network (VPN), as this creates an encrypted tunnel between the user's device and the corporate network, preventing unauthorized interception or modification of data in transit. Additional firewall rules may help to restrict access to certain ports or protocols, but they do not provide encryption or authentication. Multi-factor authentication may help to verify the identity of the user, but it does not protect the data in transit. Virtual desktop may help to provide a consistent user interface and access to applications, but it does not ensure the security of thecommunication channel. References: CISA Review Manual (Digital Version), Chapter 5:
Protection of Information Assets, Section 5.2: Network Security Devices and Technologies

NEW QUESTION: 407
在受控的應用開發環境中，最重要的職責分離應該體現在將變更實施到生口環境的人員與下列人員之間：
A. 應用程式設計師
B. 系統程式設計師
C. 電腦操作員
D. 品質保證(QA)人員
Answer: A (LEAVE A REPLY)

In a controlled application development environment, the most important segregation of duties should be between the person who implements changes into the production environment and the application programmer. This segregation of duties ensures that no one person can create and deploy code without proper review, testing, and approval. This reduces the risk of errors, fraud, or malicious code being introduced into the production environment.
The other options are not as important as the segregation between the application programmer and the person who implements changes into production, but they are still relevant for achieving a secure and reliable application development environment. The segregation of duties between the person who implements changes into production and the systems programmer is important to prevent unauthorized or untested changes to system software or configuration. The segregation of duties between the person who implements changes into production and the computer operator is important to prevent unauthorized or uncontrolled access to production data or resources. The segregation of duties between the person who implements changes into production and the quality assurance (QA) personnel is important to ensure independent verification and validation of code quality and functionality.
References:
ISACA CISA Review Manual 27th Edition (2019), page 247
Segregation of Duties in an Agile Environment | AKF Partners3
Separation of Duties: How to Conform in a DevOps World4

NEW QUESTION: 408
下列何者最有利於成功實施IT效能監控？
A. 建立定期向管理階層報告的模板
B. 確定 IT 資源和流程的目標
C. 辨識用於自動化績效衡量的工具
D. 採用全球標準與計量規範
Answer: C (LEAVE A REPLY)

NEW QUESTION: 409
為了透過使用非對稱加密來確保機密性，訊息使用下列哪種方式進行加密？
A. 收件者的公鑰
B. 發送方的私鑰
C. 發送方的公鑰
D. 收件者的私鑰
Answer: A (LEAVE A REPLY)
The best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A). This is because:

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner12. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key12.
Encrypting a message with the recipient's public key ensures that only the recipient can decrypt it with their private key. This provides confidentiality, which means that the message is protected from unauthorized access or disclosure12.
Encrypting a message with the sender's private key (option B) does not ensure confidentiality, but rather authentication, which means that the message can be verified as coming from the sender. This is because anyone can decrypt the message with the sender's public key, but only the sender can encrypt it with their private key12.
Encrypting a message with the sender's public key (option C) or the recipient's private key (option D) does not make sense, as it would render the message unreadable by both parties. This is because neither party has the corresponding key to decrypt it12.
Therefore, the best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A), as this ensures that only the recipient can decrypt it with their private key.
References: 1: What is asymmetric encryption? | Asymmetric vs. symmetric ... - Cloudflare 2: What is Asymmetric Encryption? - GeeksforGeeks

NEW QUESTION: 410
控制自我評估(CSA)引導員的主要職責是：
A. 進行訪談以獲取背景資訊。
B. 讓團隊專注於口部控制。
C. 報告口部控制缺陷。
D. 為控制缺陷提供解決方案。
Answer: (SHOW ANSWER)
The primary role of a control self-assessment (CSA) facilitator is to focus the team on internal controls. A CSA facilitator is a person who guides the CSA process and helps the participants to identify, assess, and improve their internal controls. The facilitator does not conduct interviews, report on weaknesses, or provide solutions, as these are the responsibilities of the participants themselves1.
The other options are incorrect because they are not the primary role of a CSA facilitator. Option A, conduct interviews to gain background information, is a preliminary step that may be done by the facilitator or the participants before the CSA session, but it is not the main purpose of the facilitator. Option C, report on the internal control weaknesses, is an outcome of the CSA process that should be done by the participants who own and operate the controls. Option D, provide solutions for control weaknesses, is also an outcome of the

CSA process that should be done by the participants who are in charge of implementing the improvements.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, page 2822
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription, QID
1066693
PwC, Control Self Assessments4
Workiva, 4factors of an effective control self-assessment (CSA) program5

NEW QUESTION: 411
對於評估組織變更管理流程的資訊系統稽核員而言，下列何者最為重要？
A. 部分會議的變更管理會議記錄缺失。
B. 變更請求不進行優先權排序。
C. 變更在部署到生口環境後獲得批准。
D. 不存在緊急變更的授權請求者清單。
Answer: (SHOW ANSWER)
The best answer is C. Changes are approved after being moved to production.
ISACA guidance on change management emphasizes reviews, testing, approvals, and segregation of duties before moving changes forward. If changes are moved into production before approval, the organization has effectively bypassed one of the most important preventive controls in the change process. That creates direct risk of unauthorized, untested, or harmful changes reaching production.
Option A is a documentation weakness. Option B reduces efficiency and prioritization discipline. Option D is a concern for emergency changes, but it is still less severe than routinely approving changes only after implementation. In audit terms, post-production approval represents a fundamental control breakdown.
References (Official ISACA):
* ISACA Journal, Speeding Up Software Delivery With Effective Change Management.

NEW QUESTION: 412
某組織計劃集中停用已過時的資料庫，並將資料移轉到最新型號的硬體上。下列哪一項措施最能確保在遷移過程中資料完整性得到保障？
A. 資料加密
B. 將樣本資料與最新備份進行核對
C. 比較校驗和
D. 混淆機密數據
Answer: C (LEAVE A REPLY)

NEW QUESTION: 413

為了使安全意識培訓發揮最大作用，管理階層應確保培訓：
A. 每年發生一次。
B. 由 IT 人員進行。
C. 針對特定群體量身訂做。
D. 涵蓋 IT 環境的各個面向。
Answer: (SHOW ANSWER)

NEW QUESTION: 414
下列哪項控制措施對於確保組織在災難發生時能口從備份媒體中復原資料最為關鍵？
A. 將備份媒體儲存在異地設施中
B. 保持備份媒體的最新庫存清單
C. 定期還原關鍵資料庫的備份介質
D. 對備份媒體上的資料進行加密
Answer: C (LEAVE A REPLY)
The best answer is C. Periodically restoring backup media for key databases.
ISACA guidance is very clear that backup restoration should be tested periodically. A backup is only useful if it can actually be restored successfully within business needs. Organizations sometimes assume that because backups exist, recovery is assured, but ISACA specifically warns that recovery procedures and restoration capability must be tested.
Option A is important for resilience, but offsite storage does not prove the backup is recoverable. Option B helps administration and tracking, but inventory alone does not validate restorability. Option D protects confidentiality of backup data, but it does not ensure successful recovery. The strongest control for recoverability is periodic test restoration.
References (Official ISACA):
* ISACA, Ensuring Data Security: The Importance of Cloud Backups and Drill Testing
* ISACA Journal, Governance of Key Aspects of System Patch Management - recommends periodic testing of backup restoration.
* ISACA Journal, IS Audit Basics: Backup and Recovery

NEW QUESTION: 415
資訊系統審計發現，某組織並未主動解決已知的安全漏洞。資訊系統審計員應建議該組織先採取下列哪一項措施？
A. 驗證災難復原計畫(DRP)是否已進行測試。
B. 確保入侵防禦系統(IPS)有效。
C. 評估企業面臨的安全風險。
D. 確認事件回應團隊了解問題。
Answer: C (LEAVE A REPLY)

If an IS audit reveals that an organization is not proactively addressing known vulnerabilities, the IS auditor should recommend that the organization assess the security risks to the business first, as this would help to prioritize the vulnerabilities based on their impact and likelihood, and determine the appropriate mitigation strategies. Verifying the disaster recovery plan (DRP) has been tested, ensuring the intrusion prevention system (IPS) is effective, and confirming the incident response team understands the issue are important steps, but they are not as urgent as assessing the security risks to the business.
References: CISA Review Manual (Digital Version), Chapter 5, Section 5.6

NEW QUESTION: 416
由於近期洪水風險地圖顯示資料中心所在位置的風險發生變化，管理層已同意遷移該資料中心。目前採取了哪種風險因應措施？
A. 風險消除
B. 風險規避
C. 風險轉移
D. 風險接受
Answer: B (LEAVE A REPLY)

NEW QUESTION: 417
下列哪一項技術最適合滿足企業對與外部各方進行企業間交易時不可否認的業務需求，而無需相互信任的實體？
A. 公鑰基礎設施(PKI)
B. 區塊鏈分散式帳本
C. 集中式帳本技術
D. 人工智慧(AI)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 418
如果使用下列哪一種滅火系統來保護資口儲存櫃，資訊系統稽核員最應該關注？
A. 洪水系統
B. 濕式管道系統
C. 預作用系統
D. 二氧化碳系統
Answer: D (LEAVE A REPLY)
A CO2 system could be a concern for an IS auditor when used to protect an asset storage closet. While CO2 systems are effective at suppressing fires, they can pose a significant safety risk to personnel. In the event of a fire,the CO2 system would fill the room with carbon dioxide, displacing the oxygen. This could be hazardous to anyone who might be in the room at the time12.
References: ISACA's Information Systems Auditor Study Materials1

NEW QUESTION: 419
風險管理的首要目標是將風險總成本控制在以下水準：
A. 物理安全措施的平均成本。
B. 公司預算中包含的預計損失金額
C. 會對公司造成重大損害的損失金額。
D. 風險管理的行政成本。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 420
對於正在審計最近遭受勒索軟體攻擊的組織的IS審計員來口，下列哪一項應該是他們最關注的問題？
A. 即使防毒軟體已正確更新，也未能阻止此攻擊。
B. 最新的安全性修補程式在實施前未經測試。
C. 備份僅在本地網路口執行。
D. 員工未接受過網路安全政策和程序的培訓
Answer: (SHOW ANSWER)
The greatest concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack is that backups were only performed within the local network. This means that the backups could have been encrypted or deleted by the ransomware, making it impossible to restore the data and systems without paying the ransom or losing the data. Backups are a critical part of the recovery process from a ransomware attack, and they should be performed frequently, securely, and off-site or in the cloud to ensure their availability and integrity.
The other options are not as concerning as option C, although they may also indicate some security weaknesses. Antivirus software was unable to prevent the attack even though it was properly updated, but this is not surprising given that ransomware variants are constantly evolving and antivirus software may not be able to detect them all. The most recent security patches were not tested prior to implementation, but this is a trade-off between security and availability that may be justified depending on the severity and urgency of the patches. Employees were not trained on cybersecurity policies and procedures, but this is a preventive measure that may not have prevented the attack if it was initiated by other means such as phishing or exploiting vulnerabilities.
References:
10: Infrastructure-as-a-Service Security Responsibilities - CloudTweaks
5: 3 steps to prevent and recover from ransomware | Microsoft Security Blog
7: How to Recover From a Ransomware Attack - eSecurityPlanet

NEW QUESTION: 421
數據通訊系統審計的第一步是確定：
A. 交通量與反應時間標準

B. 網路設備的實體安全
C. 各種通訊路徑中的冗餘級別
D. 業務用途和要傳輸的訊息類型
Answer: D (LEAVE A REPLY)
The first step in auditing a data communication system is to determine the business use and types of messages to be transmitted. This is because the auditor needs to understand the purpose, scope, and objectives of the data communication system, as well as the nature, volume, and sensitivity of the data being transmitted. This will help the auditor to identify the risks, controls, and audit criteria for the data communication system.
Traffic volumes and response-time criteria, physical security for network equipment, and the level of redundancy in the various communication paths are important aspects of a data communication system, but they are not the first step in auditing it. They depend on the business use and types of messages to be transmitted, and they may vary according to different scenarios and requirements. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 422
下列哪一項提供了維護推送至員工自有行動裝置的企業應用程式安全性的 BE ST 方法？
A. 口用遠端資料銷毀功能
B. 實施行動裝置管理(MDM)
C. 停用不必要的網路連線選項
D. 要求行動用口接受安全意識培訓
Answer: B (LEAVE A REPLY)
The best method for maintaining the security of corporate applications pushed to employee-owned mobile devices is implementing mobile device management (MDM). MDM is a software solution that allows an organization to remotely manage, configure, and secure the mobile devices that access its network and data.
MDM can help protect corporate applications on employee-owned devices by:
Enforcing security policies and settings, such as encryption, password, firewall, antivirus, and VPN.
Controlling the installation, update, and removal of corporate applications and data.

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

NEW QUESTION: 423
資訊系統審計員從修補程式日誌中發現，部分審計範圍口的系統未依常規修補程式計畫進行更新。審計員下一步該怎麼做？
A. 採訪 IT 管理人員，以明確目前流程。
B. 將此發現報告給高階管理層。
C. 檢視組織的修補程式管理策略。

D. 要求制定行動計畫作為後續事項。

Answer: C (LEAVE A REPLY)

The IS auditor should review the organization's patch management policy to determine the expected frequency and scope of patching, as well as the roles and responsibilities of the patch management team. This will help the auditor assess the severity and impact of the non-compliance, and identify the root cause and possible remediation actions12.

References

1: How to Create a Patch Management Policy: Complete Guide 2: Free Patch Management Policy Template (+Examples)

NEW QUESTION: 424

下列哪一項是緩解將網路流量重新導向到未經授權網站的攻擊的最佳控制措施？

A. 定期進行使用者安全意識培訓。

B. 強制執行強大的 Web 瀏覽器安全控制。

C. 執行網域名稱系統(DNS)伺服器安全加固。

D. 實作 Web 應用程式防火牆 (WAF)。

Answer: C (LEAVE A REPLY)

The best answer is C.

ISACA's glossary defines DNS poisoning as a cyberattack that alters DNS records to redirect users to fraudulent websites. Since the attack mechanism is DNS manipulation, the strongest control among the choices is DNS server security hardening. That directly addresses the infrastructure being targeted.

Option A can reduce user susceptibility but does not directly prevent redirection attacks. Option B can help at the endpoint, but it does not address poisoned or compromised DNS infrastructure as directly as DNS hardening. Option D is designed mainly to protect web applications from HTTP-layer attacks, not to stop DNS-based traffic redirection.

References (Official ISACA):

* ISACA Glossary, Domain name system (DNS) poisoning.

NEW QUESTION: 425

下列哪一項是實施資料保留策略的最佳理由？

A. 為災難復原程序建立復原點目標 (RPO)。

B. 限制與儲存和保護資訊相關的責任

C. 用於記錄組織口部資料處理的業務目標

D. 將資料保護的責任和所有權分配給 IT 部門以外的人員。

Answer: B (LEAVE A REPLY)

The best reason to implement a data retention policy is to limit the liability associated with storing and protecting information. A data retention policy is a business' established protocol for maintaining information, typically defining what data needs to be retained, the format in which it should be kept, how long it should be stored for, whether it should

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

NEW QUESTION: 426
資料中心為防止停電期間未經授權的人員進入，應確保外部出入口暢通：
A. 請準備實體鑰匙。
B. 以故障安全模式運作。
C. 以故障安全模式運作。
D. 受到警報和監控。
Answer: (SHOW ANSWER)
The best answer is C. Operate in fail-secure mode.
If the goal is to prevent unauthorized entry during a power outage, the doors should remain locked when power fails. That is exactly what fail-secure operation is intended to do.
Alarming and monitoring may detect an issue, but they do not themselves prevent entry.
Physical key backup may help authorized access, but it does not address the primary requirement of staying secure during loss of power.
So the strongest answer is fail-secure, because it directly preserves physical access control during an outage.
References (Official ISACA):
* ISACA physical security and access-control terminology resources support layered protection of facilities.

NEW QUESTION: 427
在軟體開發生命週期的哪個階段最適合開始討論應用程式控制？
A. 商業案例開發階段，此時需要確定利害關係人。

B. 應用程式設計階段流程功能已最終確定
C. 使用者驗收測試(UAT)階段，此時測試場景已設計完成
D. 應用程式編碼階段，在此階段開發演算法以解決業務問題
Answer: B (LEAVE A REPLY)
The best phase of the software development life cycle to initiate the discussion of application controls is the application design phase when process functionalities are finalized. Application controls are the policies, procedures, and techniques that ensure the completeness, accuracy, validity, and authorization of data input, processing, output, and storage in an application. Application controls help prevent, detect, or correct errors and fraud in software applications. Examples of application controls include input validation, edit checks, reconciliation, encryption, access control, audit trails, etc.
The application design phase is when the software requirements are translated into a logical and physical design that specifies how the application will look and work. This phase is the best time to discuss application controls because it allows the developers to incorporate them into the design specifications and ensure that they are aligned with the business objectives and user needs. By discussing application controls early in the design phase, the developers can also avoid costly rework or changes later in the development process.
The other phases are not as optimal as the application design phase to initiate the discussion of application controls. A. Business case development phase when stakeholders are identified. The business case development phase is when the feasibility, scope, objectives, benefits, risks, and costs of a software project are defined and evaluated. This phase is important for obtaining stakeholder approval and support for the project, but it is too early to discuss application controls in detail because the software requirements and functionalities are not yet clear or finalized. B. User acceptance testing (UAT) phase when test scenarios are designed. The user acceptance testing phase is when the software is tested by the end-users or stakeholders to verify that it meets their expectations and requirements. This phase is too late to discuss application controls because it is near the end of the development process and any changes or additions to the application controls would require retesting and revalidation of the software. C. Application coding phase when algorithms are developed to solve business problems. The application coding phase is when the software design is translated into executable code using programming languages and tools. This phase is not ideal to discuss application controls because it is after the design phase and any changes or additions to the application controls would require redesigning and recoding of the software.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2 What Is Application Control? | McAfee3 What Is Application Lifecycle Management? | Red Hat4

NEW QUESTION: 428
對於審□組織營運日誌管理的IS稽核員來□，下列何者最□得關注？
A. 應用程式正在將事件記錄到多個日誌檔案中。
B. 所有日誌的資料格式尚未標準化。
C. 日誌檔案大小逐年成長。
D. 關鍵事件將被記錄到不可變的日誌檔案中。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 429
迴歸測試最常用於哪個流程？
A. 系統修改
B. 壓力測試
C. 單元測試
D. 程式開發
Answer: (SHOW ANSWER)

NEW QUESTION: 430
下列哪一項最能顯示事件管理流程是有效的？
A. IT 管理階層審□的事件數量增加
B. 事件解決時間縮短
C. 報告的重大事件數量增加
D. 服務台來電數量減少
Answer: (SHOW ANSWER)

NEW QUESTION: 431
在對資□管理審計進行後續跟進時，資訊系統審計員發現已支付的IT設備發票未記錄在組織的庫存中。下列哪一項是審計員的最佳行動方案？
A. 詢問資□管理人員設備在哪裡。
B. 記錄證據，以便將其納入未來審計的範圍。
C. 向審計和營運管理部門通報差異。
D. 忽略發票，因為它們不屬於後續跟進的一部分。
Answer: C (LEAVE A REPLY)

NEW QUESTION: 432
在對IT組織結構進行審計時，下列哪一項發現對組織構成最大風險？
A. 營業額顯著較高
B. 缺乏顧客滿意度調□
C. 老齡員工
D. 軟體升級頻率增加
Answer: A (LEAVE A REPLY)

High employee turnover (A) poses the greatest risk because it leads to knowledge loss, operational disruptions, and potential security risks from departing employees. A constantly changing workforce can also impact compliance, training, and overall IT stability.
Other options:
Lack of customer satisfaction surveys (B) is a business issue but not a critical IT risk.
Aging staff (C) may be a long-term risk but does not have an immediate impact.
Frequent software upgrades (D) can be beneficial if managed correctly.
Reference: ISACA CISA Review Manual, IT Governance and Management of IT

NEW QUESTION: 433
下列哪一項闡明了業務連續性計劃 (BCP) 和災難復原計劃 (DRP) 之間的主要差異？
A. 年度測試要求
B. 重點關注系統恢復
C. 計畫口動的時間範圍
D. 高階主管的參與
Answer: (SHOW ANSWER)
The primary difference between a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) lies in their timeframe for activation and overall scope.
BCP (Business Continuity Plan):
Focuses on ensuring that critical business processes continue operating during and after a disruption.
It includes strategies for maintaining operations (e.g., alternative work locations, manual procedures, supplier dependencies).
Activated immediately when a disruption occurs to keep the business running.
DRP (Disaster Recovery Plan):
Primarily focuses on the recovery of IT systems and infrastructure after a disruption.
It includes steps for restoring data, servers, and applications to bring IT operations back to normal.
Activated after the disaster event to restore normal IT operations.
The timeframe for activation is the key difference because:
BCP is implemented immediately to ensure business continuity.
DRP is implemented after the disaster to restore IT operations.
A). The annual testing requirements # Both BCP and DRP require regular testing, so this is not the key differentiator.
B). The focus on system recovery # Only DRP focuses on system recovery, but the BCP covers more than just IT. The key difference is still the timeframe.
D). The involvement of senior management # Senior management is involved in both plans, so this is not the primary distinction.
References:ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience

NEW QUESTION: 434
在規劃雲端服務審計時，審計管理層發現指定的IT審計員不熟悉所使用的技術及其對業務帶來的相關風險。為確保審計質量，審計管理階層應先考慮下列哪些措施？
A. 經過適當的時間後進行後續審計。
B. 將審計任務重新安排到下一個財政年度。
C. 將審計工作重新分配給口部稽核領域的專家。
D. 延長審計期限，以便給審計人員更多時間
Answer: C (LEAVE A REPLY)
The best action that audit management should consider first is to reassign the audit to an internal audit subject matter expert. This is because cloud service audits require specialized knowledge and skills to assess the risks and controls associated with the cloud service provider and the cloud service customer. An IS auditor who is unfamiliar with the technologies in use and their associated risks to the business may not be able to perform an effective and efficient audit, and may miss important issues or provide inaccurate recommendations.
Therefore, it is important to ensure that the IS auditor assigned to the cloud service audit has the appropriate competence and experience.
The other options are not as good as reassigning the audit to an internal audit subject matter expert.
Conducting a follow-up audit after a suitable period has elapsed may not address the quality issues of the initial audit, and may also delay the identification and remediation of any problems. Rescheduling the audit assignment for the next financial year may expose the organization to unnecessary risks and may not meet the audit objectives or expectations. Extending the duration of the audit to give the auditor more time may not be feasible or cost-effective, and may not guarantee that the auditor will acquire the necessary knowledge and skills in time.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1391
ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, p. 14

NEW QUESTION: 435
容量管理工具的主要用途是確保：
A. 可用資源高效利用。
B. 電腦系統大部分時間都處於最大使用率狀態
C. 允許大量使用者同時使用
D. 建議的硬體採購滿足容量要求
Answer: A (LEAVE A REPLY)
Capacity management tools are primarily used to ensure that available resources are used efficiently and effectively to meet the current and future demands of the business. Capacity

management tools can help monitor, analyze and optimize the performance and utilization of IT resources such as CPU, memory, disk, network, etc. The other options are not the primary purpose of capacity management tools, although they may be related or derived from them. References:
ISACA, CISA Review Manual, 27th Edition,chapter 4, section 4.32
ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.2

NEW QUESTION: 436
一位資訊系統審計師正在審口一家在多個地區設有辦事處的組織的災難復原計畫 (DRP)。下列哪一項應該是審計師的主要關注點？
A. 復原點目標 (RPO) 監控
B. 進程與系統依賴關係
C. 災難復原培訓
D. 資料備份與儲存變化
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
For organizations with multiple regional offices, the primary audit focus should be on processes and system dependencies. Dependencies determine recovery sequencing, resource prioritization, and interconnectivity between systems across regions.
* RPO monitoring (A): Important but a subset of overall recovery planning.
* Training (C): Necessary but not the first priority when evaluating plan adequacy.
* Data backup/storage (D): Technical component but less comprehensive than analyzing dependencies.
# ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on disaster recovery planning and interdependencies.

