ISACA.CISM-CN.v2026-05-06.q439

Exam Code:	CISM-CN
Exam Name:	Certified Information Security Manager (CISM中文版)
Certification Provider:	ISACA
Free Question Number:	439
Version:	v2026-05-06
# of views:	102
# of Questions views:	4437
https://www.freecram.net/torrent/ISACA.CISM-CN.v2026-05-06.q439.html	

NEW QUESTION: 1
下列哪一項是資訊安全意識培訓計畫的主要好處？
A. 影響人類行為
B. 評估組織安全文化
C. 定義風險責任
D. 執行安全性策略
Answer: (SHOW ANSWER)
Influencing human behavior is the primary benefit of an information security awareness training program because it helps to reduce the human errors and vulnerabilities that can compromise the security of data and systems. An information security awareness training program is a process or a program that informs and empowers users to protect data and computing assets from security risks and cyberattacks. It includes educational offerings that cover regulatory requirements, compliance policies, and safe computing practices.
An information security awareness training program helps to influence human behavior by raising awareness of the security threats and challenges, enhancing knowledge and skills of the security best practices and controls, and fostering a positive security culture and attitude among the users. By influencing human behavior, an information security awareness training program can improve the security posture and performance of the organization, as well as prevent or mitigate the impact of security incidents. Therefore, influencing human behavior is the correct answer.
References:
* https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and-training/
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs
* https://threatcop.com/blog/benefits-and-purpose-of-security-awareness-training/.

NEW QUESTION: 2

在批准實施新的安全解決方案之前，高階管理層需要一個業務案例。下列哪一項最能支持投資的理由？

A. 此解決方案有助於制定業務策略。

B. 此解決方案提高了業務風險承受能力。

C. 此解決方案提高了業務彈性。

D. 此解決方案降低了不遵守法規的成本。

Answer: (SHOW ANSWER)

The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.

References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 3

對最近發生的安全事件的調口確定，根本原因是系統准入管理員為解決此問題而疏忽處理事件警報？

A. 進行風險評估並與高階管理層分享結果。

B. 修改事件回應計劃，以與業務流程保持一致

C. 為資料保管人提供事件回應訓練。

D. 提供資料擁有者事件回應訓練。

Answer: (SHOW ANSWER)

The best action for the system admin manager to address the issue of negligent handling of incident alerts by system admins is to provide incident response training to data custodians because it helps to improve their awareness and skills in recognizing and reporting security incidents, and following the incident response procedures and protocols. Conducting a risk assessment and sharing the result with senior management is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Revising the incident response plan to align with business processes is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Providing incident response training to data owners is not a good action because data owners are not responsible for handling incident alerts or performing incident response tasks. References: https://www.isaca.org/resources

/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca- journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 4
一家金融機構正計劃開發一款新的行動應用程式。下列哪一個是開始評估應用程式安全合規性的最佳時機？
A. 在設計階段
B. 靜態程式碼分析期間
C. 監管審口期間
D. 使用者驗收測試 (UAT) 期間
Answer: (SHOW ANSWER)

NEW QUESTION: 5
下列哪一種工具對事件回應團隊最有幫助？
A. 入侵偵測系統 (IDS)
B. 端點偵測與回應 (EDR) 解決方案
C. 使用者與實體行為分析
D. 漏洞掃描工具
Answer: (SHOW ANSWER)
An endpoint detection and response (EDR) solution provides advanced visibility, detection, and response capabilities at the endpoint level, which are critical for investigating and responding to incidents.
"EDR solutions help identify, investigate, and respond to threats on endpoints quickly, making them vital for incident response teams."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Tools and Technologies for Incident Response* ISACA's practice questions highlight EDR as the most helpful tool for comprehensive incident analysis and response.