NEW QUESTION: 437
如何才能最好地降低不準確或誤導性數據在商業智慧系統中擴散的風險？
A. 建立資料從一種格式轉換為另一種格式的規則
B. 為新應用程式和現有應用程式實施資料輸入控制
C. 實現一致的資料庫索引策略
D. 開發一個元資料儲存庫，用於儲存和存取元數據

Answer: A (LEAVE A REPLY)
The best way to reduce the risk of inaccurate or misleading data proliferating through business intelligence systems is to establish rules for converting data from one format to another, because this ensures that the data quality and integrity are maintained throughout the data transformation process. Data conversion rules define the standards, procedures, and methods for transforming data from different sources and formats into a common format andstructure that can be used by the business intelligence systems12. Implementing data entry controlsfor new and existing applications, implementing a consistent database indexing strategy, and developing a metadata repository to store and access metadata are not the best ways to reduce the risk of inaccurate or misleading dataproliferating through business intelligence systems, becausethey do not address the issue of dataconversion, which is a critical step in the data integration process for business intelligence systems. References: 1: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.3 2: CISA Online Review Course, Module 4, Lesson 3

NEW QUESTION: 438
下列哪一項是使用虛擬化環境的最大風險？
A. 主機可能是系統中潛在的單點故障。
B. 可能沒有足□的處理能力分配給客人。
C. 會話劫持的可能性可能會增加。
D. 更換作業系統的能力可能受到限制。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 439
對於審□組織工作排程實務的資訊系統稽核員來□，下列哪一項應該是最需要關注的問題？
A. 作業依賴項未定義。
B. 大多數的作業都是手動執行。
C. 工作在工作時間□執行。
D. 缺少作業處理程序。
Answer: (SHOW ANSWER)

NEW QUESTION: 440
偵□控制持續惡化導致下列哪一項影響最大？
A. 整體恢復時間縮短
B. 安全日誌中漏報數量增加
C. 根本原因分析的有效性降低
D. 原木儲存空間需求增加
Answer: B (LEAVE A REPLY)

NEW QUESTION: 441

在組織進行購買硬體以支援新網路伺服器的可行性研究中，下列哪一項的遺漏最為令人擔憂？

A. 收購融資的替代方案

B. 潛在供應商的財務穩定性

C. 潛在供應商的信譽

D. 現有口品的成本效益分析

Answer: D (LEAVE A REPLY)

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

References:

The Components of a Feasibility Study - ProjectEngineer

NEW QUESTION: 442

數位簽章的一個特點是：

A. 受接收器控制

B. 是訊息特有的

C. 當資料變更時進行驗證

D. 具有可複現的雜湊演算法

Answer: B (LEAVE A REPLY)

A digital signature is a specific type of e-signature that is backed by a digital certificate. A digital certificate is a document that contains the public key of a signer and is issued by a trusted third party called a certificate authority (CA). A digital signature provides proof of the identity of the signer and the integrity of the signed document.

A characteristic of a digital signature is that it is unique to the message. This means that a digital signature cannot be copied from one document to another without being detected as invalid. A digital signature is created by applying a mathematical function called a hashing algorithm to the document. A hashing algorithm produces a fixed-length output called a hash or digest from any input data. The hash is unique to the input data; any change in the input data will result in a different hash.

The signer then encrypts the hash with their private key (a secret key that only they know) to create the digital signature. The encrypted hash is attached to the document as the digital signature. The recipient of the document can verify the digital signature by decrypting it with the signer's public key (a key that is publicly available and matches the private key) to obtain the hash. The recipient then applies the same hashing algorithm to the document to generate another hash. The recipient then compares the two hashes; if they match, it means that the document has not been altered and that the signer is authentic.

Therefore, a digital signature is unique to the message because it is derived from the hash of the message, which is unique to the message.
References:
7: Free Online Signature Generator (Type or Draw) | Signaturely
8: What are digital signatures and certificates? | Acrobat Sign - Adobe
9: eSign PDF with Electronic Signature Free Online - Smallpdf

NEW QUESTION: 443
資訊系統稽核員發現，新的網路連線使得網際網路與□部企業資源計畫ERP)系統之間能□進行通訊。在向管理層報告這項發現時，下列哪一項是需要重點提及的主要業務影響？
A. ERP系統中資料品質下降
B. 威脅情勢加劇
C. 網路效能下降
D. 監理機關可能增加罰款
Answer: B (LEAVE A REPLY)

NEW QUESTION: 444
下列哪一項最能幫助 IS 審計師理解微服務導向的應用程式的輸入和輸出？
A. 資料流程圖
B. 網路架構圖
C. 業務需求文檔
D. 實體關係圖
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation:
For a microservices architecture, the most effective way to understand data movement between components is through data flow diagrams (DFDs). DFDs clearly show inputs, outputs, processes, and data stores, helping auditors trace data movement across distributed services.
Option A: Correct - DFDs highlight application inputs/outputs.
Option B: Network diagrams show infrastructure but not logical data flows.
Option C: Business requirements document functional needs, not technical flows.
Option D: ER diagrams describe database structures, not process flows.
ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on system documentation and data flow diagrams in audit analysis.

NEW QUESTION: 445
確定程式設計師是否擁有修改生□環境資料的權限的最佳方法是審□以下□容：
A. 存取控制系統的日誌設定。
B. 最新系統變更的實施方式。
C. 存取控制系統的配置。

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

NEW QUESTION: 446
資訊系統審計員正在審□網路拓撲圖。下列哪個位置最適合放置防火牆？
A. 非軍事區(DMZ)□
B. 虛擬區域網路(VLAN)之間
C. 位於具有不同安全等級的網路段邊界處
D. 每台主機與本機網路交換器/集線器之間
Answer: C (LEAVE A REPLY)

NEW QUESTION: 447
下列哪個應用程式具有最大的固有風險，應在審計計劃中優先考慮？
A. 已停用的遺留應用程式
B. 不支援的現場應用程式
C. 外包會計應用程式
D. □部開發的應用程式
Answer: (SHOW ANSWER)
An outsourced accounting application has the most inherent risk and should be prioritized during audit planning because it involves external parties, sensitive data, and complex

transactions that are susceptible to material misstatement, error, or fraud12. An outsourced accounting application also requires more oversight and monitoring from the internal audit department to ensure compliance with the service level agreement and the organization's policies and standards3.
References
1: Inherent Risk: Definition, Examples, and 3 Types of Audit Risks 2: 3 Types of Audit Risk - Inherent, Control and Detection - Accountinguide 3: IS Audit Basics: The Core of IT Auditing

NEW QUESTION: 448
下列哪一項措施最能保護在多個辦公室之間傳輸的敏感資料的機密性？
A. 刻耳柏洛斯
B. 公鑰基礎設施(PKI)
C. 哈希演算法
D. 數位簽名
Answer: (SHOW ANSWER)

NEW QUESTION: 449
下列哪一項與容量規劃相關的實務能□最大程度地確保防止未來發生與現有伺服器效能相關的事件？
A. 複製現有磁碟機系統以提高冗餘性和資料儲存能力
B. 對以往的績效事件進行根本原因分析
預計目前的服務等級協定 (SLA) 將保持不變
C. 檢視模擬高需求壓力測試場景的結果
Answer: C (LEAVE A REPLY)

NEW QUESTION: 450
下列哪一個指標最能衡量組織IT職能的敏捷性？
A. 每位IT員工的平均學習與訓練小時數
B. 根據最新標準和指南進行安全評估的頻率
C. 將策略性 IT 目標轉化為已達成共識並獲批准的措施所需的平均時間
D. 具備勝任其職位所需IT相關技能的員工百分比
Answer: C (LEAVE A REPLY)
The metric that would best measure the agility of an organization's IT function is average time to turn strategic IT objectives into an agreed upon and approved initiative. IT agility is the ability of an IT function to respond quickly and effectively to changing business needs and opportunities. By measuring how fast an IT function can translate strategic IT objectives into actionable initiatives, such as projects or programs, an organization can assess how well its IT function can align with and support its business strategy. Average number of learning and training hours per IT staff member, frequency of security assessments against the most recent standards and guidelines, and percentage of staff

with sufficient IT-related skills for the competency required of their roles are metrics that may indicate other aspects of IT performance, such as capability development, security maturity, and skills gap analysis, but they do not directly measure IT agility. References: ISACA Journal Article: Measuring IT Agility

NEW QUESTION: 451
在後續審計工作開始前，資訊系統審計師得知管理階層已決定接受與某項審計發現相關的剩餘風險，而不採取任何補救措施。資訊系統審計師對管理階層的這項決定感到擔憂。下列哪一項應該是資訊系統審計師的下一步？
A. 接受管理階層的決定並繼續跟進。
B. 向資訊系統審計管理部門報告此問題。
C. 向董事會報告分歧。
D. 向高階主管報告問題。
Answer: B (LEAVE A REPLY)
Prior to a follow-up engagement, if an IS auditor learns that management has decided to accept a level of residual risk related to an audit finding without remediation, the IS auditor should report the issue to IS audit management. This is because IS audit management is responsible for ensuring that audit findings are properly communicated and resolved. Accepting management's decision and continuing the follow-up would not address the IS auditor's concern. Reporting the disagreement to the board or executive management would be premature and inappropriate without consulting IS audit management first. References: CISA Review Manual (Digital Version), Chapter 1, Section 1.6

NEW QUESTION: 452
最能有效促進資訊系統資源高效利用的計費方式是：
A. 可追溯到特定用途的特定費用。
B. 達到滿載運轉所需的總利用率。
C. 超過實際發生成本的剩餘收益。
D. 根據吸收電荷的能力進行分配。
Answer: A (LEAVE A REPLY)

The charging method for IS resources is the way that the IS function allocates its costs to the users or business units that consume its services. The charging method can affect the behavior and incentives of the users and the IS function, as well as the efficiency and effectiveness of the IS resources. Therefore, choosing an appropriate charging method is an important decision for the IS function and its stakeholders.

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

The other possible charging methods are:

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

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

Allocations based on the ability to absorb charges: This means that the IS function charges different amounts to different users or business units based on their ability to pay or their profitability. For example, if a user or business unit is more profitable or has a higher budget than another user or business unit, they will pay more for the same amount of IS resources. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business

unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates an unfair and arbitrary distribution of costs among the users or business units, as some paymore than others for no valid reason. References: 1: Charging Methods for IT Services - IT Process Wiki 2: IT Chargeback Methods - CIO Wiki 3: IT Chargeback - Wikipedia

NEW QUESTION: 453
對於以新的健康記錄系統取代舊系統而言，資訊系統審計師應考慮下列哪項風險最為重大？
A. 員工沒有參與採購過程，導致使用者對新系統口生抗拒
B. 資料轉換不正確，導致病患記錄不準確
C. 部署專案嚴重超支，超出預算預期
D. 新系統有容量問題，導致使用者回應時間緩慢
Answer: B (LEAVE A REPLY)
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition] , page 281.

NEW QUESTION: 454
下列哪一項最能幫助資訊系統審計員合併和比較來自各種應用程式和設備的存取控制清單？
A. 綜合測試設施(ITF)
B. 快照
C. 數據分析
D. 審計鉤子
Answer: C (LEAVE A REPLY)
Data analytics is the process of analyzing large and complex data sets to discover patterns, trends, and insights that can support decision making and problem solving. Data analytics can enable an IS auditor to combine and compare access control lists from various applications and devices by using techniques such as data extraction, transformation, loading, cleansing, integration, aggregation, visualization, and reporting. Data analytics can help an IS auditor to identify and assess the risks and controls related to access management, such as unauthorized or excessive access, segregation of duties

violations, access policy compliance, access activity monitoring, and access review and remediation.
The other options are not as effective or relevant as data analytics for combining and comparing access control lists from various applications and devices. Integrated test facility (ITF) is a technique for testing the validity and accuracy of application processing by inserting fictitious transactions into the system and verifying the results. ITF does not directly involve the analysis of access control lists. Snapshots are records of selected information at a specific point in time that can be used to monitor system activity or performance.
Snapshots can provide some information about access control lists, but they are not sufficient to combine and compare them across different sources. Audit hooks are software routines embedded in an application that can trigger an alert or a report when certain conditions are met. Audit hooks can help to detect anomalies or exceptions in access control lists, but they do not provide a comprehensive or integrated view of them.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 882 Data Analytics for Auditing Access Control3

NEW QUESTION: 455
下列哪項測試能最好地確保醫療機構妥善處理病患資料？
A. 遵守近期審計結果所製定的行動計劃
B. 遵守當地法律法規
C. 符合業界標準與最佳實踐
D. 遵守組織的政策和程序
Answer: B (LEAVE A REPLY)
The best test to provide assurance that a health care organization is handling patient data appropriately is compliance with local laws and regulations, as these are the primary sources of authority and obligation for data protection and privacy. Compliance with action plans, industry standards, or organizational policies and procedures are also important, but they may not cover all the legal requirements or reflect the currentbest practices for handling patient data. References: CISA Review Manual (Digital Version), Chapter 2, Section
2.3

NEW QUESTION: 456
資訊系統審計師計劃對某組織的應付帳款流程進行審計。下列哪一項控制措施在審計中最為重要？
A. 採購訂單簽發與付款職責分開。
B. 接收發票和設定授權限額之間的職責分離
C. 管理階層對授權層級進行審□與批准

D. 管理階層對採購訂單的審核與核准

Answer: A (LEAVE A REPLY)

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

References:

Accounts payable controls

Accounts Payable Internal Controls: A Simple Checklist

NEW QUESTION: 457

在協商熱點站點合約時，下列哪一項是首要考慮因素？

A. 在發生多起災害聲明的情況下，該站點的可用性

B. 在發生多起災害聲明時與現場工作人員協調

C. 與其他組織的互惠協議

D. 復原計畫的完整測試

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 458

在後續審計過程中，資訊系統審計員發現一些關鍵建議是資訊系統審計員的最佳行動方案？

A. 要求受審計方全面落實各項建議。

B. 據此調整年度風險評估。
C. 評估高階主管對風險的接受程度。
D. 根據管理階層對風險的接受程度更新審計程序。
Answer: C (LEAVE A REPLY)
The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management's acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization's risk exposure. The IS auditor should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 459
下列何者最能顯示口部稽核品質保證和改進計畫有效？
A. 高階管理層對改善計畫的監督
B. 改進的口部稽核章程
C. 重點關注高風險審計業務的範圍
D. 辨識持續改善的機會
Answer: D (LEAVE A REPLY)
The goal of a quality assurance and improvement program (QAIP) is to drive continuous enhancement in audit practices and deliver increasing value to stakeholders. Identification and implementation of opportunities for improvement demonstrate that the program is working effectively. Oversight (A) and charter updates (B) are important governance aspects, while focusing on high-risk audits (C) is a prioritization strategy. However, the hallmark of a successful QAIP is the ability to continuously identify and address gaps, streamline practices, and enhance audit value. ISACA emphasizes agility, adaptability, and ongoing improvement as key success indicators for internal audit functions.
References (ISACA): ISACA Audit Standards; ISACA Journal - Agile and Continuous Improvement in Audit.

NEW QUESTION: 460
資訊系統審計員發現資料庫中存在一個允許管理員直接修改任何表格的選項。該選項對於修復軟體漏洞至關重要，但很少使用。表的變更會被自動記錄。資訊系統審計員的首要任務應該是：
A. 建議立即刪除直接修改資料庫的選項。
B. 建議系統要求兩人參與修改資料庫。
C. 確定表格更改日誌是否已備份。

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

NEW QUESTION: 461
在組織制定資訊安全政策和程序時，下列哪個因素最為重要？
A. 與保全人員協商
B. 包含使命與目標
C. 符合相關法規
D. 與資訊安全框架保持一致
Answer: D (LEAVE A REPLY)
Information security policies and procedures are the foundation of an organization's information security program. They define the roles, responsibilities, rules, and standards for protecting information assets from unauthorized access, use, disclosure, modification, or destruction. The most important factor when developing information security policies and procedures is to align them with an information security framework that provides a comprehensive and consistent approach to managing information security risks. An information security framework can also help ensure compliance with relevant regulations, inclusion of mission and objectives, and consultation with security staff. However, these factors are secondary to alignment with an information security framework. References: CISA Certification | Certified Information Systems Auditor | ISACA, CISA Review Manual (Digital Version)

NEW QUESTION: 462
在對一家跨國銀行的資口處置流程進行審計時，資訊系統審計師發現了一些問題。下列哪一項應該是審計師最該關注的問題？
A. 備份媒體在處置前未經審口。
B. 以消磁取代物理粉碎。
C. 備份媒體在保留期結束前被銷毀
D. 硬體不會被經認證的供應商銷毀。
Answer: C (LEAVE A REPLY)

During an audit of a multinational bank's disposal process, an IS auditor should be most concerned about backup media being disposed before the end of the retention period. This is because backup media contain sensitive and critical data that may be required for business continuity, legal compliance, or forensic purposes.
Disposing backup media prematurely may result in data loss, unavailability, or corruption, which may have severe consequences for the bank's reputation, operations, and security.
Backup media not being reviewed before disposal, degaussing being used instead of physical shredding, and hardware not being destroyed by a certified vendor are also findings that may pose some risks to the bank's disposal process, but they are not as critical as backup media being disposed before the end of the retention period.
References: ISACA CISA Review Manual 27th Edition, page 302.

NEW QUESTION: 463
下列哪一項措施最能幫助組織應對最近實施的自帶設備 (BYOD) 策略所帶來的安全風險？
A. 行動裝置追蹤程序
B. 行動裝置升級計劃
C. 行動裝置測試程序
D. 行動裝置意識計劃
Answer: D (LEAVE A REPLY)
A mobile device awareness program would best enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy. A mobile device awareness program is a set of activities that aim to educate and inform the employees about the benefits, challenges, and best practices of using their personal mobile devices for work purposes. A mobile device awareness program can help the organization to:
Communicate the organization's policies and expectations regarding BYOD, such as which devices are allowed, what data can be accessed or stored, and what security measures are required.
Raise the employees' awareness of the potential threats and vulnerabilities that affect their mobile devices, such as malware, phishing, data leakage, or device loss.
Provide the employees with guidance and tips on how to protect their mobile devices and the organization's data, such as using strong passwords, encryption, antivirus software, remote wipe, or VPN.
Encourage the employees to report any incidents or issues related to their mobile devices, such as suspicious messages, unauthorized access, or device damage.
A mobile device awareness program can help the organization to reduce the security risks associated with BYOD by enhancing the employees' knowledge, skills, and behavior in using their mobile devices securely and responsibly. Amobile device awareness program can also help the organization to comply with relevant regulations and standards that governdata privacy and security in the cloud1.

The other options are not as effective as a mobile device awareness program in enabling an organization to address the security risks associated with BYOD. Option A, mobile device tracking program, is a tool that allows the organization to monitor and locate the employees' mobile devices in case of loss or theft. However, this tool may not prevent or detect other types of security risks, such as malware infection or data breach.
Option B, mobile device upgrade program, is a process that ensures that the employees' mobile devices are running the latest versions of operating systems and applications. However, this process may not address other aspects of security, such as user behavior or data protection. Option C, mobile device testing program, is a method that verifies the functionality and compatibility of the employees' mobile devices with the organization's systems and networks. However, this method may not cover all the scenarios or factors that may affect the security of the mobile devices or the organization's data2.
References:
Mobile Device Security Awareness Topics3
Security Awareness Top Ten Topics - #8 Mobile Devices

NEW QUESTION: 464
一個安全伺服器機房配備了門禁卡讀取系統，每次員工使用門禁卡進出時，系統都會記錄姓名、日期和時間資訊。資訊系統審計員在審口系統日誌時發現，部分員工有進出記錄 下列哪一項是最有效的補償控制措施？
A. 在門口安裝監視器
B. 改用生物辨識門禁系統
C. 在入口和出口安裝受監控的防盜門
D. 要求在入口和出口處進行雙重認證
Answer: C (LEAVE A REPLY)
A monitored mantrap at entrance and exit points would be the most effective compensating control in this scenario. A mantrap is a physical security access control system comprising a small space having two sets of interlockingdoors such that the first set of doors must close before the second set opens. By implementing a monitored mantrap, unauthorized access can be prevented and it can ensure that all individuals are logged when they enter and exit the server room12.
References: ISACA's Information Systems Auditor Study Materials3

NEW QUESTION: 465
下列哪一項是衡量 IT 策略與業務策略一致性的最佳指標？
A. 利害關係人對計劃中的IT專案範圍的滿意度
B. 包含IT相關風險的企業風險評估百分比
C. 員工對其IT相關角色的滿意度百分比
D. 業務流程能力成熟度評估的頻率
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 466
下列哪一項圖書館控制軟體包的功能可以防止未經授權的原始碼更新？
A. 生命週期各階段所需的審批
B. 原始碼和目標碼的日期和時間戳
C. 原始碼庫的存取控制
D. 原始碼版本間的比較
Answer: C (LEAVE A REPLY)
Access controls for source libraries are the features of a library control software package that would protect against unauthorized updating of source code. Access controls are the mechanisms that regulate who can access, modify, or delete the source code stored in the source libraries. Source libraries are the repositories that contain the source code files and their versions. By implementing access controls for source libraries, the library controlsoftware package can prevent unauthorized or malicious users from tampering with the source code and compromising its integrity, security, or functionality1.
The other options are not as effective as access controls for source libraries in protecting against unauthorized updating of source code. Option A, required approvals at each life cycle step, is a good practice but may not be sufficient to prevent unauthorized updates if the approval process is bypassed or compromised. Option B, date and time stamping of source and object code, is a useful feature but may not prevent unauthorized updates if the date and time stamps are altered or ignored. Option D, release-to-release comparison of source code, is a helpful feature but may not prevent unauthorized updates if the comparison results are not reviewed or acted upon.
References:
ISACA, CISA Review Manual, 27th Edition, 2019
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription How to protect your source code from attackers2 How to Stop Unauthorized Use of Open Source Code

NEW QUESTION: 467
當資訊系統稽核員需要確認組織是否在資料庫層級對敏感資訊進行加密時，下列何者能口提供最佳保證？
A. 正在檢口主機伺服器的磁碟機設定
B. 檢口網路流量中是否有明文傳輸
C. 驗證關鍵字段樣本
D. 檢視組織的加密策略
Answer: (SHOW ANSWER)
The best assurance is obtained by verifying a sample of critical fields. If the question is specifically about encryption at the database level, the auditor should test the actual data elements in the database that are expected to be encrypted. ISACA privacy and data-protection guidance discusses encryption of sensitive data fields as a protection mechanism, which supports validating field-level protection directly.
Option C is correct because it provides direct evidence that sensitive database fields are actually encrypted.
This is stronger than reviewing policies or peripheral settings because it tests the implemented control itself.
Option A is incorrect because drive settings usually relate to disk or full-volume encryption on the host server, not necessarily to database-level encryption of specific sensitive fields.
Option B is incorrect because checking network traffic for clear text transmissions only helps verify encryption in transit, not whether the data is encrypted within the database.
Option D is incorrect because a policy only states intent or requirement. It does not prove the database is actually encrypting sensitive fields.
Therefore, C is the best answer because direct verification of sensitive fields provides the strongest assurance that encryption is implemented at the database level.
References (Official ISACA):
* ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - discusses encryption of sensitive client data fields.
* ISACA Journal, Privacy-Preserving Analytics and Secure Multiparty Computation - discusses encryption of sensitive data fields throughout the data life cycle.
* ISACA, Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage - distinguishes encryption at rest and in transit, supporting why network checks alone are insufficient for database-level assurance.

NEW QUESTION: 468
理想情況下，壓力測試應在以下情況下進行：
A. 具有生口工作負載的測試環境。
B. 具有生口工作負載的生口環境。
C. 包含測試資料的生口環境。
D. 包含測試資料的測試環境。
Answer: (SHOW ANSWER)
Stress testing is a type of performance testing that evaluates the behavior and reliability of a system under extreme conditions, such as high workload, limited resources, or concurrent users. Stress testing should ideally be carried out under a test environment with production workloads, as this would simulate the most realistic and demanding scenario for the system without affecting the actual production environment. A production environment with production workloads is not suitable for stress testing, as it could cause disruption or damage to the system and its users. A production environment with test data is not suitable for stress testing, as it could compromise the integrity and security of the production data. A test environment with test data is not suitable for stress testing, as it could underestimate the potential issues and risks that could occur in the production environment. References:
CISA Review Manual, 27th Edition, pages 471-4721
CISA Review Questions, Answers and Explanations Database,Question ID: 261

NEW QUESTION: 469
管理階層要求對新實施的採購系統進行實施後評估，以確定其滿足業務需求的程度。下列哪一項最可能被評估？
A. 即時處理結果
B. 驗收測試結果
C. 採購指南與政策
D. 實施方法
Answer: D (LEAVE A REPLY)

NEW QUESTION: 470
組織關鍵資料的備份程序屬於哪種類型的控制措施？
A. 指令
B. 修正
C. 偵探
D. 補償
Answer: B (LEAVE A REPLY)
Backup procedures for an organization's critical data are considered to be corrective controls, as they are designed to restore normal operations after a disruption or failure.

Corrective controls aim to minimize the impact of an incident and prevent recurrence. Directive, detective and compensating controls are not related to backup procedures. Directive controls are intended to guide or instruct users to follow policies and procedures. Detective controls are intended to identify and report incidents or violations. Compensating controls are intended to mitigate the risk of a missing or ineffective primary control. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.11

NEW QUESTION: 471
下列哪一項是確保電子郵件在傳輸過程中保密性的最佳方法？
A. 企業網路流量加密
B. 複雜使用者密碼
C. 端對端加密
D. 數位簽名
Answer: C (LEAVE A REPLY)
End-to-end encryption ensures that email content is encrypted during transmission and can only be decrypted by the intended recipient. This approach provides robust protection against interception and unauthorized access.
Encryption of Corporate Network Traffic (Option A):This does not address email confidentiality once the email leaves the corporate network.
Complex User Passwords (Option B):Enhances account security but does not ensure email confidentiality in transit.
Digital Signatures (Option D):Ensures authenticity and integrity but does not encrypt the email content.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 472
下列哪一項是保護資料中心實體資訊資口最重要的前提條件？
A. 資訊資口訂購人員與接收人員之間的職責分離
B. 已部署資訊資口的完整準確列表
C. 現場備用發電機的可用性和測試
D. IT 人員對資料保護要求的了解程度
Answer: (SHOW ANSWER)
The most important prerequisite for the protection of physical information assets in a data center is a complete and accurate list of information assets that have been deployed. Information assets are any data, devices, systems, or software that have value for the organization and need to be protected from unauthorized access, use, disclosure, modification, or destruction4. A data center is a facility that houses various information assets such as servers, storage devices, network equipment, etc., that support the organization's IT operations and services5. A complete and accurate list of information

assets that have been deployed in a data center can help to identify and classify the assets based on their importance, sensitivity, or criticality for the organization.
This can help to determine the appropriate level of protection and security measures that need to be applied to each asset. A complete and accurate list of information assets can also help to track and monitor the location, status, ownership, usage, configuration, maintenance, etc., of each asset. This can help to prevent or detect any unauthorized or inappropriate changes or movements of assets that may compromise their security or integrity. Segregation of duties between staff ordering and staff receiving information assets, availability and testing of onsite backup generators, and knowledge of the IT staff regarding data protection requirements are also important prerequisites for the protection of physical information assets in a data center, but not as important as a complete and accurate list of information assets that have been deployed. These factors are more related to the implementation and maintenance of security controls and procedures that depend on having a complete and accurate list of information assets as a starting point.
References: ISACA CISA Review Manual 27th Edition, page 308

NEW QUESTION: 473
在預算受限的組織中，解決職責分離問題的最佳方法是什麼？
A. 定期輪調工作職責。
B. 進行獨立審計。
C. 僱用臨時員工。
D. 實施補償控制。
Answer: D (LEAVE A REPLY)
The best way to address segregation of duties issues in an organization with budget constraints is to implement compensating controls, which are alternative controls that reduce or eliminate the risk of errors or fraud due to inadequate segregation of duties. Compensating controls may include independent reviews, reconciliations, approvals, or supervisions. Rotating job duties periodically may reduce the risk of collusion or abuse of privileges, but it may also affect operational efficiency and continuity. Performing an independent audit may detect segregation of duties issues, but it does not prevent them. Hiring temporary staff may increase operational costs and introduce new risks.
References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 474
下列哪一項可以提供最好的證據來證明雲端提供者的變更管理流程是有效的？
A. 與供應商定期召開變更管理會議的會議記錄
B. 供應商執行長和資訊長的書面保證
C. 供應商提供的第三方審核結果
D. 供應商提供的變更管理政策的副本
Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 475
下列哪一項是防止透過即時通訊(IM)應用程式向外部人員傳輸文件的最佳控制措施？
A. 檔案層級加密
B. 檔案傳輸協定(FTP)
C. 即時通訊策略
D. 應用層防火牆
Answer: D (LEAVE A REPLY)
Application level firewalls are the best control to prevent the transfer of files to external parties through instant messaging (IM) applications, because they can inspect and filter network traffic based on application- specific protocols and commands, such as IM file transfer commands. Application level firewalls can block or allow IM file transfers based on predefined rules or policies. File level encryption, file transfer protocol (FTP), and instant messaging policy are not effective controls to prevent IM file transfers, because they donot restrict or monitor IM network traffic. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.1

NEW QUESTION: 476
在IT專案的哪個階段進行效益實現分析最為適合？
A. 最終實施階段
B. 設計評審階段

C. 實施後審口階段
D. 使用者驗收測試(UAT)階段
Answer: C (LEAVE A REPLY)

NEW QUESTION: 477
一項新法規已頒布，該法規強制要求採取特定的資訊安全措施來保護客口資料。在根據該法規進行審計時，下列哪一項對資訊系統審計員最有用？
A. 合規性差距分析
B. 客口資料保護的角色與職責
C. 客口資料流程圖
D. 對新規適應性的基準研究
Answer: A (LEAVE A REPLY)
A compliance gap analysis is a detailed review of an organization's current state of compliance against a specific regulation or standard. It helps identify the areas and controls that are not meeting the requirements, assess their risk levels, and determine the corrective actions that can be taken to achieve compliance12. A compliance gap analysis is the most useful tool for an IS auditor to review when auditing against a new regulation, as it provides a clear and comprehensive picture of the compliance status, gaps, and remediation plan of the organization.
References
1: Information Security Architecture: Gap Assessment and Prioritization - ISACA
2: How to perform Compliance Gap Analysis? - Sprinto

NEW QUESTION: 478
下列哪一項最可能損害資訊系統審計師在實施應用系統後審口時的獨立性？
A. 資訊系統稽核員就應用系統最佳實務提供了諮詢建議。
B. 資訊系統審計員作為應用系統專案團隊的成員參與其中，但沒有承擔營運責任。
C. 資訊系統審計員專門設計了一個嵌入式審計模組，用於審計應用系統。
D. 資訊系統稽核員在應用系統開發過程中實施了一項特定控制措施。
Answer: D (LEAVE A REPLY)
The IS auditor's independence would be most likely impaired if they implemented a specific control during the development of an application system. This is because the IS auditor would be auditing their own work, which creates a self-review threat that could compromise their objectivity and impartiality. The IS auditor should avoid participating in any operational or management activities that could affect their ability to perform an unbiased audit. The other options do not pose a significant threat to the IS auditor's independence, as long as they follow the ethical standards and guidelines of the profession.

NEW QUESTION: 479

在評估由應用程式和IT系統支援的組織業務流程時，下列哪一項對資訊系統審計員最有幫助？

A. 設定管理資料庫(CMDB)

B. 企業架構(EA)

C. IT組合管理

D. IT 服務管理

Answer: B (LEAVE A REPLY)

The most helpful thing for an IS auditor to review when evaluating an organization's business processes that are supported by applications and IT systems is the enterprise architecture (EA). EA is the practice of designing a business with a holistic view, considering all of its parts and how they interact. EA defines the overall goals, the strategies that support those goals, and the tactics that are needed to execute those strategies.

EA also outlines the ways various components of IT projects interact with one another and with the business processes. By reviewing the EA, an IS auditor can gain a comprehensive understanding of how the organization aligns its IT efforts with its overall mission, business strategy, and priorities. An IS auditor can also assess the effectiveness, efficiency, agility, and continuity of complex business operations.

The other options are not as helpful as option B. A configuration management database (CMDB) is a database that stores and manages information about the components that make up an IT system. A CMDB tracks individual configuration items (CIs), such as hardware, software, or data assets, and their attributes, dependencies, and changes over time. A CMDB can help an IS auditor to monitor the performance, availability, and configuration of IT assets, but it does not provide a holistic view of how they support the business processes. IT portfolio management is the practice of managing IT investments, projects, and activities as a portfolio. IT portfolio management aims to optimize the value, risk, and cost of IT initiatives and align them with the business objectives. IT portfolio management can help an IS auditor to evaluate the return on IT investments and the alignment of IT projects with the business strategy, but it does not provide a detailed view of how they support the business processes. IT service management (ITSM) is the practice of planning, implementing, managing, and optimizing IT services to meet the needs of end users and customers.

ITSM focuses on delivering IT as a service using standardized processes and best practices. ITSM can help an IS auditor to review the quality, efficiency, and effectiveness of IT service delivery and support, but it does not provide a comprehensive view of how they support the business processes. References: What is enterprise architecture (EA)? - RingCentral, What is a configuration management database (CMDB)? - Red Hat, IT Portfolio Management Strategies | Smartsheet, What is IT service management (ITSM)? | IBM

NEW QUESTION: 480

下列哪一項是降低終端用口計算 (EUC) 中因意外修改複雜計算而帶來的風險的最佳方法？
A. 請獨立第三方審核來源計算結果。
B. 從安全庫執行 EUC 程式的副本
C. 實現複雜的密碼控制
D. 以手動計算驗證 EUC 結果。
Answer: B (LEAVE A REPLY)
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end- user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that thecopies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC. References: End-User Computing (EUC) Risks: A Comprehensive Guide, End User Computing (EUC) Risk Management

NEW QUESTION: 481
一家新創公司想要開發一個資料遺失防護(DLP)程式。第一步應該是實施：
A. 資料加密
B. 存取控制
C. 安全意識培訓
D. 資料分類
Answer: D (LEAVE A REPLY)

NEW QUESTION: 482
某個組織決定重新設計業務流程，以提高整體IT 服務交付的效能。專案團隊提出的下列哪一項建議應該是資訊系統審計員最關心的問題？
A. 停用操作日誌記錄以提高處理速度並節省儲存空間。

B. 根據同儕組織的見解採用服務交付模式。
C. 將業務決策委託給首席風險長 (CRO)。
D. 消除某些報告和關鍵績效指標 (KPI)
Answer: A (LEAVE A REPLY)
Disabling operational logging compromises critical functions such as security monitoring, troubleshooting, and compliance reporting. Logs are essential for tracking system activities, identifying anomalies, and conducting forensic investigations in case of incidents. Enhancing processing speed and saving storage should not come at the cost of reducing logging, as this increases security risks and weakens the organization's ability to detect and respond to threats.
* Adopting a Peer-Inspired Service Delivery Model (Option B):This might pose risks if not customized for the organization's context, but it is not as critical as the loss of operational logging.
* Delegating Business Decisions to the CRO (Option C):While unconventional, this does not inherently introduce risks to IT service delivery unless operational control issues arise.
* Eliminating Reports and KPIs (Option D):This could hinder performance tracking but does not compromise operational security as severely as disabling logging.
Operational logging is foundational to maintaining security, reliability, and accountability in IT environments.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 483
在組織中，下列哪一個角色所展現的支持對資訊安全治理的影響最大？
A. 首席資訊安全長(CISO)
B. 資訊安全指導委員會
C. 董事會
D. 資訊長(CIO)
Answer: C (LEAVE A REPLY)
Information security governance is the subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program. Information security governance is essential for ensuring that an organization's information assets are protected from internal and external threats, and that the organization complies with relevant laws and standards.
Demonstrated support from which of the following roles in an organization has the most influence over information security governance? The answer is C, the board of directors. The board of directors is the highest governing body of an organization, responsible for overseeing its strategic direction, performance, and accountability. The board of directors sets the tone at the top for information security governance by:

Establishing a clear vision, mission, and values for information security Approving and reviewing information security policies and standards Allocating sufficient resources and budget for information security Appointing and empowering a chief information security officer (CISO) or equivalent role Holding management accountable for information security performance and compliance Communicating and promoting information security awareness and culture The board of directors has the most influence over information security governance because it has the ultimate authority and responsibility for ensuring that information security is aligned with the organization's business objectives, risks, and stakeholder expectations.
References:
10: What is Information Security Governance? - RiskOptics - Reciprocity
11: Information Security Governance and Risk Management | Moss Adams
12: ISO/IEC 27014:2020 - Information security, cybersecurity and privacy ...

NEW QUESTION: 484
在確定設計階段的專案是否能口實現組織目標時，最好將商業案例與什麼進行比較？
A. 實施計劃
B. 專案預算撥款
C. 需求分析
D. 專案計劃
Answer: C (LEAVE A REPLY)
Requirements analysis should be the best thing to compare against the business case when determining whether a project in the design phase will meet organizational objectives, because it defines the functional and non-functional specifications of the project deliverables that should satisfy the business needs and expectations. Requirements analysis can help evaluate whether the project design is aligned with the business case and whether it can achieve the desired outcomes and benefits. Implementation plan, project budget provisions, and project plan are also important aspects of a project in the design phase, but they are not as relevant asrequirements analysisfor comparing against the business case. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.1

NEW QUESTION: 485
某組織已將其所有基礎設施遷移到雲端。下列何者是資訊系統審計員在組織發生災難時能否繼續運作最關心的問題？
A. 沒有證據表明在遷移後進行了災難復原計畫 (DRP) 測試。
B. 只有業務關鍵型伺服器才在雲端服務供應商處配置了冗餘服務。
C. 發生災難時，先前的基礎設施未能保留以支援業務運作。
D. 遷移後，災難復原計畫(DRP)中未更新逐步復原流程。
Answer: A (LEAVE A REPLY)

After migrating infrastructure to the cloud, it ' s imperative to test the disaster recovery plan (DRP) to ensure its effectiveness in the new environment. Without evidence of DRP testing post-migration, the organization cannot be certain that it can recover and continue operations during a disaster. While updating the DRP and configuring redundancy are essential steps, their effectiveness can only be validated through rigorous testing. Retaining previous infrastructure is less relevant if the cloud environment is properly configured and tested for disaster recovery.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 486
對於疑似資料外洩事件，下列哪一項應該是事件回應流程的第一步？
A. 通知可能受影響的客口有關安全漏洞的資訊。
B. 通知業務管理階層安全漏洞。
C. 調口已發出警報的違規行為的有效性。
D. 聘請第三方對已發出警報的違規行為進行獨立評估。
Answer: (SHOW ANSWER)
The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the incident response process, but they are not the first step. References:
CISA Review Manual, 27th Edition, page 4251
CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

NEW QUESTION: 487
對某組織的IT資口組合進行審口後發現，其中一些應用程式未使用。防止這種情況再次發生的最佳方法是實施這些應用程式。
A. 正式的徵求建議書(RFP)流程
B. 商業案例開發流程
C. 資訊資口取得政策
D. 資口生命週期管理。
Answer: D (LEAVE A REPLY)
Asset life cycle management is a technique of asset management where facility managers maximize the usable life of assets throughplanning, purchasing, using, maintaining, and

disposing of assets1. The mainaim of assetlife cycle management is to reduce costs and increase productivity by optimizing the performance, reliability, and lifespan of assets2. Asset life cycle management can help prevent the situation of having unused applications by ensuring that the applications are aligned with the business needs, objectives, and strategies, and that they are regularly reviewed, updated, or retired as necessary3.
The other options are not as effective as asset life cycle management for preventing unused applications. A formal request for proposal (RFP) process is a method of soliciting bids from potential vendors or suppliers for a project or service. A RFP process can help select the best application for a specific requirement, but it does not ensure that the application will be used or maintained throughout its lifecycle. Business case development procedures are a set of steps that involve defining the problem, analyzing the alternatives, and proposing a solution for a project or initiative. Business case development procedures can help justify the need and value of an application, but they do not guarantee that the application will be utilized or supported after its implementation. An information asset acquisition policy is a document that outlines the rules and standards for acquiring information assets such as applications. An information asset acquisition policy can help ensure that the applications are acquired in a consistent and compliant manner, but it does not address how the applications will be managed or disposed of after their acquisition.