NEW QUESTION: 6
一名遠端員工使用虛擬私人網路 (VPN) 連線將財務資料從公司伺服器複製到筆記型電腦。下列哪一項是決定該事件是否應歸類為資料外洩事件的最重要因素？
A. 資料所有權
B. 員工的職位
C. 有效用例
D. 審口稽核日誌
Answer: (SHOW ANSWER)

NEW QUESTION: 7
下列哪一項對資訊安全政策的製定影響最大？
A. 商業策略

B. 過去與現在的威脅
C. IT 安全框架
D. 業界標準
Answer: A (LEAVE A REPLY)
Business strategy is the overarching driver for any organizational initiative, including security. Information security policies must align with the strategic goals of the organization to ensure relevance, support, and effectiveness.
Security policies that do not consider the business context may hinder operations or fail to protect key objectives. Business-driven policies are more likely to gain executive support and compliance from stakeholders, creating a strong foundation for governance.
"Information security policies must be aligned with business goals and objectives to ensure that they support the overall mission and are embraced by stakeholders."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Strategy Alignment*

NEW QUESTION: 8
下列何者最能確保及時、可靠地存取服務？
A. 不可否認性
B. 真實性
C. 可用性
D. 復原時間目標 (RTO)
Answer: (SHOW ANSWER)
= According to the CISM Review Manual, availability is the degree to which information and systems are accessible to authorized users in a timely and reliable manner1. Availability ensures that services are delivered to the users as expected and agreed upon. Nonrepudiation is the ability to prove the occurrence of a claimed event or action and its originating entities1. It ensures that the parties involved in a transaction cannot deny their involvement. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication1. It ensures that the identity of a subject or resource is valid. Recovery time objective (RTO) is the maximum acceptable period of time that can elapse before the unavailability of a business function severely impacts the organization1. It is a metric used to measure the recovery capability of a system or service, not a factor that ensures timely and reliable access to services. References = CISM Review Manual, 16th Edition, Chapter 2, Information Risk Management, pages 66-67.

NEW QUESTION: 9
定義安全基線時，最重要的是基線：
A. 可能因係統的安全分類而異。
B. 對於同一類型的所有資口都是統一的。
C. 基於利害關係人的共識而製定。
D. 與關鍵風險指標 (KRI) 一致。

Answer: (SHOW ANSWER)
A security baseline is a set of minimum security requirements for a system or asset type. The CISM Review Manual states that a baseline should be uniform for all assets of the same type to ensure consistency, enforceability, and ease of monitoring. This standardization supports effective compliance and security operations. While other factors can influence baseline adjustments, uniformity for similar asset types is most critical.
Reference:ISACA CISM Review Manual, 16th Edition, Page 207, "Establishing Security Baselines".

NEW QUESTION: 10
供應鏈攻擊最有可能出現下列哪一種風險情境？
A. 透過第三方資源損害關鍵資□
B. 供應商提供的服務不可用
C. 因□品缺貨而失去客□
D. 供應商提供的硬體和軟體資源不可靠
Answer: (SHOW ANSWER)
= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page 189 1; CISM Practice Quiz 2

NEW QUESTION: 11
下列哪一項是在整個組織□傳達資訊安全責任的最有效方法？
A. 實施安全意識計劃
B. 在職位□明中記錄資訊安全職責
C. 制定技能矩陣
D. 在安全性策略中定義資訊安全責任
Answer: (SHOW ANSWER)

Documenting information security responsibilities within job descriptions is the most effective way to convey information security responsibilities across an organization because it clearly defines the roles, expectations, and accountabilities of each employee regarding information security. It also helps to align the information security objectives with the business goals and performance indicators, and to ensure compliance with the security policies and standards.
References = CISM Review Manual 15th Edition, What is CISM? - Digital Guardian

NEW QUESTION: 12
資訊安全經理最近收到與第三方服務提供者相關的潛在安全風險的通知。接下來該做什麼來解決這個問題？
A. 上報給首席風險長 (CRO)。
B. 進行漏洞分析。
C. 進行風險分析。
D. 確定補償控制。
Answer: C (LEAVE A REPLY)
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third- party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION: 13
安全審口發現文件伺服器上的機密資訊已被組織口未經授權的使用者存取。資訊安全經理應該先執行下列哪一項操作？
A. 呼叫事件回應計劃
B. 實現基於角色的存取控制（RBAC）
C. 刪除對資訊的存取權限
D. 從檔案伺服器中刪除訊息
Answer: (SHOW ANSWER)
The first step is to invoke the incident response plan to ensure a systematic, controlled, and compliant response to the security incident.
"The incident response plan should be activated immediately to investigate, contain, and resolve incidents of unauthorized access."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Execution* ISACA practice questions also reinforce that invoking the incident response plan is the essential first response to contain the breach.