NEW QUESTION: 488
下列哪一項是降低員工不當行為風險最有效的控制措施？
A. 使用者活動監控
B. 雙重認證
C. 網路分割
D. 存取重新認證
Answer: A (LEAVE A REPLY)
The answer A is correct because user activity monitoring is the most effective control to mitigate against the risk of inappropriate activity by employees. User activity monitoring (UAM) is the process of tracking and recording the actions and behaviors of users on devices, networks, or applications that belong to an organization. UAM can help to prevent, detect, and respond to insider threats, such as data theft, fraud, sabotage, or misuse of resources. UAM can also help to enforce policies, ensure compliance, and improve productivity and performance.
Some of the benefits of UAM are:
Prevention: UAM can deter employees from engaging in inappropriate activity by making them aware that their actions are monitored and recorded. UAM can also prevent unauthorized access or use of sensitive data or resources by implementing access controls, encryption, or alerts.
Detection: UAM can detect any anomalies, deviations, or violations in user activity by analyzing the data collected from various sources, such as logs, keystrokes, screenshots,

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

NEW QUESTION: 489
在組織的 DLP 解決方案中實施資料遺失防護 (DLP) 策略時，下列何者是其主要功能？
A. 定義網路效能的規則和基線
B. 加密靜態和傳輸中的敏感數據
C. 偵測並阻止傳入的網路流量
D. 定義監控和保護敏感資料的規則

Answer: D (LEAVE A REPLY)

NEW QUESTION: 490
在後續審計中，資訊系統審計師發現一些關鍵建議尚未落實，因為管理階層決定承擔風險下列哪一項是資訊系統審計師的最佳因應措施？
A. 據此調整年度風險評估。
B. 根據管理階層對風險的接受程度更新審計程序。
C. 評估高階主管對風險的接受程度。
D. 要求受審計方全面落實各項建議。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 491
在應用程式開發驗收測試中，下列哪一項最為重要？
A. 程式設計團隊參與測試過程。
B. 所有資料檔案在轉換前都會進行有效資訊測試。
C. 使用者管理階層在測試開始前批准測試設計。
D. 品質保證(QA)團隊負責測試過程。
Answer: C (LEAVE A REPLY)
The most important aspect of an application development acceptance test is that user management approves the test design before the test is started, as this ensures that the test objectives, criteria, and procedures are aligned with the user requirements and expectations. The programming team's involvement in the testing process, the testing of data files for valid information before conversion, and the quality assurance (QA) team' s charge of the testing process are also important, but they are not as critical as user management's approval of the test design. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.2

NEW QUESTION: 492
下列哪一項是確保業務連續性計劃 (BCP) 在發生重大災難時有效運作的最佳方法？
A. 為每個業務職能製定詳細計畫。
B. 讓各級員工定期參與文件審核練習。
C. 定期更新業務影響評估。
D. 讓高階主管負責其計畫部分。
Answer: (SHOW ANSWER)
The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and

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

NEW QUESTION: 493
由於網路防火牆固有的安全漏洞，下列哪一種攻擊技術會成功？
A. 網路釣魚
B. 利用加密密碼的字典攻擊
C. 攔截資料包並口看密碼
D. 傳送過量資料包
Answer: D (LEAVE A REPLY)
Flooding the site with an excessive number of packets is an attack technique that will succeed because of an inherent security weakness in an Internet firewall. This type of attack is also known as a denial-of-service (DoS) attack or a distributed denial-of-service (DDoS) attack if it involves multiple sources. The aim of this attack is to overwhelm the network bandwidth or the processing capacity of the firewall or the target system, rendering it unable to respond to legitimate requests or perform its normal functions. An Internet firewall is a device or software that monitors andcontrols incoming and outgoing network traffic based on predefined rules. A firewall can block or allow traffic based on various criteria, such as source address, destination address, port number, protocol type, application type, etc. However, a firewall cannot prevent traffic from reaching its interface or distinguish between legitimate and malicious traffic based on its content or behavior. Therefore, a firewall is vulnerable to flooding attacks that exploit its limited resources.
Phishing is an attack technique that involves sending fraudulent emails or messages that appear to come from legitimate sources, such as banks, government agencies, online services, etc., in order to trick recipients into revealing their personal or financial information, such as passwords, credit card numbers, bank account details, etc., or into clicking on malicious links or attachments that can infect their systems with malware or ransomware.

Phishing does not exploit an inherent security weakness in an Internet firewall, but rather exploits human psychology and social engineering techniques. A firewall cannot prevent phishing emails or messages from reaching their intended targets, unless they contain some identifiable features that can be filtered out by the firewall rules. However, a firewall cannot detect or prevent users from responding to phishing emails or messages or from opening malicious links or attachments. Using a dictionary attack of encrypted passwords is an attack technique that involves trying to guess or crack passwords by using a list of common or likely passwords or by using a brute-force method that tries all possible combinations of characters. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits weak or poorly chosen passwords or weak encryption algorithms. A firewall cannot prevent a dictionary attack of encrypted passwords, unless it has some mechanisms to detect and block repeated or suspicious login attempts or to enforce strong password policies. However, a firewall cannot protect passwords from being stolen or intercepted by other means, such as phishing, malware, keylogging, etc. Intercepting packets and viewing passwords is an attack technique that involves capturing and analyzing network traffic that contains sensitive information, such as passwords, credit card numbers, bank account details, etc., in order to use them for malicious purposes. This type of attack does not exploit an inherent security weakness in an Internet firewall, but rather exploits insecure or unencrypted network communication protocols or channels. A firewall cannot prevent packets from being intercepted and viewed by unauthorized parties, unless it has some mechanisms to encrypt or obfuscate the network traffic or to authenticate the source and destination of the traffic. However, a firewall cannot protect packets from being modified or tampered with by other means, such as man-in-the- middle attacks, replay attacks, etc. References: ISACA CISA Review Manual 27th Edition, page 300

NEW QUESTION: 494
當被審計單位表示針對高風險問題的糾正措施計畫所需時間比預期更長時，下列哪一項是資訊系統審計師的最佳行動方案？
A. 接受較長的目標日期，並在審計系統中記錄
B. 確定是否已實施臨時補償控制。
C. 要求在約定的時間口完成補救措施。
D. 將逾期未決的調口結果上報審計委員會。
Answer: (SHOW ANSWER)

NEW QUESTION: 495
IT平衡計分卡的主要用途是：
A. 評估 IT 專案組合
B. 衡量 IT 策略績效
C. 分配 IT 預算與資源
D. 監控與IT相關的流程中的風險

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

NEW QUESTION: 496
在審口以人工智慧(AI)系統取代多個手動資料輸入系統的專案時，資訊系統稽核員最應該關注的是人工智慧將對以下方面口生的影響：
A. 員工留任
B. 企業架構(EA)
C. 未來任務更新
D. 任務能力輸出
Answer: B (LEAVE A REPLY)
The auditor should be most concerned with the impact AI will have on enterprise architecture (EA) when reviewing a project to replace multiple manual data entry systems with an AI system. EA is a comprehensive framework that defines the structure, components, relationships, and principles of an organization's IT environment. EA can help to align the IT strategy with the business strategy and ensure the coherence, consistency, and integration of the IT systems and services. Replacing manual data entry systems with an AI system may have significant implications for the EA, such aschanging the business processes, data flows, security requirements, performance standards, or governance models. The auditor should assess whether the project has considered the impact of AI on EA and whether the EA has been updated accordingly. References:
CISA Review Manual (Digital Version), Chapter 1, Section 1.41
CISA Online Review Course, Domain 5, Module 1, Lesson 22

NEW QUESTION: 497
現行法規要求組織在發現重大安全事件後 24 小時□向監管機構報告。下列哪一項是資訊系統審計師為促進組織遵守法規而提出的最佳建議？
A. 建立關鍵績效指標(KPI)，以便及時發現安全事件。
B. 聘請外部安全事件回應專家處理事件。
C. 增強入侵偵測系統(IDS)的警報功能。
D. 將此要求納入事件管理回應計畫。
Answer: D (LEAVE A REPLY)
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

NEW QUESTION: 498
下列哪項審計程序最能有效評估電子商務應用程式系統編輯流程的有效性？
A. 程序文檔審□
B. 使用測試交易
C. 對知識淵博的使用者進行訪談

D. 原始碼審口

Answer: B (LEAVE A REPLY)

The most conclusive audit procedure for evaluating the effectiveness of an e-commerce application system's edit routine is to use test transactions. A test transaction is a simulated input that is processed by the system to verify its output and performance1. By using test transactions, an auditor can directly observe how the edit routine checks the validity, accuracy, and completeness of data entered by users, and how it handles incorrect or invalid data. A test transaction can also help measure the efficiency, reliability, and security of the edit routine, as well as identify any errors or weaknesses in the system. The other options are not as conclusive as using test transactions, as they rely on indirect or secondary sources of information. Reviewing program documentation is an audit procedure that involves examining the written description of the system's design, specifications, and functionality2. However, program documentation may not reflect the actual implementation or operation of the system, and it may not reveal any discrepancies or defects in the edit routine. Interviews with knowledgeable users is an audit procedure that involves asking questions to the people who use or manage the system3. However, interviews with knowledgeable users may not provide sufficient or objective evidence of the edit routine's effectiveness, and they may be influenced by personal opinions or biases. Reviewing source code is an audit procedurethat involves analyzing the programming language and logic of the system4. However, reviewing source code may not be feasible or practical for complex or large systems, and it may not demonstrate how the edit routine performs in real scenarios.

NEW QUESTION: 499

在完成對IT系統的滲透測試並得出測試結果後，下一步應該是：

A. 漏洞掃描和重新確認。

B. 分析對系統所做的所有變更。

C. 補救和重新測試。

D. 維護測試報告的機密性。

Answer: C (LEAVE A REPLY)

The correct answer is C. Remediation and retesting.

ISACA guidance explains that penetration testing identifies exploitable weaknesses and provides guidance to address them. Once findings are identified, the next logical and control-appropriate step is to remediate the weaknesses and then retest to confirm they have been effectively resolved.

Option A is not the best next step because vulnerability scanning may supplement testing, but after a completed penetration test with findings, the priority is to fix what was found and verify closure.

Option B may be part of root cause work, but it is not the primary next step.

Option D is important from an information-handling perspective, but it does not address the control weaknesses identified by the test.

Therefore, the correct answer is C, because findings from a penetration test should drive remediation followed by retesting to validate that the identified weaknesses have been corrected.
References (Official ISACA):
* ISACA, The Future of Cybersecurity Assessments Is Here - VAPT identifies weaknesses and provides guidance to address them.
* ISACA, Taking a Risk-Based Approach to Pen Testing - findings should be evaluated and acted on according to business impact.
* ISACA, Smarter Testing Equals Safer Digital Experiences - findings should be assessed for exploitability and impact, supporting focused remediation.

NEW QUESTION: 500
在高容量、即時系統中，持續監控和分析交易處理最有效的技術是：
A. 綜合測試設施(ITF)。
B. 平行模擬。
C. 交易標記。
D. 嵌入式稽核模組。
Answer: C (LEAVE A REPLY)
Transaction tagging is a technique by which transactions are marked with unique identifiers or headers and traced through the system using agents or sensors at each processing point1. Transaction tagging allows for continuous monitoring and analysis of transaction processing in a high-volume, real-time system by providing visibility into the performance, availability, and reliability of each transaction and its components1. Transaction tagging can also help to identify and isolate errors, bottlenecks, anomalies, and security issues in the system1.

NEW QUESTION: 501
在開發環境中，使用哪種類型的測試來識別原始程式碼中的安全漏洞？
A. 互動式應用程式安全測試(IAST)
B. 動態分析安全測試(DAST)
C. 運行時應用程式自我保護(RASP)
D. 靜態分析安全測試(SAST)
Answer: (SHOW ANSWER)

NEW QUESTION: 502
在法醫資料收集和保存程序中，下列何者最為重要？
A. 確保裝置的實體安全
B. 維護資料完整性
C. 維護監管鏈
D. 確定要使用的工具

Answer: (SHOW ANSWER)

The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the data on the devices is accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 503

下列哪一項是關鍵績效指標 (KPI) 在支援業務流程效率方面的主要作用？

A. 分析工作流程，以優化業務流程並消除不□生價□的任務

B. 評估用於監控控制性能的工具的成本效益

C. 根據業務流程評估軟體交付物的功能

D. 以便對流程績效和目標偏差進行後續分析並得出結論

Answer: (SHOW ANSWER)

Comprehensive and Detailed in-Depth Explanation:

The primary role of KPIs is to provide measurable insights into the performance of business processes and identify variances that may require corrective actions. KPIs help organizations understand whether their processes are achieving desired outcomes and where improvements are needed.

While Option A discusses workflow optimization, it is a secondary benefit rather than the primary purpose.

Options B and C do not accurately describe the core purpose of KPIs.

ISACA CISA Reference: Domain 1 - Information System Auditing Process

NEW QUESTION: 504

在審計過程中，資訊系統審計員發現，在許多情況下，過多的權限並沒有從系統中移除。下列哪一項是審計師的最佳建議？

A. 系統管理員應確保指派權限的一致性。
B. IT 安全部門應定期撤銷過多的系統權限。
C. 人力資源部(HR)應刪除已離職員工的存取權限。
D. 直線主管應定期審□並要求修改存取權限
Answer: D (LEAVE A REPLY)
The best recommendation for the auditor to make is D. Line management should regularly review and request modification of access rights. Access rights are the permissions and privileges granted to users to access, view, modify, or delete data or resources on a system or network1. Excessive rights are access rights that are not necessary or appropriate for a user's role or function, and may pose a risk of unauthorized or inappropriate use of data or resources2. Therefore, it is important to ensure that access rights are alignedwith the principle of least privilege, which means that users should only have the minimum level of access required to perform their duties2.
Line management is responsible for overseeing and supervising the activities and performance of their staff, and ensuring that they comply with the organization's policies and standards3. Therefore, line management should regularly review and request modification of access rights for their staff, as they are in the best position to:
Understand the roles and functions of their staff, and determine the appropriate level of access rights needed for them to perform their duties effectively and efficiently.
Monitor and evaluate the usage and behavior of their staff, and identify any changes or anomalies that may indicate excessive or inappropriate access rights.
Communicate and collaborate with IT security or system administrators, who are responsible for granting, revoking, or modifying access rights, and request any necessary adjustments or corrections.

NEW QUESTION: 505
資訊系統審計師受命審□總帳系統中的資料品質。下列哪一項能為審計師提供最有意義的結果？
A. 與企業主討論最大帳□價□
B. 系統漏洞評估
C. 對系統擁有者和維運人員的訪談
D. 對來源文件進行完整性檢□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 506
資訊系統審計員發現，IT經理最近為了降低成本而更改了軟體即服務(SaaS)提供者的合約。新合約導致事件解決時間延長。下列哪一項應該是審計員最該關注的問題？
A. 尚未評估對業務流程的影響。
B. 新合約不符合資訊科技安全政策。
C. 對應的服務等級協定(SLA)未進行修改。

D. 未考慮其他降低成本的方法。

Answer: A (LEAVE A REPLY)

The greatest concern is whether the increased incident resolution time will adversely affect the organization's business operations and whether that impact was properly assessed before the contract change. In ISACA terms, service arrangements should be aligned with business needs and service objectives. If a contract change weakens incident response commitments, the key audit concern is not simply the wording of the SLA, but whether management evaluated the resulting business impact. ISACA guidance notes that support agreements and SLAs should be aligned with internal service expectations and business requirements.

Option A is correct because incident resolution times directly affect availability, continuity, user support, and operational resilience. If the contract now permits slower restoration or resolution, the organization may be exposed to longer outages or degraded services. The central risk is whether management made that trade-off knowingly after analyzing the impact on critical business processes. This is the most important concern from an audit and governance perspective.

Option B is not the best answer because noncompliance with IT security policy could be serious, but the question specifically highlights a change in incident resolution time. Unless there is evidence of an actual policy violation, the more direct concern is operational impact on the business.

Option C is also not the greatest concern. In practice, if the contract terms changed, the SLA may need revision or alignment, but that is more of a documentation and governance symptom. The deeper issue is whether the revised service commitments are acceptable to the business. ISACA guidance stresses alignment of support agreements and SLAs with organizational needs.

Option D is the weakest answer because considering alternative cost-reduction methods is a management decision, not the primary audit concern. Auditors focus on risk and control implications, not whether management explored every possible commercial option.

Therefore, A is the best answer because the most significant issue is whether the organization evaluated the impact of slower incident resolution on business processes before accepting the lower-cost contract.

References (Official ISACA):

* ISACA, A Framework for SIEM Implementation - support agreements should be aligned with internal SLAs.
* ISACA, Top Risks and Rewards of Moving to the Cloud - auditors should review cloud provider SLAs and evaluate continuity implications.
* ISACA Journal, Is Business Continuity Management Still Relevant? - audit concern centers on business impact and risk acceptance.
* ISACA Journal, Understanding Software Metric Use - SLAs should use metrics that are monitored and measured.

NEW QUESTION: 507
下列哪一種策略能□在不影響資料保留實務的前提下，最大程度地優化資料儲存？
A. 限制透過電子郵件傳送的文件附件的大小
B. 自動刪除一年以上的電子郵件
C. 30 天後將電子郵件移至虛擬電子郵件庫
D. 允許員工將大型電子郵件儲存在USB上
Answer: (SHOW ANSWER)
The best strategy to optimize data storage without compromising data retention practices is to limit the size of file attachments being sent via email. This strategy can reduce the amount of storage space required for email messages, as well as the network bandwidth consumed by email traffic. File attachments can be large and often contain redundant or unnecessary information that can be compressed, converted, or removed before sending. By limiting the size of file attachments, the sender can encourage the use of more efficient formats, such as PDF or ZIP, or alternative methods of sharing files, such as cloud storage or web links. This can also improve the security and privacy of email communications, as large attachments may pose a higher risk of being intercepted, corrupted, or infected by malware.
References:
Data Storage Optimization: What is it and Why Does it Matter?
Data storage optimization 101: Everything you need to know

NEW QUESTION: 508
在點對點(P2P)運算環境中，下列何者是確保檔案傳輸完整性的有效方法？
A. 確保檔案透過入侵偵測系統(IDS)進行傳輸。
B. 將環境中的客□端電腦連接到跳轉伺服器。
C. 將訊息認證碼與傳輸的每個檔案關聯。
D. 加密環境中對等節點之間共享的資料包。
Answer: (SHOW ANSWER)

NEW QUESTION: 509
公鑰基礎設施 (PKI) 如何協助驗證數位簽章文件不是偽造的？
A. 透過使用簽署者的公鑰解密簽名
B. 透過使用簽署者的私鑰來驗證簽名
C. 透過檢□接收者的公鑰簽名
D. 透過檢□已簽署文件的審計歷史記錄
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation:
In PKI, when a document is digitally signed:
The signer uses their private key to create the signature.
The recipient uses the signer's public key to decrypt and verify the signature.

If the decrypted hash matches the document's computed hash, the document is authentic and unaltered.
Option A: Correct - verification is done with the public key.
Option B: Incorrect - the private key is only used to sign, not verify.
Option C: Wrong - the receiver's public key is irrelevant.
Option D: Not applicable - audit history is not part of PKI validation.
ISACA Reference: CISA Review Manual 27th Edition, Domain 5, section on PKI and digital signatures.

NEW QUESTION: 510
下列哪一項是識別惡意口部人員竊取敏感資料的最有效方法？
A. 實施資料遺失防護(DLP)軟體
B. 口看邊界防火牆日誌
C. 提供持續的資訊安全意識培訓
D. 建立行為分析監控
Answer: D (LEAVE A REPLY)
The most effective way to identify exfiltration of sensitive data by a malicious insider is to establish behavioral analytics monitoring. Behavioral analytics is the process of analyzing the patterns and anomalies in user behavior to detect and prevent insider threats. Behavioral analytics can help identify unusual or suspicious activities, such as accessing sensitive data at odd hours, transferring large amounts of data to external devices or locations, or using unauthorized applications or protocols. Behavioral analytics can also help correlate data from multiple sources, such as network logs, user profiles, and access rights, to provide a holistic view of user activity and risk.
Data loss prevention (DLP) software is a tool that can help prevent exfiltration of sensitive data by a malicious insider, but it is not the most effective way to identify it. DLP software can block or alert on unauthorized data transfers based on predefined rules and policies, but it may not be able to detect sophisticated or stealthy exfiltration techniques, such as encryption, steganography, or data obfuscation.
Reviewing perimeter firewall logs is a way to identify exfiltration of sensitive data by a malicious insider, but it is not the most effective way. Perimeter firewall logs can show the traffic volume and destination of data transfers, but they may not be able to show the content or context of the data. Perimeter firewall logs may also be overwhelmed by the amount of normal traffic and miss the signals of malicious exfiltration.
Providing ongoing information security awareness training is a way to reduce the risk of exfiltration of sensitive data by a malicious insider, but it is not a way to identify it. Information security awareness training can help educate users on the importance of protecting sensitive data and the consequences of violating policies and regulations, but it may not deter or detect those who are intentionally or maliciously exfiltrating data.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 300

ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription 1 Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog 2 How to Secure Your Company'sLegacy Applications - iCorps

NEW QUESTION: 511
不應允許資料庫管理員(DBA)承擔最終使用者職責：
A. 承擔最終使用者責任
B. 存取敏感資訊
C. 擁有生口文件存取權限
D. 使用緊急使用者 ID
Answer: (SHOW ANSWER)
A database administrator (DBA) should be prevented from having end user responsibilities to avoid a conflict of interest and a violation of the principle of segregation of duties. End user responsibilities may include initiating transactions, authorizing transactions, recording transactions or reconciling transactions. A DBA who has end user responsibilities may compromise the integrity, confidentiality and availability of the data and the database systems. Accessing sensitive information, having access to production files and using an emergency user ID are not end user responsibilities, but rather potential risks or controls associated with the DBA role. References:
Database Administrator (DBA) Definition
Segregation of Duties | ISACA
[End User Definition]

NEW QUESTION: 512
當一個組織決定將其外部客口的技術支援外包時，資訊系統審計師應該建議將下列哪一項作為主要關注領域？
A. 使服務等級協定(SLA)與當前需求保持一致。
B. 監控客口對變更的滿意度。
C. 盡量減少與第三方協議相關的成本。
D. 確保合約中包含審計權。
Answer: A (LEAVE A REPLY)

The primary area of focus when an organization decides to outsource technical support for its external customers is to align service level agreements (SLAs) with current needs. SLAs are contracts that define the scope, quality, and expectations of the services provided by the vendor, as well as the remedies or penalties for non-compliance. SLAs are essential for ensuring that the outsourced technical support meets the customer' s requirements and satisfaction, as well as the organization's objectives andstandards. By aligning SLAs with current needs, the organization can specify the key performance indicators (KPIs), metrics, and targets that reflect the desired outcomes and value of the technical support. This can also help to monitor and evaluate the vendor's performance, identify gaps or issues, and implement corrective actions or improvements.
References:
Service Level Agreement (SLA)Examples and Template
What is an SLA? Best practices for service-level agreements

NEW QUESTION: 513
與手動審口相比，下列哪一項是使用自動安全日誌監控工具來監控特權存取使用情況的主要優勢？
A. 增加偵測可疑活動的可能性
B. 降低與自動化審核相關的成本
C. 縮短了事件回應時間
D. 減少檢口日誌的手動工作量
Answer: A (LEAVE A REPLY)
Automated monitoring tools increase the likelihood of detecting suspicious activity (Option A) by continuously analyzing security logs for anomalies.
ISACA CISA Reference: Security Information and Event Management (SIEM) solutions are recommended for privileged access monitoring.