NEW QUESTION: 14
某組織使用的雲端應用程式被發現有嚴重漏洞。評估風險後，下列哪一項是資訊安全經理的最佳行動方案？

A. 指示供應商進行滲透測試。
B. 暫停與防火牆中應用程式的連接
C. 向應用程式的業務所有者報告情況。
D. 口動組織的事件回應流程。
Answer: (SHOW ANSWER)
= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability.
The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application.
Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action.
Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application.
Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual
2023, page 211 1; CISM Practice Quiz 2

NEW QUESTION: 15
一個組織收購了國外的公司，以在新市場中獲得優勢。下列哪一項是資安經理應該採取的第一步？
A. 決定將使用哪個國家/地區的資訊安全法規。
B. 合併兩個現有的資訊安全程序。
C. 將現有的資訊安全計畫應用於被收購的公司。
D. 評估適用於被收購公司的資訊安全法。
Answer: (SHOW ANSWER)
The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and

challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

NEW QUESTION: 16
下列哪些因素會對組織的資訊安全治理模式口生最顯著的影響？
A. 外包流程
B. 安全預算
C. 員工人數
D. 企業文化
Answer: (SHOW ANSWER)
The corporate culture of an organization is the set of values, beliefs, norms, and behaviors that shape how the organization operates and interacts with its stakeholders. The corporate culture can have a significant impact on an organization's information security governance mode, which is the way the organization establishes, implements, monitors, and evaluates its information security policies, standards, and objectives. A strong information security governance mode requires a supportive corporate culture that fosters a shared vision, commitment, and accountability for information security among all levels of the organization. A supportive corporate culture can also help to overcome resistance to change, promote collaboration and communication, encourage innovation and learning, and enhance trust and confidence in information security12. References = CISM Review Manual (Digital Version), Chapter 1: Information Security Governance CISM Review Manual (Print Version), Chapter 1: Information Security Governance

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
在向高階主管介紹資訊安全計畫的當前狀態時，下列哪一項是最重要的考量因素？
A. 包含態勢預測
B. 使用適合目標受眾的語言
C. 包含指標趨勢圖
D. 使用評級系統來證明計劃的有效性

Answer: (SHOW ANSWER)

= When briefing executives about the current state of the information security program, the most important consideration is to use appropriate language for the target audience. This means avoiding technical jargon, acronyms, and details that may confuse or bore the executives, and instead focusing on the business value, risks, and benefits of the information security program. The other options are not as important or relevant as using appropriate language, although they may also be useful to include in the briefing. For example, a situational forecast may be helpful to show the future trends and challenges, but it is not as essential as communicating the current state clearly and concisely. Similarly, trend charts for metrics and a rating system to demonstrate program effectiveness may be useful to support the briefing, but they are not as critical as using language that the executives can understand and relate to. References = Information Security Guide for Government Executives, page 7: "Reminding employees of their responsibilities and demonstrating management's commitment to the security program are key to maintaining effective security within the constantly changing information security environment." Information security guide for government executives - NIST, page 3: "The executive should communicate the importance of information security to the organization and its staff, using language that is meaningful to the target audience." Information Security Committee Charter - SecurityStudio, page 1: "The committee also coordinates and communicates the direction, current state, and oversight of the information security program."

NEW QUESTION: 18

下列哪一項是保護高價口資口或處理信任問題的環境的最佳縱深防禦實施？

A. 劃分

B. 重疊冗餘

C. 持續監控

D. 多重身份驗證

Answer: (SHOW ANSWER)

Compartmentalization is the best defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns because it is a strategy that divides the network or system into smaller segments or compartments, each with its own security policies, controls, and access rules.

Compartmentalization helps to isolate and protect the most sensitive or critical data and functions from unauthorized or malicious access, as well as to limit the damage or impact of a breach or compromise.

Compartmentalization also helps to enforce the principle of least privilege, which grants users or processes only the minimum access rights they need to perform their tasks. Therefore, compartmentalization is the correct answer.