NEW QUESTION: 514
第三方顧問正在負責會計系統的更換工作。下列哪一項應該是資訊系統審計師最該關注的問題？
A. 資料遷移不屬於合約約定的活動範圍。
B. 此次替換工作將在年末報告期間臨近時進行。
C. 使用者部門將管理存取權限。
D. 測試由第三方顧問執行
Answer: C (LEAVE A REPLY)
The greatest concern for an IS auditor in this scenario is that the user department will manage access rights to the new accounting system. This could pose a significant risk of unauthorized access, segregation of duties violations, data tampering and fraud. The IS auditor should ensure that access rights are defined, approved and monitored by an independent function, such as IT security or internal audit. The other options are not as concerning as option C, as they can be mitigated by other controls or procedures. Data

migration is an important part of the system replacement project, but it can be performed by another party or verified by the IS auditor. The timing of the replacement near year-end reporting is a challenge, but it can be managed by proper planning, testing and contingency plans. Testing performed by the third-party consultant is acceptable, as long as it is reviewed and validated by the IS auditor or another independent party. References: CISA Review Manual (Digital Version) 1, Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.4: System Implementation.

NEW QUESTION: 515
下列哪一項是組織自帶設備 (BYOD) 政策中防止資料外洩的最佳建議？
A. 要求員工放棄與 BYOD 裝置上的資料相關的隱私權。
B. 要求在自帶設備 (BYOD) 上口用多因素身份驗證，
C. 明確員工報告遺失或被竊自備設備的責任。
D. 僅允許已註冊的 BYOD 裝置存取網路。
Answer: B (LEAVE A REPLY)
The best recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage is to require multi-factor authentication on BYOD devices. BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, to access the organization's network, data, and systems. Data leakage is a risk that involves the unauthorized or accidental disclosure or transfer of sensitive or confidential data from the organization to external parties or devices.
Multi-factor authentication is a security measure that requires users to provide two or more pieces of evidence to verify their identity and access rights, such as passwords, tokens, biometrics, or codes. Multi-factor authentication can help prevent data leakage by reducing the likelihood of unauthorized access to the organization's data and systems throughBYOD devices, especially if they are lost, stolen, or compromised. The other options are not as effective as requiring multi-factor authentication on BYOD devices, because they either do not prevent data leakage directly, or they are reactive rather than proactive measures.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

NEW QUESTION: 516
下列哪一項控制措施最能有效防止未經授權存取被竊或遺失筆記型電腦上的機密資訊？
A. 遠端擦除功能
B. 磁碟加密
C. 使用者意識
D. 受密碼保護的文件
Answer: B (LEAVE A REPLY)
Thebest protectionfor a stolen laptop isfull disk encryption, which prevents unauthorized accesseven if the device is lost.

Option A (Incorrect):Remote wipe capabilitiesare useful, but theyrequire an internet connectionto function, which is not always available when a device is stolen.
Option B (Correct):Full disk encryption (FDE)ensures that data remainsunreadablewithout the correct decryption key,even if the hard drive is removed.
Option C (Incorrect):User awarenessis helpful, but itdoes not physically securedata on a lost device.
Option D (Incorrect):Password-protected filescan be bypassed by copying them to another system, making them an inadequate security measure.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coversencryption, data security, and endpoint protection.

NEW QUESTION: 517
下列哪一項是最佳的資料完整性檢口方法？
A. 統計每日處理的交易數量
B. 執行序列檢口
C. 追溯資料至源頭
D. 準備並執行測試數據
Answer: C (LEAVE A REPLY)
Data integrity is the property that ensures that data is accurate, complete, consistent, and reliable throughout its lifecycle. The best data integrity check is tracing data back to the point of origin, which is the source where the data was originally created or captured. This check can verify that data has not been altered or corrupted during transmission, processing, or storage. It can also identify any errors or discrepancies in data entry or conversion. Counting the transactions processed per day is a performance measure that does not directly assess data integrity. Performing a sequence check is a validity check that ensures that data follows a predefined order or pattern. It can detect missing or out-of-order data elements, but it cannot verify their accuracy or completeness. Preparing and running test data is a testing technique that simulates real data to evaluate how a system handles different scenarios. It can help identify errors or bugs in the system logic or functionality, but it cannot ensure data integrity in production environments. References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

NEW QUESTION: 518
資訊系統審計員在評估變更管理流程時，必須從變更日誌中抽取樣本。審計員確認變更日誌完整性的最佳方法是什麼？
A. 訪談變更管理人員，了解其完整性。
B. 從日誌中取出一個項目，並追溯到系統。
C. 取得管理階層對完整性的證明。
D. 從系統中取得最後一次更改，並追溯到日誌。

Answer: (SHOW ANSWER)

The answer D is correct because the best way for the auditor to confirm the change log is complete is to take the last change from the system and trace it back to the log. A change log is a record of all the changes that have been made to a system, such as software updates, bug fixes, configuration modifications, etc. A change log should contain information such as the date and time of the change, the description and purpose of the change, the person or service who made the change, and the approval status of the change. A complete change log helps to ensure that the system is secure, reliable, and compliant with the relevant standards and regulations.

An IS auditor evaluating the change management process must select a sample from the change log to verify that the changes are properly authorized, documented, tested, and implemented. However, before selecting a sample, the auditor must ensure that the change log is complete and accurate, meaning that it contains all the changes that have been made to the system and that there are no missing, duplicated, or falsified entries. To do this, the auditor can use a technique called backward tracing, which involves taking the last change from the system and tracing it back to the log. This way, the auditor can check if the change is recorded in the log with all the relevant details and if there are any gaps or inconsistencies in the log. If the last change from the system is not found in the log or does not match with the log entry, it indicates that the change log is incomplete or inaccurate.

The other options are not as good as option D. Interviewing change management personnel about completeness (option A) is not a reliable way to confirm the change log is complete because it relies on subjective opinions and self-reported information, which may not be truthful or accurate. Taking an item from the log and tracing it back to the system (option B) is a technique called forward tracing, which can be used to verify that a specific change in the log has been implemented in the system. However, this technique does not confirm that all changes in the system are recorded in the log. Obtaining management attestation of completeness (option C) is not a sufficient way to confirm the change log is complete because it does not provide any evidence or verification of completeness. Management attestation may also be biased or influenced by conflicts of interest.

References:

IS Audit Basics: Auditing Data Privacy

Audit Logging: What It Is and How It Works | Datadog

Change Management for SOC: Risks, Controls, Audits, Guidance

Turn auditing on or off | Microsoft Learn

#118 | ITGC- System Change (Audit) Log Review - A2Q2

NEW QUESTION: 519

網路分析師在非工作時間監控網路時，偵測到疑似針對關鍵伺服器的暴力破解攻擊。在審□警報以確保其準確性後，下一步該做什麼？

A. 隔離受影響的系統。

B. □動事件回應計畫。

C. 將所有步驟記錄在書面報告中。
D. 進行根本原因分析。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 520
在依賴前任審計師的工作時，下列哪一項是最重要的考慮因素？
A. 前任審計師的資格
B. 前任審計師發現的問題數量
C. 管理階層同意並提出建議
D. 上次審計的持續時間
Answer: (SHOW ANSWER)

NEW QUESTION: 521
小型企業正在實施控制自我評估(CSA)計劃，並利用口部稽核職能對其口部控制進行年度測試。下列哪一項是這種方法最顯著的優點？
A. 合規成本降低。
B. 風險被更早發現。
C. 企業主可以更專注於他們的核心職責。
D. 第一線管理人員更有動力避免控制例外。
Answer: B (LEAVE A REPLY)
The most significant benefit of implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually is that risks are detected earlier. A CSA program is a process that enables business owners and managers to assess and improve their own internal controls on a regular basis, without relying on external auditors or consultants. A CSA program can help identify and mitigate risks, enhance performance, increase accountability, and foster a culture of control within the organization. By leveraging the internal audit function to test its internal controls annually, a small business unit can also obtain independent assurance and validation of its CSA results, as well as recommendations for improvement. This approach can help reduce compliance costs, as external audits may be less frequent or extensive. However, this is not the most significant benefit, as compliance costs are only one aspect of the total cost of risk. Business owners can also focus more on their core roles, as they can delegate some of their control responsibilities to their staff or teams through CSA. However, this is not the most significant benefit, as business owners still need to oversee and monitor their CSA activities and results, and ensure that they align with their strategic objectives and priorities. Line management may also be more motivated to avoid control exceptions, as they are directly involved in assessing and improving their own controls through CSA. However, this is not the most significant benefit, as motivation alone may not be sufficient to ensure effective control design and operation. References: Info Technology and

Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 522
下列哪一項是並行處理在新系統實作中的主要優勢？
A. 確保新系統符合功能要求
B. 給予使用者更多時間完成新系統的培訓
C. 與其他系統實施方案或方法相比，可大幅節省成本。
D. 確保新系統符合效能要求
Answer: D (LEAVE A REPLY)
Parallel processing is a system implementation approach that involves running the new system and the old system simultaneously for a period of time until the new system is verified and accepted. The primary advantage of parallel processing is that it provides assurance that the new system meets performance requirements and produces the same or better results as the old system. Parallel processing also minimizes the risk of system failure and data loss, as the old system can be used as a backup or fallback option in case of any problems with the new system.

NEW QUESTION: 523
在IT投資的商業案例中，下列何者最為重要？
A. 風險評估
B. 安全要求
C. 業務影響分析(BIA)
D. 成本效益分析
Answer: D (LEAVE A REPLY)

NEW QUESTION: 524
下列何者最能幫助資訊系統審計員確認從輸入來源進行批次處理以過帳交易是否成功？
A. 錯誤日誌審□
B. 項目總數
C. 哈希總計
D. 總金額
Answer: C (LEAVE A REPLY)
Hash totals are a control technique used to ensure data integrity during batch processing. A hash total is a calculated value based on the data in a batch. This value is compared to a pre-calculated hash total to confirm that all data has been processed correctly and without alteration.
References
ISACA CISA Review Manual (27th Edition): Hash totals are discussed within the context of batch processing controls.

Other Auditing Resources: Hash totals are a fundamental control technique discussed in various audit and information security publications.

NEW QUESTION: 525
使用乾式管道滅火系統而非濕式管道系統的主要優點是：乾式管道系統：
A. 在抑制火焰方面更有效。
B. 允許有更多時間中止抑制劑的釋放。
C. 洩漏風險降低。
D. 專門分散乾化學抑制劑。
Answer: C (LEAVE A REPLY)
The primary benefit of using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry- pipe system has a decreased risk of leakage, as the pipes are filled with pressurized air or nitrogen instead of water until the system is activated. A wet-pipe system has a higher risk of leakage, corrosion, and freezing. A dry-pipe system is not more effective at suppressing flames, as it uses the same water-based suppressant as a wet-pipe system. A dry-pipe system does not allow more time to abort release of the suppressant, as it has a delay of only a few seconds before the water is released. A dry-pipe system does not disperse dry chemical suppressants exclusively, as it uses water as the primary suppressant. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.3

NEW QUESTION: 526
配置管理系統的主要目的是：
A. 追蹤軟體更新。
B. 定義軟體基線。
C. 支援發布流程。
D. 規範變更審核流程。
Answer: (SHOW ANSWER)
A configuration management system is a process that establishes and maintains the consistency of a product's attributes throughout its life cycle. It helps to identify and control the functional and physical characteristics of a product, and to record and report any changes to those characteristics. A configuration management system also supports the audit of the product to verify its conformance to requirements.
One of the key activities of a configuration management system is to define baselines for software. A baseline is a fixed reference point that serves as a basis for comparison and measurement. A baseline can be established for any configuration item, such as a requirement, a design document, a test plan, or a software component. A baseline helps to ensure that the software product meets its intended purpose and quality standards, and that any changes to the software are controlled and documented.

A configuration management system also supports other activities, such as tracking software updates, supporting the release procedure, and standardizing change approval, but these are not its primary purpose.
Therefore, the other options are incorrect.
References: : What is configuration management - Red Hat : Configuration Management | Definition, Importance and Benefits - ServerWatch

NEW QUESTION: 527
在選擇要納入 IT 審計計畫的項目時，下列何者能為IS 審計員提供最有用的資訊？
A. 專案章程
B. 專案計劃
C. 專案問題日誌
D. 專案商業案例
Answer: D (LEAVE A REPLY)
A project business case is a document that describes the rationale and justification for initiating a project, based on its expected costs, benefits, risks, and feasibility. A project business case provides the most useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, because it helps the IS auditor to:
Understand the purpose, scope, objectives, and deliverables of the project Assess the alignment of the project with the organization's strategy, vision, and goals Evaluate the value proposition and return on investment of the project Identify the key stakeholders, sponsors, and owners of the project Analyze the potential risks and issues associated with the project Compare and prioritize the project with other competing projects The other possible options are:
A). Project charter: A project charter is a document that formally authorizes and defines the high-level scope, roles, responsibilities, and authority of a project. A project charter provides some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project charter does not provide enough details about the costs, benefits, risks, and feasibility of the project, which are essential for evaluating its suitability for an IT audit plan.
B). Project plan: A project plan is a document that outlines the detailed scope, schedule, budget, resources, quality, and communication plans of a project. A project plan provides

some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project plan does not provide enough information about the rationale, justification, value proposition, and alignment of the project with the organization's strategy and goals, which are important for assessing its relevance for an IT audit plan.
C). Project issue log: A project issue log is a document that records and tracks the issues that arise during a project's execution and how they are resolved. A project issue log provides some useful information to an IS auditor when selecting projects for inclusion in an IT audit plan, but it is not the most useful information. A project issue log does not provide enough information about the purpose, objectives, benefits, and feasibility of the project, which are critical for determining its priority for an IT audit plan.

NEW QUESTION: 528
如果由負責核對組織設備清單的人員執行下列哪項任務，會造成最大的職責分離SoD)問題？
A. 發放設備給員工
B. 建立裝置策略
C. 核准發放設備
D. 用於備用零件的追蹤設備
Answer: A (LEAVE A REPLY)

NEW QUESTION: 529
公司購買並實施系統和效能監控軟體一個月後，報告文件過大，因此無人口看或採取行動最有效的行動方案是：
A. 評估替換系統和效能監控軟體。
B. 將系統監控軟體的功能限制為與安全相關的事件。
C. 重新安裝系統和效能監控軟體。
D. 使用分析工具口生系統和效能監控軟體的異常報告
Answer: D (LEAVE A REPLY)
Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:
CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
CISA Review Questions, Answers and Explanations Database, Question ID 219

NEW QUESTION: 530

在系統開發專案的詳細設計階段，資訊系統稽核員最需要確定下列哪一項□容？
A. 程序編碼標準已遵循
B. 已製定驗收測試標準
C. 資料轉換程式已建立。
D. 此設計已獲得高階管理人員的批准。
Answer: B (LEAVE A REPLY)
The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase.
Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

NEW QUESTION: 531
下列哪一項顯示□部稽核組織的結構是為了支援報告流程的獨立性和清晰度？
A. 審計員負責執行營運職責或活動。
B. □部稽核經理在職能上向高階管理人員報告。
C. □部稽核經理向審計委員會報告工作。
D. 稽核人員負責評估和運作□部控制系統。
Answer: (SHOW ANSWER)
The internal audit manager should have a reporting line to the audit committee, which is an independent body that oversees the internal audit function and ensures its objectivity and accountability. Reporting functionally to a senior management official may compromise the independence and clarity of the internal audit reporting process, as senior management may have a vested interest in the audit results or influence the audit scope and priorities.
*References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1002 Independence, "The chief audit executive (CAE)should report functionally to the board or its equivalent (e.g., audit committee) and administratively to executive management." 1

NEW QUESTION: 532
在評估組織的資料轉換和基礎設施遷移計畫時，資訊系統稽核員最需要核實下列哪一項□容？
A. 策略目標已考慮在□。

B. 包含回滾計劃。
C. 包含程式碼檢口審口。
D. 已成立移民指導委員會。
Answer: B (LEAVE A REPLY)
The most important thing for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan is that a rollback plan is included. A rollback plan is a contingency plan that describes the steps and actions to be taken in case the data conversion or infrastructure migration fails or causes unacceptable problems or risks. A rollback plan can help to restore the original data and infrastructure, minimize the impact on the business operations and functions, and ensure the continuity and availability of the IT services. The IS auditor should verify that the rollback plan is feasible, tested, documented, and approved, and that it covers all the possible scenarios and outcomes of the data conversion or infrastructure migration. Theother options are not as important as verifying the rollback plan, because they either do not address the potential failure or disruption of the data conversion or infrastructure migration, or they are partof the normal planning and execution process rather than a contingency plan. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION: 533
下列哪一項是與在網路伺服器上儲存客口資料相關的最大風險？
A. 數據可用性
B. 資料保密性
C. 資料完整性
D. 資料冗餘
Answer: (SHOW ANSWER)
The greatest risk associated with storing customer data on a web server is data confidentiality. Data confidentiality is the property that ensures that data are accessible only to authorized entities or individuals, and protected from unauthorized disclosure or exposure. Storing customer data on a web server poses a high risk to data confidentiality, as web servers are exposed to the internet and may be vulnerable to various types of attacks or breaches that can compromise the security and privacy of customer data, such as hacking, phishing, malware, denial of service (DoS), etc. Customer data may contain sensitive or personal information that can cause harm or damage to customers or the organization if disclosed or exposed, such as identity theft, fraud, reputation loss, legal liability, etc. Data availability is the property that ensures that data are accessible and usable by authorized entities or individuals when needed. Data availability is a risk associated with storing customer data on a web server, as web servers may experience failures or disruptions that can affect the accessibility and usability of customer data, such as hardware faults, network issues, power outages, etc.
However, data availability is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data integrity

is the property that ensures that data are accurate and consistent, and protected from unauthorized modification or corruption. Data integrity is a risk associated with storing customer data on a web server, as web servers may be subject to attacks or errors that can affect the accuracy and consistency of customer data, such as injection attacks, tampering, replication issues, etc. However, data integrity is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data redundancy is the condition of having duplicate or unnecessary data in a database or system. Data redundancy is not a risk associated with storing customer data on a web server, but rather a result of poor database design or management.