References:

* https://www.csoonline.com/article/3667476/defense-in-depth-explained-layering-tools-and-processes- for-better-security.html
* https://www.fortinet.com/resources/cyberglossary/defense-in-depth

* https://sciencepublishinggroup.com/journal/paperinfo?journalid=542&doi=10.11648/j.ajai.20190302.11

NEW QUESTION: 19
資訊安全事件事後檢討的主要目標是：
A. 更新風險狀況
B. 最小化影響
C. 防止再發生。
D. 確定影響
Answer: (SHOW ANSWER)
post-incident review of an information security incident is a process that aims to identify the root causes, contributing factors, and lessons learned from the incident, and to implement corrective and preventive actions to avoid or mitigate similar incidents in the future. The primary objective of a post-incident review is to prevent recurrence, as it helps to improve the security posture, awareness, and resilience of the organization. Preventing recurrence also helps to reduce the impact and cost of future incidents, as well as to enhance the reputation and trust of the organization. Updating the risk profile, minimizing impact, and determining the impact are not the primary objectives of a post-incident review, although they may be part of its outcomes or outputs.
References = CISM Review Manual, 16th Edition, page 1011

NEW QUESTION: 20
下列哪一種風險是風險轉移的例子？
A. 利用第三方應用程式
B. 將風險所有權轉移至另一個部門
C. 進行異地備份
D. 購買網路安全保險
Answer: (SHOW ANSWER)
Purchasing cybersecurity insurance is a textbook example of risk transfer - transferring financial risk to a third party (the insurer).
"Risk transfer shifts the impact of a risk to another party, such as through insurance or outsourcing."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*

NEW QUESTION: 21
電子郵件數位簽章將：
A. 保護電子郵件的機密性。
B. 向收件者驗證電子郵件的完整性。
C. 自動修正對電子郵件的未經授權的修改。
D. 防止對電子郵件進行未經授權的修改。
Answer: (SHOW ANSWER)

An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References: https://support.microsoft.com/en-us/office/secure- messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com /searchsecurity/definition/digital-signature

NEW QUESTION: 22
事件響應政策應包括：
A. 測試方法的描述。
B. 通知要求。
C. 基礎架構圖。
D. 復原時間目標 (RTO)。
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Incident response policies must provide clear and actionable steps to ensure effective handling of incidents.
Notification requirements are critical to ensure timely communication with stakeholders during an incident.
* A. A description of testing methodology: While testing is important, it is typically addressed in incident response plans, not the policy itself.
* B. Notification requirements: This is the BEST answer as it ensures that key stakeholders are informed promptly, allowing for coordination and mitigation efforts.
* C. An infrastructure diagram: This is useful for understanding system architecture but is not a core policy requirement.
* D. Recovery time objectives (RTOs): RTOs are part of business continuity and disaster recovery plans, not incident response policies.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) emphasizes the importance of clear communication and notification procedures in incident response.

NEW QUESTION: 23
某組織正在製定風險緩解計劃，考慮使用冗餘電源來降低與關鍵系統中斷相關的業務風險。正在考慮哪種類型的控制？
A. 預防性

B. 修正
C. 偵探
D. 威懾
Answer: (SHOW ANSWER)
A preventive control is a type of control that aims to prevent or reduce the occurrence or impact of potential adverse events that can affect the organization's objectives and performance. Preventive controls are proactive measures that are implemented before an incident happens, and they are designed to address the root causes or sources of risk. Preventive controls can also help the organization to comply with the relevant laws, regulations, standards, and best practices regarding information security1.
An example of a preventive control is a redundant power supply, which is a backup or alternative source of power that can be used in case of a power outage or failure. A redundant power supply can reduce the business risk associated with critical system outages, which can result from power disruptions caused by natural disasters, technical faults, human errors, or malicious attacks. A redundant power supply can provide the following benefits for information security2:
* Maintain the availability and continuity of the critical systems and services that depend on power, such as servers, databases, networks, or applications. A redundant power supply can ensure that the critical systems and services can operate normally or resume quickly after a power outage or failure, minimizing the downtime and data loss that can affect the organization's operations, customers, or reputation.
* Protect the integrity and reliability of the critical systems and data that are stored or processed by the power-dependent devices, such as computers, hard drives, or memory cards. A redundant power supply can prevent or reduce the damage or corruption of the critical systems and data that can be caused by sudden or unexpected power fluctuations, surges, or interruptions, which can compromise the accuracy, completeness, or consistency of the information.
* Enhance the resilience and redundancy of the power infrastructure and network that supports the critical systems and services. A redundant power supply can provide an alternative or backup route for power delivery and distribution, which can increase the flexibility and adaptability of the power infrastructure and network to cope with different scenarios or conditions of power supply or demand.
The other options are not the type of control that is being considered by the organization. A corrective control is a type of control that aims to restore or recover the normal state or function of the affected systems or processes after an incident has occurred. A corrective control is a reactive measure that is implemented during or after an incident, and it is designed to address the consequences or impacts of risk. A corrective control can also help the organization to learn from the incident and improve its information security practices1. An example of a corrective control is a backup or restore system, which is a method of creating and restoring copies of the system or data that have been lost or damaged due to an incident.
A detective control is a type of control that aims to identify or discover the occurrence or existence of an incident or a deviation from the expected or desired state or behavior of the systems or processes. A detective control is a monitoring or auditing measure that is implemented during or