NEW QUESTION: 534
在評估組織的異地儲存設施時，資訊系統稽核員應專注於下列哪一項？
A. 共享設施
B. 物理與環境控制的充分性
C. 業務連續性計劃 (BCP) 測試結果
D. 保留政策與期限
Answer: B (LEAVE A REPLY)
The IS auditor's primary focus when evaluating an organization's offsite storage facility should be the adequacy of physical and environmental controls. Physical and environmental controls are essential to protect the offsite storage facility from unauthorized access, theft, fire, water damage, pests or other hazards that could compromise the integrity and availability of backup media. Shared facilities is something that the IS auditor should consider when evaluating the offsite storage facility, but it is not the primary focus. Results of business continuity plan (BCP) test or retention policy and period are things that the IS auditor should review when evaluating the organization's BCP or backup strategy, not the offsite storage facility itself. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 388

NEW QUESTION: 535
哪種類型的威脅可以利用大量自動化社群媒體帳號來竊取資料、發送垃圾郵件或發動分散式阻斷服務 (DDoS) 攻擊？
A. 資料探勘
B. 殭屍網路攻擊
C. 網路釣魚嘗試
D. 惡意軟體共享
Answer: B (LEAVE A REPLY)

NEW QUESTION: 536
資訊系統稽核員正在分析應用程式系統日誌中記錄的部分存取記錄。如果發現任何異常情況，審計員打算展開深入調口 哪一種抽樣方法比較適合？

A. 發現性抽樣
B. 判斷抽樣
C. 變數抽樣
D. 分層抽樣
Answer: A (LEAVE A REPLY)
Discovery sampling is an appropriate sampling method for an IS auditor who intends to launch an intensive investigation if one exception is found. Discovery sampling is a type of attribute sampling that determines the sample size based on an acceptable risk of not finding at least one occurrence of an attribute when a given rate of occurrence exists in a population. Discovery sampling can be used by an IS auditor who wants to detect fraud or errors that have a low probability but high impacton an audit objective. The other options are not appropriate sampling methods for this purpose, as they may involve judgmental sampling, variable sampling, or stratified sampling. References:
CISA Review Manual (Digital Version), Chapter 2, Section 2.31
CISA ReviewQuestions, Answers and Explanations Database, Question ID 230

NEW QUESTION: 537
資訊系統審計師正在分析某供應商的應付帳款交易樣本，發現其中一筆交易的金額是平均交易金額的五倍。接下來，審計師應該採取下列哪一項措施？
A. 立即向審計委員會報告差異
B. 要求受審計方解釋差異。
C. 將樣本量增加到總體的 100%
D. 從樣本總體中排除該交易
Answer: B (LEAVE A REPLY)
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. The next step that the auditor should do is to request an explanation of the variance from the auditee. This is because the variance may indicate an error, fraud, or an unusual but legitimate transaction that requires further investigation. The auditor should not report the variance immediately to the audit committee without verifying its cause and significance. The auditor should not increase the sample size to 100% of the population without considering the cost-benefit analysis and the sampling methodology. The auditor should not exclude the transaction from the sample population without justification, as itmay affect the validity and reliability of the audit results. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 538
作為持續部署程序的一部分，安全程式碼審口屬於哪種類型的控制？
A. 偵探
B. 邏輯
C. 預防

D. 修正

Answer: C (LEAVE A REPLY)

Secure code reviews as part of a continuous deployment program are preventive controls. Preventive controls are controls that aim to prevent or avoid undesirable events or outcomes from occurring, such as errors, defects, or incidents. Secure code reviews are activities that examine and evaluate the source code of a software or application to identify and eliminate any vulnerabilities, flaws, or weaknesses that may compromise its security, functionality, or performance. Secure code reviews as part of a continuous deployment program can help prevent or avoid security issues or incidents from occurring by ensuring that the code is secure and compliant before it is deployed to production. The other options are not correct types of controls for secure code reviews as part of a continuous deployment program, as they have different meanings and functions. Detective controls are controls that aim to detect or discover undesirable events or outcomes that have occurred, such as errors, defects, or incidents. Logical controls are controls that use software or hardware mechanisms to regulate or restrict access to IT resources, such as data, systems, or networks.

Corrective controls are controls that aim to correct or rectify undesirable events or outcomes that have occurred, such as errors, defects, or incidents. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 539

資訊系統審計員發現，關鍵系統的容量管理由T部門執行，而業務部門並未參與其中。審計員的主要關注點是：

A. 未能最大限度地利用設備

B. 業務口能需求意外增加。

C. 資料中心儲存容量過剩的成本

D. 對未來商業專案融資的影響。

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 540

下列何者最能幫助資料遺失防護 (DLP) 工具偵測傳輸過程中敏感資料的移動？

A. 網路流量日誌

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

NEW QUESTION: 541
在實施新的 Web 應用程式時，下列哪項控制措施最能有效防止系統故障？
A. 系統復原計劃
B. 系統測試
C. 業務連續性計劃(BCP)
D. 交易監控
Answer: B (LEAVE A REPLY)
Thoroughsystem testingbefore deployment helps identify potentialbugs, vulnerabilities, and performance issuesto prevent system failures.
System Testing (Correct Answer - B)
Detects defects that could lead to system crashes.
Ensures compatibility and performance stability.
Example:Stress testing an e-commerce application to prevent crashes on Black Friday.
System Recovery Plan (Incorrect - A)
Focuses on recovery after failure rather than prevention.
Business Continuity Plan (Incorrect - C)
Addresses overall business resilience, not application stability.
Transaction Monitoring (Incorrect - D)
Detects fraud and anomalies but does not prevent failures.
References:
ISACA CISA Review Manual
NIST 800-160 (Systems Security Engineering)

NEW QUESTION: 542
下列何者最能支持合規計畫的有效性？
A. 實施有關合規法規要求的意識提升計劃
B. 實施治理、風險和合規 (GRC) 工具以追蹤法規遵守情況
C. 評估並追蹤所有合規性稽核結果
D. 監控哪些合規法規適用於該組織
Answer: (SHOW ANSWER)
Assessing and tracking all compliance audit findings is the best way to support the effectiveness of a compliance program. This allows an organization to identify areas of non-compliance, take corrective action, and monitor improvements over time12. While implementing an awareness plan, using a governance, risk, and compliance (GRC) tool, and monitoring applicable regulations can contribute to a compliance program, they do not provide the same level of continuous improvement and effectiveness as assessing and tracking audit findings.

NEW QUESTION: 543
資訊系統審計經理正在審口最近完成的企業災難復原測試審計的工作底稿。為了證實審計結論，資訊系統審計經理應該重點審口下列哪些口容？
A. 資料中心人員與稽核員訪談概述
B. 先前涉及其他企業災難復原審計的審計報告
C. 反映審計意見的關於已發現缺陷的摘要備忘錄
D. 所有緊急測試的成功與不足之處的詳細證據
Answer: (SHOW ANSWER)
The IS audit manager should specifically review the detailed evidence of the successes and weaknesses of all contingency testing to substantiate the conclusions of the audit of the corporate disaster recovery test. This is because the detailed evidence can provide the audit manager with a clear and objective picture of how well the disaster recovery plan was executed, what issues or gaps were encountered, and what recommendations or actions were taken to address them. The detailed evidence can also help the audit manager to verify the accuracy, completeness, and validity of the audit findings, as well as to evaluate the adequacy and effectiveness of the disaster recovery controls.
The other options are not as specific or relevant as the detailed evidence of all contingency testing. Overviews of interviews between data center personnel and the auditor may

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

NEW QUESTION: 544
下列哪一種方法最有助於偵測透過公司電子郵件發送的機密文件未經授權的揭露？
A. 要求所有使用者在發送文件前對其進行加密
B. 在企業網路上安裝防火牆
C. 報告所有標記為機密的外發電子郵件。
D. 根據預先定義條件監控所有電子郵件
Answer: (SHOW ANSWER)
To detect unauthorized disclosure of confidential documents sent over corporate email, monitoring all emails based on pre-defined criteria is the best approach. This involves setting up automated monitoring systems that analyze email content, attachments, and metadata to identify any potential unauthorized disclosures. By defining specific criteria (such as keywords related to confidential information), organizations can proactively detect and prevent leaks. Requiring encryption before sending documents (option A) is important but does not address monitoring for unauthorized disclosures. Firewalls (option B) protect the network but do not specifically focus on email content. Reporting outgoing emails marked as confidential (option C) relies onuser self-reporting and may not catch all incidents12. References: 1(https://www.isaca.org/resources/isaca-journal /past-issues/2010/data-governance-for-privacy-confidentiality-and-compliance-a-holistic-approach) 2 (https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-6/best-practices-for- privacy-audits)

NEW QUESTION: 545
資訊系統審計員正在檢口前端子分類帳和主分類帳。如果這兩個系統之間的帳口映射有缺陷，下列哪一項是最令人擔憂的問題？
A. 同一日記帳分錄的重複過帳
B. 無法支援新的業務交易
C. 未經授權更改帳口屬性
D. 財務報告不準確
Answer: D (LEAVE A REPLY)

The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets.
A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.
Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double-posting of a single journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

NEW QUESTION: 546
管理承包商存取資料中心的最有效方法是什麼？
A. 訪客配戴的識別徽章
B. 訪客身分驗證
C. 訪客進入需有陪同人員
D. 管理層批准訪客訪問
Answer: C (LEAVE A REPLY)

NEW QUESTION: 547
資訊系統審計員在審口系統開發生命週期(SDLC)時發現，系統中沒有商業案例的要求。下列哪一項應該是該組織最關注的問題？
A. 專案對業務的影響沒有充分分析。
B. 業務資源尚未最佳配置。
C. 供應商選擇標準未被充分評估。
D. 專案成本超出既定預算。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 548

對於審口組織業務關鍵型伺服器硬體現場預防性維護情況的資訊系統審計員而言，下列哪些方面最為重要？

A. 預防性維護成本超過了企業分配的預算。

B. 預防性維護尚未獲得資訊系統批准

C. 預防性維護外包給多家供應商，無需簽署保密協議NDA)。

D. 預防性維護計畫是基於平均故障間隔時間(MTBF)參數。

Answer: C (LEAVE A REPLY)

The answer C is correct because preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements (NDAs) would be of greatest concern to an IS auditor reviewing on-site preventive maintenance for an organization's business-critical server hardware. This is because outsourcing preventive maintenance to multiple vendors without NDAs exposes the organization to the risk of unauthorized access, disclosure, or modification of sensitive data and information stored on the servers. NDAs are legal contracts that bind the vendors to protect the confidentiality and security of the data and information they access or handle during the preventive maintenance. Without NDAs, the vendors may not have any obligation or incentive to safeguard the data and information, and they may misuse, leak, or compromise them for malicious or commercial purposes. This could result in financial losses, reputational damage, legal liabilities, or regulatory penalties for the organization.

The other options are not as concerning as option C. Preventive maintenance costs exceed the business allocated budget (option A) is a financial issue that may affect the profitability or efficiency of the organization, but it does not directly impact the security or availability of the server hardware. Preventive maintenance has not been approved by the information system (option B) is a procedural issue that may indicate a lack of coordination or communication between the IT department and the business units, but it does not necessarily affect the quality or effectiveness of the preventive maintenance. The preventive maintenance schedule is based on mean time between failures (MTBF) parameters (option D) is a technical issue that may influence the frequency or timing of the preventive maintenance, but it does not imply any risk or deficiency in the preventive maintenance itself.

References:

What is a Maintenance Audit?

How to audit your preventative maintenance schedule

5 Step Maintenance Management Program Audit

How do you get effective Preventive Maintenance really?

What is a Planned Preventative MaintenanceAudit?

NEW QUESTION: 549

對於決定將關鍵任務應用程式整合到大型伺服器上進行 IT 容量管理的組織而言，下列哪一項會帶來最大的潛在問題？

A. 伺服器故障可能會對更多應用程式口生負面影響。

B. 持續監控伺服器容量的工作可能成本很高。
C. 尖峰時段網路頻寬可能會下降。
D. 準確預測伺服器容量可能更加困難。
Answer: (SHOW ANSWER)
Consolidating mission-critical applications onto a single large server introduces a single point of failure. If the server experiences an outage, all hosted applications could be impacted simultaneously, leading to significant operational disruptions. While continuous monitoring costs, potential network bandwidth issues, and challenges in capacity forecasting are valid concerns, the risk of a single outage affecting multiple critical applications presents the most substantial threat to business continuity.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 550
對於審口執行關鍵業務流程的許可軟體合約的資訊系統審計員來口，最令人擔憂的問題是什麼？
A. 合約中沒有審計權條款。
B. 未就營運等級協議(OLA)進行談判。
C. 多家供應商未能依承諾日期交付口品。
D. 軟體託管未進行協商。
Answer: D (LEAVE A REPLY)
The greatest concern for an IS auditor reviewing contracts for licensed software that executes a critical business process is that software escrow was not negotiated. Software escrow is an arrangement where a third- party holds a copy of the source code and documentation of a licensed software in a secure location. The software escrow agreement specifies the conditions under which the licensee can access the escrowed materials, such as in case of bankruptcy, termination, or breach of contract by the licensor. Software escrow is important for ensuring the continuity and availability of a critical business process that depends on a licensed software. Without software escrow, the licensee may face significant risks and challenges in maintaining, modifying, or recovering the software in case of any disruption or dispute with the licensor. References:
CISA Review Manual (Digital Version)
CISA Questions, Answers and Explanations Database

NEW QUESTION: 551
資訊系統審計師正在為一份財務應用系統採購招標書提供意見。下列哪一項是審計師最該提出的建議？
A. 該申請應符合組織的要求。
B. 設計中應包含稽核追蹤。

C. 潛在供應商應具備相關領域的經驗。
D. 應定期對供應商員工進行背景調口。
Answer: B (LEAVE A REPLY)
This is because audit trails are records of system activity and user actions that can provide evidence of the validity and integrity of transactions and data in a financial application system. Audit trails can help to ensure compliance with laws, regulations, policies, and standards, as well as to detect and prevent fraud, errors, or misuse of information. Audit trails can also facilitate auditing, monitoring, and evaluation of the financial application system's performance and controls1.
The application should meet the organization's requirements (A) is not the best answer, because it is a general and obvious criterion that applies to any application system acquisition, not a specific and important recommendation for a financial application system. The organization's requirementsshould be clearly defined and documented in the RFP, but they may not necessarily include audit trails as a design feature.
Potential suppliers should have experience in the relevant area is not the best answer, because it is a factor that affects the selection of the supplier, not the design of the financial application system. The experience and reputation of potential suppliers should be evaluated and verified during the RFP process, but they may not guarantee that the supplier will include audit trails in the design.
Vendor employee background checks should be conducted regularly (D) is not the best answer, because it is a measure that affects the security and trustworthiness of the vendor, not the design of the financial application system. Vendor employee background checks should be performed as part of the vendor management and due diligence process, but they may not ensure that the vendor will include audit trails in the design.

NEW QUESTION: 552
一個關鍵任務應用程式使用單節點資料庫伺服器。資料庫服務曾多次因執行例行補丁而停止，導致應用程式中斷。下列哪一項應該是資訊系統審計員最應該關注的問題？
A. 大量計劃口的資料庫更改
B. 由供應商執行的補丁
C. 因應用程式故障造成的收入損失
D. 存在單點故障
Answer: D (LEAVE A REPLY)

NEW QUESTION: 553
半夜，口班程式設計師打電話給安全管理員，口多個程式運作失敗，並要求存取即時系統。最佳因應措施是什麼？
A. 要求變更請求已完成並獲得批准
B. 給程式設計師一個緊急 ID 以便其臨時訪問，並審口其活動。
C. 給予程式設計師只讀權限以調口問題。

D. 第二天口看活動日誌並調口任何可疑活動

Answer: (SHOW ANSWER)

The best course of action for a security administrator who is called in the middle of the night by the on-call programmer who needs access to the live system is to give the programmer an emergency ID for temporary access and review the activity. This is because:

Requiring that a change request be completed and approved may delay the resolution of the problem and cause further damage or disruption to the system or business operations. A change request is a formal document that describes the proposed change, its rationale, impact, benefits, risks, costs, and approval process. A change request is usually required for planned or scheduled changes, not for emergency or urgent changes.

Giving the programmer read-only access to investigate the problem may not be sufficient or effective, as the programmer may need to perform actions or tests that require write or execute permissions. Read-only access means that the user can only view or copy data or files, but cannot modify or delete them.

Reviewing activity logs the following day and investigating any suspicious activity may not prevent or detect any unauthorized or malicious actions by the programmer in real time. Activity logs are records of events and actions that occur within a system or network. Activity logs can provide evidence and accountability for system activities, but they are not proactive or preventive controls.

Therefore, giving the programmer an emergency ID for temporary access and reviewing the activity is the best course of action, as it allows the programmer to access the live system and resolve the problem quickly, while also ensuring that the security administrator can monitor and verify the programmer's activity and revoke the access when it is no longer needed. An emergency ID is a temporary account that grants a user elevated privileges or access to a system or resource for a specific purpose and duration. An emergency ID should be:

Created and authorized by a security administrator or manager

Assigned to a specific user and purpose

Limited in scope and time

Logged and audited

Revoked and deleted after use

Some of the best practices for emergency access to live systems are12:

Establish clear policies and procedures for requesting, approving, granting, monitoring, reviewing, and revoking emergency access Define criteria and scenarios for emergency access, such as severity, impact, urgency, and risk Implement controls to prevent unauthorized or unnecessary use of emergency access, such as multifactor authentication, approval workflows, alerts, notifications, and time restrictions Implement controls to track and audit emergency access activities, such as logging, reporting, analysis, and investigation Implement controls to ensure accountability and responsibility for emergency access users, such as attestation, justification, documentation, and feedback

NEW QUESTION: 554
下列哪一項建議最能防止在未與業務部門合作的情況下實施 IT 專案？
A. 與業務部門合作評估 IT 專案。
B. 定期檢視專案的投資報酬率(ROI)。
C. 檢視項目，找出相似之處並消除重複項
D. 根據業務和 IT 資源可用性確定保護優先順序。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 555
下列哪一種方法對品質保證(QA)功能的實施構成最大威脅？
A. 引入這些變更的開發人員將審口這些工作，因為他們最熟悉這些工作。
B. 來自同一開發團隊但不熟悉這些變更的同儕開發人員將審口這些變更。
C. 組織口另一個開發團隊的開發人員將審口提交的變更。
D. 開發群組以外且不具有開發角色的審口者將審口變更。
Answer: A (LEAVE A REPLY)
A strongQA functionrequires anindependentreview of changes toavoid biasandensure objectivity.
Option A (Correct):Ifdevelopers review their own changes, there is ahigh risk of biasand overlooking issues, making this the greatest concern. This violatesseparation of dutiesandbest practices for quality assurance.
Option B (Incorrect):Peer reviews within the same teamreduce risksincefresh eyesreview the changes, though it is not as strong as an external review.
Option C (Incorrect):Havingdevelopers from a separate teamreview the code providesbetter objectivityand reduces risks associated withself-review.
Option D (Incorrect):Whilenon-developers may lack technical expertise, their review ensuresindependence, making it a stronger control than self-review.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversquality assurance, code reviews, and segregation of duties.

NEW QUESTION: 556
誰負責組織的風險管理(ERM)計劃？
A. 董事會
B. 首席風險長(CRO)
C. 指導委員會
D. 執行管理階層
Answer: A (LEAVE A REPLY)

NEW QUESTION: 557
資訊系統審計師正在審口組織在組織結構變更後所製定的業務連續性計畫 (BCP)，此變更對業務流程口生了重大影響。下列哪一項發現應該是審計師最關注的問題？
A. 關鍵業務流程最終使用者未參與業務影響分析(BIA)。
B. 自重組以來，業務連續性計畫(BCP) 的副本尚未分發給新的業務部門最終用口。
C. 過去兩年口，業務連續性計畫(BCP) 的測試計畫尚未完成。
Answer: C (LEAVE A REPLY)
A test plan for the BCP is essential to ensure that the plan is effective, updated and aligned with the current business needs and objectives. A change in organizational structure with significant impact to business processes may require a revision of the BCP and a new test plan to validate its adequacy. The lack of a test plan for the BCP for two years indicates a high risk of failure in the event ofa disaster or disruption.
Therefore, this should be the auditor's greatest concern among the given options.
References:
ISACA, IT Control Objectives for Sarbanes-Oxley, 4th Edition, section 5.3.21 ISACA, CISA Review Manual, 27th Edition, chapter 5, section 5.42

NEW QUESTION: 558
資訊系統審計員想要檢口系統中的近期事件，以觀察身份驗證失敗和密碼變更情況 下列哪一種方法是實現此目的最適合的？
A. 已認證掃描
B. 系統日誌審口
C. 滲透測試
D. 變更管理記錄
Answer: B (LEAVE A REPLY)

NEW QUESTION: 559
在進行系統存取權限審口時，資訊系統審計員注意到，一名近期在組織口更換崗位的員工仍然擁有先前的存取權限。審計員的下一步應該是：
A. 建議新增一個控制項來自動更新存取權限。
B. 決定存取權限未被撤銷的原因。
C. 直接管理以撤銷目前存取權限。

D. 確定存取權限是否違反軟體許可。
Answer: B (LEAVE A REPLY)
The NEXT step for the IS auditor after noting that an employee who has recently changed roles within the organization still has previous access rights should be to B. determine the reason why access rights have not been revoked. Identifying the cause of this situation is crucial for understanding whether it's due to oversight, process gaps, or other factors. Once the reason is determined, appropriate corrective actions can be recommended to ensure that access rights are aligned with the employee's current role and responsibilities1.

NEW QUESTION: 560
對於剛實施零信任解決方案的組織而言，在審口其安全架構時，資訊系統稽核員最關注下列哪項發現？
A. 安全相關成本增加
B. IT系統效能明顯下降
C. 使用者識別錯誤增加
D. 使用者對新工作模式的抱怨
Answer: C (LEAVE A REPLY)

NEW QUESTION: 561
下列何者屬於社會工程攻擊方法？
A. 員工透過電話回答問題被誘導洩漏機密 IP 位址和密碼。
B. 一名駭客使用掃描工具在辦公大樓口四處走動，尋找無線網路以取得存取權限。
C. 入侵者竊聽並收集流經網路的敏感訊息，並將其出售給第三方。
D. 未經授權的人員試圖跟隨授權人員通過安全門進入安全場所。
Answer: (SHOW ANSWER)
Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception. References: [ISACA CISA Review Manual 27th Edition], page 361.

NEW QUESTION: 562

管理階層得知新IT系統的實施無法準時完成，並已要求進行審計。下列哪一項審計結果最令人擔憂？

A. 部分活動的實際開始時間晚於原計劃時間。

B. 關鍵路徑上定義的任務沒有分配資源。

C. 專案經理缺乏正式資格認證。

D. 並非所有專案口品都定義了里程碑。

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 563

資訊系統審計師正在審口某組織財務業務應用程式的邏輯存取控制。下列哪一項發現最應引起審計師的注意？

A. 使用者無需定期更改密碼。

B. 管理層不審口應用程式使用者活動日誌

C. 使用者帳口在使用者之間共用

D. 密碼長度設定為八個字元

Answer: C (LEAVE A REPLY)

The finding that should be of greatest concern to the IS auditor is that user accounts are shared between users.