after an incident, and it is designed to provide information or evidence of risk. A detective control can also help the organization to analyze or investigate the incident and determine the root cause or source of risk1. An example of a detective control is a log or alert system, which is a tool of recording or reporting the activities or events that have occurred or are occurring within the systems or processes.
A deterrent control is a type of control that aims to discourage or dissuade the potential perpetrators or sources of risk from initiating or continuing an incident or an attack. A deterrent control is a psychological or behavioral measure that is implemented before or during an incident, and it is designed to influence or manipulate the motivation or intention of risk. A deterrent control can also help the organization to reduce the likelihood or frequency of incidents or attacks1. An example of a deterrent control is a warning or notification system, which is a method of communicating or displaying the consequences or penalties of violating the information security policies or rules. References = Risk Control Techniques: Preventive, Corrective, Directive, And ..., Learn Different types of Security Controls in CISSP - Eduonix Blog

NEW QUESTION: 24
資訊安全經理被要求提供資訊安全計劃的一年和五年計劃。長期計劃的主要目的是什麼？
A. 促進 IT 組織的持續改進
B. 確保控制符合安全需求
C. 建立並記錄所需的 IT 能力
D. 比一年計畫更長期地優先考慮安全風險
Answer: (SHOW ANSWER)
The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.
The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3:
Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION: 25
一個組織計劃利用流行的社交網路平台來推廣其口品和服務。下列哪一項是資訊安全經理支持該計劃的最佳行動方案？
A. 建立在社群網路上發佈口容的流程。
B. 評估使用社群網路相關的安全風險。
C. 在社群網路平台上進行漏洞評估。
D. 發展社交網路使用的安全控制。
Answer: (SHOW ANSWER)
The best course of action for the information security manager to support the initiative of leveraging popular social network platforms to promote the organization's products and services is to assess the security risk associated with the use of social networks. Security risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a security risk assessment, the information security manager can provide valuable input to the decision-making process regarding the benefits and costs of using social networks, as well as the appropriate security controls and mitigation strategies to reduce the risk to an acceptable level. The other options are not the best course of action, although they may be part of the security risk management process. Establishing processes to publish content on social networks is an operational task that should be performed after assessing the security risk and implementing the necessary controls. Conducting vulnerability assessments on social network platforms is a technical activity that may not be feasible or effective, as the organization does not have control over the platforms' infrastructure and configuration. Developing security controls for the use of social networks is a preventive measure that should be based on the results of the security risk assessment and aligned with the organization's risk appetite and tolerance

NEW QUESTION: 26
在機密性、完整性和可用性 (CIA) 三元組中，下列哪項活動最能支援機密性概念？
A. 確保管理員憑證的雜湊口
B. 執行服務等級協定 (SLA)
C. 確保傳輸中的資料加密
D. 利用正式的變更管理流程
Answer: (SHOW ANSWER)
Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

NEW QUESTION: 27
組織聘請第三方供應商來監控和支援受監管機構嚴格審□的金融應用程式。下列哪項控制措施能□最有效管理組織的風險？
A. 實現系統與資料之間的職責分離
B. 在供應商合約中包含不合規的罰款條款
C. 監控關鍵風險指標 (KRI)
D. 停用供應商存取並僅在需要存取時重新□用
Answer: (SHOW ANSWER)