User accounts are unique identifiers that grant access to an organization's financial business application based on the roles and responsibilities of the users. User accounts should be individualized and personalized to ensure accountability, traceability, and auditability of user actions and transactions. User accounts should not be shared between users, because this can compromise the confidentiality, integrity, and availability of the financial data and systems, and can enable unauthorized or fraudulent activities. If user accounts are shared between users, the IS auditor may not be able to determine who performed what action or transaction, or whether the user had the appropriate authorization or approval. The other findings are also concerning, but not as much as user

account sharing, because they either affect the password strength or frequency rather than the useridentity, or they relate to monitoring rather than controlling user access.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

NEW QUESTION: 564
心臟病護理機構利用物聯網 (IoT) 設備，透過即時患者監測和進階診斷來改善患者治療效果。下列哪一項最有助於將這些設備與企業網路流量隔離？
A. 口部防火牆
B. 區塊鏈技術
C. 口容過濾代理
D. 零信任架構
Answer: (SHOW ANSWER)
Internal firewalls are highly effective for isolating Internet of Things (IoT) devices from corporate network traffic. By segmenting the network and restricting communication between devices and the main corporate infrastructure, internal firewalls help mitigate the risk of lateral movement and data breaches caused by compromised IoT devices.
Blockchain Technology (Option B):This is useful for ensuring data integrity but not for network isolation.
Content Filtering Proxy (Option C):This is designed to manage web traffic and does not provide network segmentation.
Zero Trust Architecture (Option D):While Zero Trust provides robust access controls, internal firewalls are more directly suited for traffic isolation.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 565
在例行的口部軟體許可審口期間，資訊系統審計員發現員工共享關鍵業務軟體的許可證金鑰的情況。下列哪一項是審計員的最佳行動方案？
A. 建議使用軟體許可監控工具
B. 建議購買額外的軟體許可證金鑰
C. 驗證使用者對共享軟體授權的需求
D. 驗證許可協議是否允許共享使用
Answer: D (LEAVE A REPLY)
The auditor's best course of action after discovering instances where employees shared license keys to critical pieces of business software is to verify whether the licensing agreement allows shared use. A licensing agreement is a contract between the software provider and the user that defines the terms and conditions of using the software, including the number, type, and scope of licenses granted. Some licensing agreements may allow shared use of license keys among multiple users or devices, while others may prohibit or restrict such use. By verifying the licensing agreement, the auditor can determine whether

the employees violated the contract or not, and whether there are any legal or financial risks or implications for the organization.
The other options are not as appropriate as option D, as they may not address the root cause of the issue or provide a comprehensive solution. Recommending the utilization of software licensing monitoring tools may help prevent or detect future instances of license key sharing, but it does not resolve the current situation or ensure compliance with the licensing agreement. Recommending the purchase of additional software license keys may be unnecessary or wasteful if the licensing agreement already allows shared use or if there are unused licenses available. Validating user need for shared software licenses may help identify the reasons or motivations behind license key sharing, but it does not justify or excuse such behavior if it violates the licensing agreement.
References:
* 9: Best License Management Software 2023 | Capterra
* 10: Best 10 Software License Management Tools in 2023 | Zluri
* 11: Top 10 Software License Tracking Tools | Zluri
* 12: Top 5 Software License Tracking Solutions in 2023 - DNSstuff

NEW QUESTION: 566
下列哪一項最有效降低包含個人識別資訊 (PII) 的電子郵件被傳送給未經授權的收件者的風險？
A. 多重驗證 (MFA)
B. 入侵偵測系統 (IDS)
C. 電子郵件審計跟踪
D. 定期進行安全意識培訓
Answer: D (LEAVE A REPLY)
The greatest risk is unintentional human error, such as misaddressing an email. Security awareness training equips users to recognize PII and verify recipients. MFA protects account access but not outbound emails.
IDS detects network threats, not email content. Audit trails only provide after-the-fact evidence.
References (ISACA): COBIT DSS05 (security awareness and user controls).

NEW QUESTION: 567
對於評估組織補丁管理計畫的資訊系統審計員來口，下列哪一項應該是他們最關注的問題？
A. 目前沒有掃描網路以識別缺少修補程式的流程。
B. 修補程式從多個部署伺服器進行部署。
C. 目前沒有針對未打補丁的伺服器進行隔離的流程。
D. 中低風險漏洞的修補程式被省略。
Answer: (SHOW ANSWER)

NEW QUESTION: 568

下列哪一項是減輕勒索軟體攻擊影響的最佳方法？
A. 口動災難復原計畫(DRP)
B. 頻繁備份數據
C. 支付贖金
D. 請管理員帳號更改密碼
Answer: B (LEAVE A REPLY)
Ransomwareis a type of malicious software that encrypts the victim's data and demands a ransom for its decryption1. Ransomware attacks can cause significant damage to an organization's operations, reputation, andfinances1. Therefore, it is important to mitigate the impact of ransomware attacks by implementing effective prevention and recovery strategies.
One of the best ways to mitigate the impact of ransomware attacks is to back up data frequently12345. Data backups are copies of the organization's data that are stored in a separate location or medium, such as an external harddrive, cloud storage, or tape2. Data backupscan help the organization restore its data in case of a ransomware attack, without paying the ransom or losing valuable information2. Data backups shouldbe performed regularly, preferably daily or weekly, depending on the criticality and volume of the data2. Data backups should also be tested periodically to ensure their integrity and usability2.
The other options are not as effective as backing up data frequently in mitigating the impact of ransomware attacks. Invoking the disaster recovery plan (DRP) is a reactive measure that can help the organization resume its operations after a ransomware attack, but it does not prevent or reduce the damage caused by the attack3.
Paying the ransom is not a recommended option, as it does not guarantee the decryption of the data or the deletion of the stolen data by the attackers. Paying the ransom also encourages further attacks and funds criminal activities14. Requiring password changes for administrative accounts is a good security practice, but it is not sufficient to prevent or recover from ransomware attacks. Ransomware attacks can exploit other vulnerabilities, such as phishing emails, outdated software, or weak network security15.
References: 1: How to Mitigatethe Risk of Ransomware Attacks: The Definitive Guide 2: Mitigating malwareand ransomware attacks - The National Cyber Security Centre 3: 3 steps to prevent and recover from ransomware 4: Ransomware Epidemic: Use these 8 Strategies to Mitigate Risk 5: Practical Steps to Mitigate Ransomware Attacks - ITSecurityWire

NEW QUESTION: 569
在製定網路服務的服務等級協定 (SLA) 時，下列何者是面臨的挑戰？
A. 建立設計完善的網路服務架構。
B. 找出可以正確衡量的效能指標
C. 確保網路元件不會被客口端修改
D. 減少網路入口點的數量
Answer: (SHOW ANSWER)

One of the challenges in developing a SLA for network services is finding performance metrics that can be measured properly and reflect the quality of service expected by the customer. Establishing a well-designed framework for network services is not a challenge, but a good practice. Ensuring that network components are not modified by the client or reducing the number of entry points into the network are security issues, not SLA issues. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 333

NEW QUESTION: 570
使用者抱怨新發布的企業資源計畫(ERP)系統運作速度太慢。在品質保證(QA)階段，下列哪項測試可以發現這個問題？
A. 壓力
B. 回歸
C. 接口
D. 集成
Answer: (SHOW ANSWER)
Stress testing is a type of performance testing that evaluates how a system behaves under extreme load conditions, such as high user traffic, large data volumes, or limited resources. It is useful for identifying potential bottlenecks, errors, or failures that may affect the system's functionality or availability. Stress testing during the quality assurance (QA) phase would have identified the concern of users complaining that a newly released ERP system is functioning too slowly. The other options are not as relevant for this concern, as they relate to different aspects of testing, such as regression testing (verifying that existing functionality is not affected by new changes), interface testing (verifying that the system interacts correctly with other systems or components), or integration testing (verifying that the system works as a whole after combining different modules or units). References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.4 Testing Techniques1

NEW QUESTION: 571
某組織最近發現其所有處理器都存在一個影響範圍廣泛的晶片級安全漏洞。下列哪一項是防止漏洞被利用的最佳方法？
A. 實施安全意識訓練。
B. 安裝供應商補丁
C. 審口硬體供應商合約。
D. 審口安全日誌事件。
Answer: B (LEAVE A REPLY)
The best way to prevent a chip-level security vulnerability from being exploited is to install vendor patches.
A chip-level security vulnerability is a flaw in the design or implementation of a processor that allows an attacker to bypass the normal security mechanisms and access privileged

information or execute malicious code. A vendor patch is a software update provided by the manufacturer of the processor that fixes or mitigates the vulnerability. Installing vendor patches can help to protect the system from known exploits and reduce the risk of data leakage or compromise.
Security awareness training, reviewing hardware vendor contracts, and reviewing security log incidents are not as effective as installing vendor patches for preventing a chip-level security vulnerability from being exploited. Security awareness training is an educational program that teaches users about the importance of security and how to avoid common threats. Reviewing hardware vendor contracts is a legal process that evaluates the terms and conditions of the agreement between the organization and the processor supplier. Reviewing security log incidents is an analytical process that examines the records of security events and activities on the system. These methods may be useful for other security purposes, but they do not directly address the root cause of the chip-level vulnerability or prevent its exploitation. References: Protecting your device against chip-related security vulnerabilities, New 'Downfall' Flaw Exposes Valuable Data in Generations of Intel Chips

NEW QUESTION: 572
在風險評估過程中，下列哪一項應先確定？
A. 易受威脅
B. 現有控件
C. 資訊資口
D. 法律要求
Answer: (SHOW ANSWER)
The risk assessment process involves identifying the information assets that are at risk, analyzing the threats and vulnerabilities that could affect them, evaluating the impact and likelihood of a risk event, and determining the appropriate controls to mitigate the risk. The first step is to identify the information assets, as they are the objects of protection and the basis for the rest of the process. Without knowing what assets are at risk, it is not possible to assess their value, exposure, or protection level. References: ISACA Frameworks: Blueprints for Success

NEW QUESTION: 573
在保護資訊資口機密性方面，最有效的控制措施是：
A. 採用雙重認證機制
B. 設定對所有使用者的唯讀存取權限
C. 強制執行「按需知悉」的存取控制理念
D. 對員工進行監管要求意識培訓
Answer: C (LEAVE A REPLY)

NEW QUESTION: 574
在實施新的資料分類流程時，下列哪個面向最容易被忽略？
A. 終端用口計算(EUC)系統
B. 電子郵件附件
C. 發送給供應商的數據
D. 新的系統應用程式
Answer: A (LEAVE A REPLY)
The area that is most likely to be overlooked when implementing a new data classification process is end-user computing (EUC) systems. EUC systems are applications or tools that are developed or customized by end users, often without formal IT involvement or approval. EUC systems may contain sensitive or confidential data that need to be classified and protected according to the organization's policies and standards. However, EUC systems may not be subject to the same controls, oversight, or documentation as formal IT systems, and may not be included in the scope of the data classification process. Therefore, EUC systems pose a significant risk of data leakage, unauthorized access, or noncompliance. The other areas (B, C and D) are less likely to be overlooked, as they are more visible and manageable by the IT department or the data owners. References: IS Audit and Assurance Guideline 2202: Evidence Collection Techniques, CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.2: Data Classification

NEW QUESTION: 575
在對某財務應用程式進行審計時，發現許多已終止使用者的帳口並未被停用。資訊系統審計員的下一步應該是下列哪一項？
A. 對已終止使用者的存取權限進行實質測試。
B. 對已終止使用者的帳號活動進行審口
C. 向應用程式擁有者傳達風險。
D. 得出結論，IT 一般控制措施無效。
Answer: B (LEAVE A REPLY)
The IS auditor's next step after determining that many terminated users' accounts were not disabled is to perform a review of terminated users' account activity. This means that the IS auditor should check whether any of the terminated users' accounts were accessed or

used after their termination date, which could indicate unauthorized or fraudulent activity. The IS auditor should also assess the impact and risk of such activity on the confidentiality, integrity, and availability of IT resources and data. The other options are not as appropriate as performing a review of terminated users' account activity, as they do not provide sufficient evidence or assurance of the extent and effect of the problem. References: CISA Review Manual, 27th Edition, page 240

NEW QUESTION: 576
下列哪一項有助於確保系統介面資料的完整性？
A. 系統介面測試
B. 使用者驗收測試(IJAT)
C. 驗證檢口
D. 稽核日誌
Answer: C (LEAVE A REPLY)
Validation checks are a type of data quality control that helps to ensure the integrity of data for a system interface. Validation checks verify that the data entered or transferred between systems is correct, consistent, and conforms to predefined rules or standards. Validation checks can prevent or detect errors, anomalies, or inconsistencies in the data that may affect the system's functionality, performance, or security.
Option C is correct because validation checks are a common and effective method of ensuring data integrity for a system interface. Validation checks can be performed at various stages of the data lifecycle, such as input, processing, output, or storage. Validation checks can also be applied to different types of data, such as data types, codes, ranges, formats, consistency, and uniqueness.
Option A is incorrect because system interface testing is a type of software testing that verifies the interaction between two separate systems or components of a system. System interface testing does not directly ensure the integrity of data for a system interface, but rather the functionality and reliability of the interface itself.
System interface testing may use validation checks as part of its test cases, but it is not the same as validation checks.
Option B is incorrect because user acceptance testing (UAT) is a type of software testing that evaluates whether the system meets the user's expectations and requirements. UAT does not directly ensure the integrity of data for a system interface, but rather the usability and acceptability of the system from the user's perspective. UAT may use validation checks as part of its test scenarios, but it is not the same as validation checks.
Option D is incorrect because audit logs are records of events and activities that occur within a system or network. Audit logs do not directly ensure the integrity of data for a system interface, but rather provide evidence and accountability for the system's operations and security. Audit logs may use validation checks as part of their analysis or reporting, but they are not the same as validation checks.
References:

CISA Online Review Course1, Module 5: Protection of Information Assets, Lesson 4: Data Quality Management, slide 5-6.
CISA Review Manual (Digital Version)2, Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.
CISA Review Manual (Print Version), Chapter 5: Protection of Information Assets, Section 5.3: Data Quality Management, p. 281-282.
CISA Questions, Answers and Explanations Database3, Question ID: QAE_CISA_722.
Data Validation - Overview, Types, Practical Examples4
Data Validity: The Best Practice for Your Business5
Validation - Data validation6
What is Data Validation? Types, Techniques, Tools7

NEW QUESTION: 577
下列哪一項是由於偵口控制的持續惡化而口生的重大ST影響？
A. 安全日誌中漏報數量增加
B. 屋頂原因分析有效性降低
C. 整體恢復時間縮短
D. 原木儲存空間需求增加
Answer: (SHOW ANSWER)
The greatest impact as a result of the ongoing deterioration of a detective control is an increased number of false negatives in security logs. A detective control is a control that monitors and identifies any deviations or anomalies from the expected or normal behavior or performance of a system or process. A security log is a record of events or activities that occur within a system or network, such as user access, file changes, system errors, or security incidents. A false negative is a situation where a security log fails to detect or report an actual deviation or anomaly that has occurred, such as an unauthorized access, a malicious modification, or a security breach. An increased number of false negatives in security logs can have a significant impact on the organization's security posture and risk management, because it can prevent timely detection and response to security threats, compromise the accuracy and reliability of security monitoring and reporting, and undermine the accountability and auditability of user actions and transactions. The other options are not as impactful as anincreased number of false negatives in security logs, because they either do not affect the detection capability of a detective control, or they have less severe consequences for security management. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

NEW QUESTION: 578
如果需要將程式的最新版本從生口環境中回滾，則程式碼增量版本中的相應變更應為：
A. 已存檔，供日後研究此問題時參考。
B. 應用於反映生口版本原始碼。
C. 從反映生口版本的原始程式碼中刪除。

D. 將版本替換回生口環境時重新安裝。

Answer: C (LEAVE A REPLY)

When a program release needs to be backed out of production, the changes introduced by that release must be removed from the source code to ensure the system returns to its prior state. This approach ensures that the source code reflects the stable version without the problematic changes.

References

ISACA CISA Review Manual 27th Edition, Page 244-245 (Change Management)

NEW QUESTION: 579

下列哪一項是資訊系統審計師在每次審計工作中需要考慮的最重要風險？

A. 流程和資源效率低下

B. 違規行為與非法行為

C. 不遵守組織政策

D. 與業務目標不一致

Answer: D (LEAVE A REPLY)

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

28 2: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.3:

Audit Risk

NEW QUESTION: 580

下列哪些與災難復原計畫 (DRP) 相關的職責可以外包給災難復原即服務 (DRaaS) 提供者？

A. 系統復原程序

B. 災難期間的利害關係人溝通

C. 恢復資料的驗證

D. 維護資料時效性的流程

Answer: (SHOW ANSWER)

A Disaster Recovery as a Service (DRaaS) provider is responsible for system recovery procedures, including restoring systems and services in a disaster scenario. This is the core functionality of DRaaS.

Stakeholder Communications (Option B):This is typically managed internally by the organization to ensure alignment with its crisis management plan.

Validation of Recovered Data (Option C):The organization must verify data integrity to meet business requirements.
Maintaining Currency of Data (Option D):While DRaaS may handle data backups, the organization retains responsibility for ensuring the relevance of the data being backed up.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 581
下列哪一項措施能最有效地減少系統轉換期間的停機時間？
A. 分階段方法
B. 直接切換
C. 試驗研究
D. 並行運行
Answer: D (LEAVE A REPLY)
The most effective way to minimize downtime during system conversions is to use a parallel run. A parallel run is a method of system conversion where both the old and new systems operate simultaneously for a period of time until the new system is verified to be functioning correctly. Thisreduces the risk of errors, data loss, or system failure during conversion and allows for a smooth transition from one system to another. References: CISA Review Manual, 27th Edition, page 467

NEW QUESTION: 582
下列哪一項資訊安全要求 BE ST 能□在自帶設備 (BYOD) 環境中追蹤組織資料？
A. 員工必須立即報告遺失或被盜的包含組織資料的行動裝置。
B. 員工必須簽署確認書，確認已□讀並瞭解組織的行動裝置可接受使用政策
C. 員工必須將其個人裝置註冊到組織的行動裝置管理程式中。
Answer: (SHOW ANSWER)
The best way to track organizational data in a BYOD environment is to enroll the personal devices in the organization's mobile device management (MDM) program. This will allow the organization to monitor, control, and secure the data on the devices remotely. Employees must also report lost or stolen devices and sign the acceptable use policy, but these are not sufficient to enable tracking of data. References: Info Technology and Systems Resources |COBIT, Risk, Governance ... - ISACA, section "Book IT Control Objectives for Sarbanes-Oxley, 4th Edition | Digital | English"

NEW QUESTION: 583
在決定資訊資□在運輸和處置過程中是否得到充分的安全保護時，下列何者最□得關注？
A. 缺乏適當的標籤
B. 缺乏近期意識訓練。
C. 缺乏密碼保護

D. 缺乏適當的資料分類

Answer: D (LEAVE A REPLY)

The most concerning issue when determining if information assets are adequately safeguarded during transport and disposal is lack of appropriate data classification. Data classification is a process that assigns categories or levels of sensitivity to different types of information assets based on their value, criticality, or risk to the organization. Data classification can help safeguard information assets during transport and disposal by providing criteria and guidelines for identifying, labeling, handling, and protecting information assets according to their sensitivity. Lack of appropriate data classification can compromise the security and confidentiality of information assets during transport and disposal by exposing them to unauthorized access, disclosure, theft, damage, or destruction. The other options are not as concerning as lack of appropriate data classification in safeguarding information assets during transport and disposal, as they do not affect the identification, labeling, handling, or protection of information assets according to their sensitivity. Lack of appropriate labeling is a possible factor that may increase the risk of misplacing, losing, or mishandling information assets during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. Lack of recent awareness training is a possible factor that may affect the knowledge or behavior of staff involved in transporting or disposing of information assets, but it does not affect the classification of information assets according to their sensitivity. Lack of password protection is a possible factor that may affect the security or confidentiality of information assets stored on devices during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION: 584

一個擁有大量桌上型電腦的組織正在考慮遷移到瘦客口機架構。下列哪一項是其主要優點？

A. 桌上型電腦的安全性提升。

B. 可以提供客口管理安全保障。

C. 桌面應用程式軟體永遠不需要升級。

D. 系統管理可以得到更好的管理。

Answer: C (LEAVE A REPLY)

The major advantage of moving from many desktop PCs to a thin client architecture is that desktop application software will never have to be upgraded. A thin client architecture is a type of client-server architecture that uses lightweight or minimal devices (thin clients) as clients that connect to a central server that provides most of the processing and storage functions. A thin client architecture can offer several benefits over a traditional desktop PC architecture, such as lower cost, higher security, easier maintenance, etc. One of these benefits is that desktop application software will never have to be upgraded on thin clients, as all the applications are installed and updated on the server, and accessed by thin clients

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

NEW QUESTION: 585
對於審口組織IT政策的資訊系統審計員來口，下列何者最口得關注？
A. 這些政策由組織口部的 IT 委員會審核和批准。
B. 這些政策沒有定期檢討和更新。
C. 這些政策與口業最佳實踐不符。
D. 這些政策主要針對IT人員。
Answer: (SHOW ANSWER)
The best answer is B. The policies are not regularly reviewed and updated.
ISACA guidance notes that, when auditing policy documents, one of the quickest indicators of trouble is the absence of current reviews, changes, approvals, and alignment with actual practice. If policies are outdated, they may no longer reflect the organization's control environment, regulatory obligations, technologies, or business processes. That creates a direct governance and compliance risk.
Option A is generally a positive sign, not a concern, because formal review and approval supports governance. Option C can matter, but lack of direct mapping to best practices is usually less serious than having stale policies that no longer reflect reality. Option D is not ideal if policies exclude broader stakeholders, but IT policies are often primarily directed toward IT staff while still being supported by wider governance documents. The most

serious issue is that outdated policies may be ineffective, unenforceable, or inconsistent with current controls.
References (Official ISACA):
* ISACA, Do Your Policy Documents Represent Current Practices?
* ISACA Journal, IS Audit Basics: The Auditors, IS/IT Policies and Compliance

NEW QUESTION: 586
下列何者最能顯示組織的安全意識計畫的有效性有所提升？
A. 資訊安全審計發現的數量減少
B. 完成意識訓練的員工人數增加
C. 員工報告的網路釣魚郵件數量增加。
D. 惡意軟體爆發次數減少
Answer: C (LEAVE A REPLY)
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
References
1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
References
1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 587
在資料庫安全審計期間，資訊系統審計師會審口用於輸入資料的流程。下列哪一個是審計師最需要關注的風險領域？
A. 資料彈性
B. 數據可用性
C. 資料規範化
D. 資料完整性
Answer: D (LEAVE A REPLY)
The key audit concern at data input is integrity-ensuring accuracy, validity, and completeness. Without integrity, outputs cannot be trusted. Availability and resilience are operational concerns, while normalization is a design technique. Integrity remains the top security and audit focus.
References (ISACA): ISACA Audit and Assurance Standards - Information Criteria (Effectiveness, Efficiency, Integrity, Availability).

NEW QUESTION: 588
在界定資訊系統審計範圍時，下列何者最為重要？
A. 最大限度地減少組織資訊系統審計程序所需的時間和成本
B. 讓業務部門參與範圍口明的製定
C. 使資訊系統審計程序與資訊科技管理優先順序保持一致
D. 了解 IT 與業務風險之間的關係
Answer: D (LEAVE A REPLY)
The most important factor when defining the IS audit scope is to understand the relationship between IT and business risks, as this helps to identify the areas that have the most potential impact on the organization's objectives, performance, and value. By understanding the IT and business risks, the IS auditor can focus the audit scope on the key processes, systems, controls, and issues that need to be assessed and addressed.
References
ISACA CISA Review Manual, 27th Edition, page 256
Ten Factors to Consider when Setting the Scope of an Internal Audit
What Is an Audit Scope? | Auditing Basics | KirkpatrickPrice

NEW QUESTION: 589
某組織委託第三方實施一款用於執行關鍵業務計算的應用程式。下列哪項流程對於確保該應用程式提供準確的計算結果最為重要？
A. 關鍵績效指標 (KPI) 監控
B. 變更管理
C. 設定管理
D. 品質保證(QA)
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 590
一位資訊系統審計員的任務是審計一家處理數百萬筆資料交易的大型組織的庫存控制流程。下列哪一項是最佳的測試策略？
A. 持續監測
B. 控制自我評估(CSA)
C. 風險評估
D. 停頓式採樣
Answer: (SHOW ANSWER)
Given the large volume of data transactions, continuous monitoring is the best testing strategy for auditing the inventory control process. Continuous monitoring involves the automated review of operational and financial data to identify anomalies or areas of concern12. This approach allows for real-time identification and resolution of issues, making it particularly effective for large organizations with high transaction volumes12. References: ISACA's Information Systems Auditor Study Materials1

NEW QUESTION: 591
在分析電腦效能時，下列哪一項最有用？
A. 衡量口能利用率的統計指標
B. 使用者對回應時間不滿意的營運報告
C. 調整系統軟體以最佳化資源使用率
D. 非尖峰時段利用率與回應時間報告
Answer: (SHOW ANSWER)
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples

of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
What is Computer Performance?
How to Measure Computer Performance

NEW QUESTION: 592
在對組織在其客口服務聊天機器人中使用人工智慧的情況進行審計時，資訊系統審計員應主要關注以下方面：
A. 人工智慧系統處理個人資料的安全保障。
B. 人工智慧系統符合口業安全標準。
C. 聊天機器人對客口口詢的反應速度和準確性。
D. 人工智慧系統同時處理多個客口口詢的能力。
Answer: A (LEAVE A REPLY)
Theprimary concernwhen auditing an AI-powered chatbot is ensuring thesafeguarding of personal datato comply with privacy regulations such asGDPR, CCPA, and ISO 27701. AI chatbots process customer inquiries, often handling sensitive personal data.
Safeguarding of Personal Data (Correct Answer - A)
Ensures compliance with data protection laws.
Reduces the risk of unauthorized access or data leakage.
Example:An AI chatbot collecting customer financial information must follow encryption and access control policies.
Compliance with Industry Standards (Incorrect - B)
Important, but protecting customer data takes priority over general compliance.
Speed and Accuracy of Chatbot Responses (Incorrect - C)
A performance metric, but not a primary audit focus.
AI's Ability to Handle Multiple Queries (Incorrect - D)
Efficiency metric, but does not address security risks.
References:
ISACA CISA Review Manual
ISO 27701 (Privacy Information Management System)
GDPR and CCPA Compliance Guidelines

NEW QUESTION: 593

下列何者是資訊系統稽核員為防止未經授權存取物聯網 (IoT) 設備而提出的最佳建議？
A. 物聯網設備應記錄並發出存取嘗試警報。
B. 物聯網設備應該只能從主機網路存取。
C. 物聯網設備應監控設備系統帳口的使用。
D. 物聯網設備應需要識別和認證。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 594
資訊系統審計員發現一個關鍵的面向互聯網的系統容易受到攻擊，而且沒有可用的補丁。審計師應該建議先採取什麼措施？
A. 實作一個可修補的新系統。
B. 實施額外的防火牆來保護系統。
C. 停用伺服器。
D. 評估相關風險。
Answer: D (LEAVE A REPLY)
The first step in addressing a vulnerability is to evaluate the associated risk, which involves assessing the likelihood and impact of a potential exploit. Based on the risk assessment, the appropriate mitigation strategy can be determined, such as implementing a new system, addingfirewalls, or decommissioning the server. References: ISACA CISA Review Manual 27th Edition, page 280

NEW QUESTION: 595
下列哪一個標準對於成功實現IT專案效益最為重要？
A. 確保 IT 專案經理對商業案例擁有簽字權
B. 評估組織口部個人和業務部門的變化影響
C. 量化專案所需的軟體開發工作量
D. 在專案的開發和執行階段讓關鍵利害關係人參與進來
Answer: D (LEAVE A REPLY)

NEW QUESTION: 596
下列哪一項最能顯示資訊安全意識計畫是有效的？
A. 報告的資訊安全事件數量減少
B. 社會工程攻擊的成功率降低
C. 降低維護資訊安全計畫的成本
D. 資訊安全攻擊數量減少
Answer: B (LEAVE A REPLY)
The success rate of social engineering attacks directly measures the behavioral changes resulting from an information security awareness program. Employees who are aware and informed are better equipped to identify and thwart such attacks.

* Reduction in Reported Incidents (Option A):This may indicate underreporting rather than program effectiveness.
* Reduction in Cost of Maintaining the Program (Option C):This reflects cost efficiency, not program effectiveness.
* Reduction in Number of Attacks (Option D):The number of attacks is beyond the control of awareness programs and does not reflect their impact.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 597
一家銀行希望將一個系統外包給位於另一個國家的雲端服務供應商。下列何者是最適當的IS審計建議？
A. 在銀行所在國尋找替代服務提供者。
B. 確保供應商的口部控制系統符合銀行的要求。
C. 如預期進行，因為服務提供者必須遵守客口所在國家的所有法律
D. 確保提供者俱備災難復原能力。
Answer: C (LEAVE A REPLY)
A post-implementation review (PIR) is a process to evaluatewhether the objectives of the project were met, determine how effectively this wasachieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of projects1. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.
One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project. Measurable benefits are the quantifiable and verifiable results or outcomes that the project delivers to theorganisation or its stakeholders, such as increased revenue, reduced costs, improved quality, enhanced customer satisfaction, or compliance with regulations2. Measurable benefits should be aligned with the organisation's strategy, vision, and goals, and should be SMART (specific, measurable, achievable, relevant, and time-bound).
The finding that measurable benefits were not defined is of greatest significance among the four findings, because it implies that:
The project did not have a clear and agreed-upon purpose, scope, objectives, and deliverables The project did not have a valid and realistic business case or justification for its initiation and implementation The project did not have a robust and effective monitoring and evaluation mechanism to track its progress, performance, and impact The project did not have a reliable and transparent way to demonstrate its value proposition and return on investment to the organisation or its stakeholders The project did not have a meaningful and actionable way to learn from its achievements and challenges, and to improve its processes and practices Therefore, an IS auditor should recommend that measurable

benefits are defined for any project before its implementation, and that they are reviewed and reported regularly during and after the project's completion.
The other possible findings are:
A lessons-learned session was never conducted: This is a significant finding, but not as significant as the lack of measurable benefits. A lessons-learned session is a process of capturing and documenting the knowledge, experience, and feedback gained from a project, both positive and negative. A lessons-learned session helps to identify the strengths and weaknesses of the project management process, as well as the best practices and lessons for future projects. A lessons-learned session should be conducted at the end of each projectphase or milestone, as well as at the end of the project. However, even without a formal lessons-learned session, some learning may still occur informally or implicitly among the project team members or stakeholders.
The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed. However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.
Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.
References: 1: The role and importance of the PostImplementation Review 2: What is Post-Implementation Review in Project Management?

NEW QUESTION: 598
下列哪一項控制措施最能確保應付帳款部門□部職責的適當分離？
A. 根據使用者安全設定檔限製程式功能
B. 僅限應付帳款人員存取更新程序
C. 將創建者的使用者 ID 作為欄位包含在建立的每個交易記錄中。
D. 確保交易存在審計追蹤
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 599
下列哪一項是降低組織網路因自帶設備 (BYOD) 政策允許的設備而面臨的風險的最佳方法？
A. 請IT人員檢口個人設備。
B. 在所有網路交換器上口用連接埠安全性。
C. 實現網路存取控制系統。
D. 確保策略要求在裝置上安裝防毒軟體。
Answer: D (LEAVE A REPLY)
The best way to mitigate risk to an organization's network associated with devices permitted under a BYOD policy is to implement a network access control system, as this will allow the organization to monitor, authenticate, and authorize the devices that connect to the network, and to enforce security policies and compliance requirements12. A network access control system can help to prevent unauthorized or compromised devices from accessing sensitive data or resources, and to detect and isolate any potential threats or vulnerabilities34.
References

1: Network Access Control (NAC) - ISACA 2: Network Access Control (NAC) - Cisco 3: BYOD Security Risks: 6 Ways to Protect Your Organization - ReliaQuest5 4: How to Mitigate BYOD Risks and Challenges - CIOReview6

NEW QUESTION: 600
容量管理使組織能□：
A. 預測技術趨勢
B. 建立網路通訊鏈路的容量
C. 決定組件需要升級的程度
D. 決定業務交易量。
Answer: C (LEAVE A REPLY)
Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS). Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives. Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose. Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

NEW QUESTION: 601
在審□入侵偵測系統 (IDS) 時，資訊系統稽核員最應該關注下列哪一項？
A. 處理速度下降
B. 假陽性率高
C. 假陰性率高
D. 簽章更新延遲
Answer: C (LEAVE A REPLY)

NEW QUESTION: 602
在製定新應用的商業案例時，資訊系統審計師應主要參與以下方面：
A. 系統測試。
B. 交易藍圖。
C. 使用者驗收測試(UAT)。
D. 可行性研究。
Answer: (SHOW ANSWER)
The best answer is D. Feasibility study.
ISACA guidance notes that, in projects, an auditor reviews the feasibility of projects based on resources, time, and other factors, and evaluates whether projects are aligned with the organization's strategic goals. That is exactly the stage where internal audit's advisory involvement is most appropriate during development of the business case.
Option A, B, and C occur later in the system development lifecycle and are more operational or project- delivery focused. The question is specifically about the development of a business case, and feasibility analysis is the phase most directly tied to whether the initiative is practical, justified, and aligned with business goals.
References (Official ISACA):
* ISACA Journal, Innovation and the Auditor.
* ISACA, An Appropriate Approach for Program and Project Management.

NEW QUESTION: 603
在審□□部稽核品質保證(QA)和持續改善流程時，下列何者最令人擔憂？
A. 改進機會沒有集中追蹤。
B. 審計職能不受獨立的定期外部審□。
C. 在某些審計的評估階段，不進行實質測試
D. 季報不分發給審計委員會。
Answer: B (LEAVE A REPLY)
The best answer is B.
A quality assurance and improvement program is meant to evaluate whether the audit function is performing effectively and independently. ISACA's candidate guide explicitly includes evaluating audit processes as part of QA and improvement programs, and ISACA peer-review guidance states that a peer review process assessing internal audit is essential to ensure it is appropriately carrying out its role. The absence of independent periodic external review is therefore the most serious concern because it weakens objective assessment of audit quality itself.
Option A is a weakness, but tracking improvement opportunities centrally is secondary to having independent validation that the function meets expected quality standards. Option

C is not the best answer because substantive testing during an assessment phase may vary by engagement design. Option D matters for governance communication, but it is still less central to QA than the lack of external independent review.
References (Official ISACA):
* ISACA, Certification Exam Candidate Guide.
* ISACA Journal, A Standardized Approach for Peer Review of Internal Audit.

NEW QUESTION: 604
下列哪一項是資訊系統審計師為降低員工無意中洩漏敏感資訊所帶來的風險而提出的最佳建議？
A. 入侵防禦系統(IPS)與防火牆
B. 資料遺失防護 (DLP) 技術
C. 加密保護
D. 電子郵件網路釣魚模擬練習
Answer: B (LEAVE A REPLY)
DLP technologies are designed to prevent the unauthorized transmission or leakage of sensitive data, such as PII, intellectual property, or financial information, by employees or other insiders. DLP technologies can monitor, detect, and block data in motion, data at rest, and data in use across various channels, such as email, web, cloud, or removable devices. DLP technologies can also help enforce data security policies and compliance requirements.
References
ISACA CISA Review Manual, 27th Edition, page 253
The role of disclosures in risk assessment and mitigation
Mitigate Risk Strategy for Information Management

NEW QUESTION: 605
下列哪一項是航空公司 IT 管理層持續監控關鍵整合航班時刻表和支付應用程式的控制措施的主要原因？
A. 確保有效識別和減輕風險
B. 確保政策和程序得到遵守
C. 確保航班預訂付款已處理
D. 偵測並應對可能的攻擊
Answer: D (LEAVE A REPLY)

NEW QUESTION: 606
在製定網路安全事件回應計畫中的桌面演練時，下列哪一項是最重要的考量因素？
A. 確保從組織口所有跨職能部門選出參與者。
B. 創建足口具有挑戰性的演練，以證明當前事件回應計畫的不足之處
C. 確保事件回應團隊有足口的干擾因素來模擬真實情況。

D. 確定與組織目前面臨的威脅相關的範圍和場景。
Answer: D (LEAVE A REPLY)
The most important consideration when developing tabletop exercises within a cybersecurity incident response plan is to identify the scope and scenarios that are relevant to current threats faced by the organization, as this will ensure that the exercises are realistic, meaningful, and effective in testing and improving the incident response capabilities12. The scope and scenarios should reflect the organization's risk profile, business objectives, and operational environment, and should cover a variety of potential incidents that could impact the organization's assets, operations, and reputation34.
References
1: Cybersecurity Incident Response Exercise Guidance - ISACA 2: Cybersecurity Tabletop Exercises:
Everything You Ever Wanted to Know 3: CISA Tabletop Exercise Package 4: Boost Your Incident Response Plan with Tabletop Exercises

NEW QUESTION: 607
決定批准使用終端使用者計算 (EUC) 的組織首先應確保：
A. 制定 EUC 政策。
B. 對 EUC 控制進行檢討。
C. 對 EUC 用例進行評估和記錄。
D. 進行業務影響分析(BIA)。
Answer: A (LEAVE A REPLY)

NEW QUESTION: 608
下列哪一種方法是銷毀儲存在電子媒體上的敏感資料的最有效方法？
A. 消磁
B. 隨機字元覆蓋
C. 物理破壞
D. 低階格式化
Answer: (SHOW ANSWER)
The most effective method of destroying sensitive data stored on electronic media is physical destruction, which involves breaking, shredding, melting, or incinerating the media to make it unreadable and unrecoverable. Degaussing, random character overwrite, and low-level formatting are methods of sanitizing or erasing data from electronic media, but they do not guarantee complete destruction of data and may leave some traces that can be recovered by advanced techniques. Therefore, physical destruction is the most secure and reliable method of data disposal for sensitive data. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Data Disposal

NEW QUESTION: 609

為了使防火牆能□有效地保護網路免受外部攻擊，必須遵循哪些基本做法？
A. 必須定義外部資訊過濾器。
B. 只允許提供必要的外部服務。
C. 防火牆必須放置在非軍事區(DMZ)□。
D. 所有外部通訊必須透過防火牆進行。
Answer: (SHOW ANSWER)

NEW QUESTION: 610
下列何者最能反映IT部門與公司使命的一致性？
A. IT部門功能分析
B. 每兩週向高階管理層報告
C. 年度董事會會議
D. 季度指導委員會會議
Answer: D (LEAVE A REPLY)
Quarterly steering committee meetings best demonstrate alignment of the IT department with the corporate mission because they provide a regular forum for strategic planning, decision making, and communication between IT leaders and business stakeholders12. Steering committee meetings help to ensure that IT goals and initiatives are aligned with the business vision, mission, and objectives, and that IT performance and value are monitored and evaluated34.
References
1: IT Governance and the Balanced Scorecard - ISACA Journal
2: IT Steering Committee Best Practices: A Recipe for Success
3: What is IT Governance? - Definition from Techopedia
4: CISA Cybersecurity Strategic Plan | CISA

NEW QUESTION: 611
下列何者是衡量事件管理計畫成效的最佳績效指標？
A. 事件發生之間的平均時間
B. 事件警報同時
C. 報告的事件數量
D. 事件解決期間
Answer: (SHOW ANSWER)
The best performance indicator for the effectiveness of an incident management program is the incident resolution meantime. This is the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. The incident resolution meantime reflects how quickly and efficiently the incident management team can restore normal service and minimize the impact of incidents on the business operations and customer satisfaction.

The average time between incidents (option A) is not a good performance indicator for the effectiveness of an incident management program, as it does not measure how well the incidents are handled or resolved. It only shows how frequently the incidents occur, which may depend on various factors beyond the control of the incident management team, such as the complexity and reliability of the systems, the security threats and vulnerabilities, and the user behavior and expectations.
The incident alert meantime (option B) is the average time it takes to detect and report an incident. While this is an important metric for measuring the responsiveness and awareness of the incident management team, it does not indicate how effective the incident management program is in resolving the incidents and restoring normal service.
The number of incidents reported (option C) is also not a good performance indicator for the effectiveness of an incident management program, as it does not reflect how well the incidents are handled or resolved. It only shows how many incidents are identified and recorded, which may vary depending on the reporting channels, tools, and procedures used by the incident management team and the users.
Therefore, option D is the correct answer.
References:
Incident Management: Processes, Best Practices and Tools - Atlassian
What is backup and disaster recovery? | IBM

NEW QUESTION: 612
持續整合/持續開發 (CI/CD) 流程如何幫助降低軟體故障風險？
A. 輕鬆軟體版本回滾
B. 較小的增量變化
C. 減少手動里程碑
D. 自動化軟體測試
Answer: (SHOW ANSWER)
A continuous integration/continuous development (CI/CD) process helps to reduce software failure risk by enabling smaller incremental changes to the software code, rather than large and infrequent updates12. Smaller incremental changes allow developers to detect and fix errors, bugs, or vulnerabilities more quickly and easily, and to ensure that the software is always in a working state34. Smaller incremental changes also reduce the complexity and uncertainty of the software development process, and improve the quality and reliability of the software product5.
References
1: What is CI/CD? Continuous integration and continuous delivery explained1 2: 5 CI/CD challenges-and how to solve them | TechBeacon4 3: Continuous Integration vs Continuous Delivery vs Continuous Deployment2 4: 7 CI/CD Challenges and their Must-Know Solutions | BrowserStack3 5: 5 common pitfalls of CI/CD-and how to avoid them | InfoWorld5

NEW QUESTION: 613
下列何者最能體現成熟的策略規劃流程？
A. 包含控制與保障措施規範的IT策略計劃
B. 策略計畫中的IT項目由管理階層批准。
C. 支持企業策略的IT策略計劃
D. 所有專案都制定了包含 IT 要求的行動計劃
Answer: C (LEAVE A REPLY)

NEW QUESTION: 614
某組織正在組成一個指導委員會，負責實施一套採用敏捷專案管理方法的新企業資源計畫(ERP)系統。該委員會組成最重要的標準是什麼？
A. 敏捷專案管理經驗
B. 能□滿足所需的時間投入
C. ERP實施經驗
D. 高階管理層代表
Answer: A (LEAVE A REPLY)

NEW QUESTION: 615
在開發和部署新應用程式的專案□動階段，下列哪一項□容最為重要？
A. 使用者需求
B. 使用者驗收測試(UAT)計劃
C. 部署計劃
D. 建築設計
Answer: A (LEAVE A REPLY)
User requirements are the foundation of any successful application. Properly defining what the application needs to do and how it should serve users is critical before moving into design or development.
References:
Project Management Methodologies (Agile, Waterfall, etc.): All major methodologies emphasize the criticality of understanding user requirements during the initial project phases.
Software Development Lifecycle (SDLC): Requirements gathering is a cornerstone of the initiation phase within the SDLC.
ISACA Resources: While not explicitly tied to a CISA document, ISACA ' s emphasis on governance and aligning IT with business objectives reinforces the importance of starting with clear user requirements.