NEW QUESTION: 28
下列哪一項指標可以準確衡量資訊安全計畫的表現？
A. 從分配給安全計畫的各種措施中得出的單一數字分數
B. 支持決策的定性和定量趨勢的組合
C. 準確衡量安全異常的定性指標集合
D. 與□業基準進行比較的量化指標集合
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
下列哪一項是確保使用雲端服務提供者時資料不會混合或暴露的最佳方法？
A. 取得獨立審計報告。
B. 要求提供者遵循嚴格的資料分類程序。
C. 在合約中包含對安全漏洞的高額處罰。
D. □看提供者的資訊安全政策。
Answer: (SHOW ANSWER)
Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of

the enterprise." Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers. One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

NEW QUESTION: 30

在確定內部關鍵應用程式、資料庫或伺服器的復原時間目標 (RTO) 時，下列哪一項應該是最重要的考量？

Freecram.net

A. 恢復測試結果
B. 服務中斷的影響
C. 確定復原點目標 (RPO)
D. 高階管理層的指示
Answer: (SHOW ANSWER)

NEW QUESTION: 31

下列何者最能向董事會展示組織資訊安全計畫的狀態？
A. 資訊安全計畫指標
B. 最近的外部審核結果
C. 資訊安全營運矩陣
D. 資訊安全風險的變化
Answer: (SHOW ANSWER)

Information security program metrics are the best way to demonstrate the status of an organization's information security program to the board of directors, as they provide relevant and meaningful information on the performance, effectiveness, and value of the program, as well as the current and emerging risks and the corresponding mitigation strategies. Information security program metrics should be aligned with the business objectives and risk appetite of the organization, and should be presented in a clear and concise manner that enables the board of directors to make informed decisions and provide oversight. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32

在向高階主管報告資訊以獲得其對加強控制的支援時，下列何者最需要強調？
A. 殘餘風險暴露
B. 針對口部系統的威脅
C. 縱深防禦架構中的控制漏洞
D. 同一口業近期發生的資料外洩事件
Answer: (SHOW ANSWER)
Residual risk exposure (A) is the most important factor to emphasize because senior management is responsible for accepting or rejecting risk on behalf of the organization. CISM guidance stresses that executives are less concerned with technical details and more focused on what risk remains after controls are applied and whether it exceeds risk appetite. Threat details (B), architectural gaps (C), and industry breaches (D) can provide context, but they do not directly answer the key governance question: What level of risk does the organization still face? Presenting residual risk enables informed decision-making about whether additional controls are justified.
References: ISACA CISM Review Manual (Governance-risk reporting, executive decision-making); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 33
高階管理層剛剛接受了不遵守新法規的風險 資安經理應該做什麼 NEX*P
A. 向合規官報告決定
B. 更新風險登記冊中的詳細資料。
C. 重新評估組織的風險承受能力。
D. 評估法規的影響。
Answer: (SHOW ANSWER)
Updating details within the risk register is the next step for the information security manager to do after senior management has accepted the risk of noncompliance with a new regulation because it records and communicates the risk status, impact, and response strategy to the relevant stakeholders. Reporting the decision to the compliance officer is not the next step, but rather a possible subsequent step that involves informing and consulting with the compliance officer about the risk acceptance and its implications.
Reassessing the organization's risk tolerance is not the next step, but rather a possible subsequent step that involves reviewing and adjusting the organization's risk appetite and thresholds based on the risk acceptance and its implications. Assessing the impact of the regulation is not the next step, but rather a previous step that involves analyzing and evaluating the potential consequences and likelihood of noncompliance with the regulation. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure- the-effectiveness-of-information-security-using-iso-27004 https://www.isaca.org/resources/isaca-journal
/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

NEW QUESTION: 34
在製定事件回應計畫的升級程序時，要確保下列哪一項最重要？
A. 每個流程都分配給一個負責方。
B. 聯絡人清單定期更新。
C. 維持最低監理要求。
D. 高階管理層的批准已記錄在案。
Answer: (SHOW ANSWER)
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
* 1: Information Security Incident Response Escalation Guideline2, page 4
* 2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
* 3: Computer Security Incident Handling Guide4, page 18

NEW QUESTION: 35
下列哪一項對於確保適當的利害關係人在網路安全事件期間做出決策至關重要？
A. 利害關係人計劃
B. 升級計劃
C. 最新的風險登記冊
D. 資口分類
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
During a cybersecurity incident, it is vital to ensure that the right people are involved and that decision- making occurs promptly.
A). Stakeholder plan: While identifying stakeholders is important, it does not outline decision-making during an incident.
B). Escalation plan: This is the BEST answer because it specifies how incidents are escalated to the appropriate level of authority, ensuring timely and effective decisions.
C). Up-to-date risk register: Although useful for understanding risks, it does not facilitate decision-making in real-time incidents.
D). Asset classification: This helps identify critical assets but does not address decision-making protocols during an incident.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) highlights the importance of escalation procedures to manage incidents efficiently.

NEW QUESTION: 36

下列哪一項對成功執行災難復原計畫 (DRP) 的能力影響最大？
A. 進行該計劃的桌面演習
B. 定期更新計劃
C. 向所有利害關係人傳達計劃
D. 審口升級程序
Answer: (SHOW ANSWER)
The CISM Review Manual emphasizes that the success of a DRP (Disaster Recovery Plan) depends greatly on clear communication of the plan to all stakeholders. Stakeholders must be aware of their roles and responsibilities during an incident to ensure the plan can be effectively executed. While testing, updating, and reviewing the plan are also important, communication is critical to effective execution.
Reference:ISACA CISM Review Manual, 16th Edition, Page 250-251, "Disaster Recovery Planning - Key Success Factors".

NEW QUESTION: 37
某個組織遭遇了影響關鍵系統的大規模安全事件。決定在備用位置恢復系統後，應呼叫哪個計畫？
A. 事件回應計劃
B. 業務連續性計劃 (BCP)
C. 溝通計劃
D. 災難復原計畫 (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 38
下列哪位人士應被指定為與組織的新工資系統相關的新發現風險的所有者？
A. IT 部門主管
B. 資料隱私官
C. 人力資源主管 (HR)
D. 資訊安全經理
Answer: (SHOW ANSWER)

NEW QUESTION: 39
在定義控制目標時，下列哪一項是最重要的考量因素？
A. 業界最佳實踐
B. 資訊安全框架
C. 控制最近審核的建議
D. 組織的風險偏好
Answer: (SHOW ANSWER)
The organization's risk appetite is the most important factor to consider when defining control objectives, because it reflects the amount and type of risk that the organization is willing to accept or avoid in pursuit of its goals. Control objectives should align with the risk appetite and support the achievement of the organization's objectives. Industry best practices, an information security

framework, and control recommendations from a recent audit are also useful sources of guidance, but they are not as critical as the risk appetite.
References = CISM Review Manual, 16th Edition, page 75

NEW QUESTION: 40
下列哪一項最能幫助組織保留法律上可接受的證據?
A. 有關取證記錄保留的記錄流程
B. 健全的法律框架，附有法律行動口明
C. 帶有聯絡人的監管鍊表格
D. 法醫人員培訓，包括技術操作
Answer: (SHOW ANSWER)
Chain of custody forms with points of contact are the best way to enable an organization to maintain legally admissible evidence because they document the sequence of control, transfer, and analysis of the evidence, and every person who handled it, the dates and times, and the purpose for each action1. They also ensure the authenticity and integrity of the evidence, and prevent tampering or loss1. Documented processes around forensic records retention are not sufficient to maintain legally admissible evidence because they do not track or verify the handling of the evidence. Robust legal framework with notes of legal actions are not sufficient to maintain legally admissible evidence because they do not record or validate the preservation of the evidence. Forensic personnel training that includes technical actions are not sufficient to maintain legally admissible evidence because they do not account or certify the custody of the evidence.
References: 1 https://www.researchgate.net/publication/326079761_Digital_Chain_of_Custody

NEW QUESTION: 41
資安經理得知風險負責人已批准例外情況，以較弱的補償控制取代關鍵控制，以提高流程效率下列哪一項應該是最口得關注的？
A. 風險等級可能會超出可接受的限度。
B. 安全審核可能會報告更多高風險發現。
C. 補償控制可能不具成本效益。
D. 可能會導致不遵守口業最佳實務。
Answer: (SHOW ANSWER)
Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

NEW QUESTION: 42
某個組織正在經歷與網路釣魚訊息相關的事件急劇增加。根本原因是供應商不再支援過時的電子郵件過濾系統。下列哪一項應該是資訊安全經理的首要行動方案？
A. 加強最終使用者的安全意識實踐。
B. 暫時將電子郵件系統外包給雲端供應商。
C. 開發替換系統的業務案例。
D. 監控防火牆上的傳出流量。
Answer: (SHOW ANSWER)
Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics." Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages." Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

NEW QUESTION: 43
針對近期零時差攻擊數量激增所帶來的安全漏洞，最佳的因應方法是什麼？
A. 在公司範圍口實施 USB 連接埠控制。
B. 實施自動防毒更新。
C. 實現行為異常檢測解決方案。
D. 開發一個補丁程式。
Answer: (SHOW ANSWER)
Zero-day attacks exploit unknown vulnerabilities for which patches and signatures do not yet exist.
Therefore, behavior anomaly detection (C) is the most effective approach because it focuses on abnormal system behavior, not known attack patterns. USB controls (A) address a specific threat vector but do not broadly mitigate zero-day risks. Automated antivirus updates (B) and patching programs (D) are essential baseline controls, but they are reactive and ineffective against unknown exploits. CISM emphasizes a risk- based, layered defense strategy, where advanced detection capabilities are used to identify and respond to emerging threats that bypass traditional

controls. Behavior-based detection improves resilience against evolving and unknown attack techniques.
References: ISACA CISM Review Manual (Risk management-threat landscape, control selection, emerging risks); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 44
下列哪一項最能讓資訊安全經理獲得實施安全控制的組織支援？
A. 定期進行漏洞評估
B. 傳達業務影響分析 (BIA) 結果
C. 建立有效的利害關係人關係
D. 定義組織的風險管理框架
Answer: (SHOW ANSWER)
The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

NEW QUESTION: 45
在設計安全控制措施時，最重要的是：
A. 採用風險為本的方法

B. 對敏感資料應用技術控制
C. 考慮業務影響分析(BIA)結果
D. 重點在於預防性控制
Answer: (SHOW ANSWER)
A risk-based approach (A) is fundamental to control design in CISM. Controls must be proportionate to risk, aligned with business objectives, and consistent with risk appetite. Focusing solely on technical controls (B), BIA results (C), or preventive controls (D) limits effectiveness. A risk-based approach ensures balanced use of preventive, detective, and corrective controls. References: ISACA CISM Review Manual (Risk management-control selection); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 46
下列人員中，誰最適合評估業務影響？
A. 高階管理層
B. 資訊安全經理
C. IT 經理
D. 行程管理器
Answer: D (LEAVE A REPLY)
The process manager is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The process manager has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the process manager is in the best position to evaluate the business impacts of a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The process manager can identify and quantify the potential losses, damages, or consequences that could result from the disruption or incident, such as revenue loss, customer dissatisfaction, regulatory non-compliance, reputational harm, or legal liability. The process manager can also provide input and feedback to the information security manager and the senior management on the business continuity and disaster recovery plans, the risk assessment and treatment, and the security controls and measures that are needed to protect and recover the business processes and functions. References = CISM Review Manual 15th Edition, page 2301; CISM Practice Quiz, question 1302

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here:

https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 47
在減輕與新興技術相關的安全風險時，下列哪一項應該是主要關注領域？
A. 與舊系統的兼容性
B. 企業強化標準的應用
C. 與現有存取控制集成
D. 未知漏洞
Answer: (SHOW ANSWER)
= The primary area of focus when mitigating security risks associated with emerging technologies is unknown vulnerabilities. Emerging technologies are new and complex, and often involve multiple parties, interdependencies, and uncertainties. Therefore, they may have unknown vulnerabilities that could expose the organization to threats that are difficult to predict, detect, or prevent1. Unknown vulnerabilities could also result from the lack of experience, knowledge, or best practices in implementing, operating, or securing emerging technologies2. Unknown vulnerabilities could lead to serious consequences, such as data breaches, system failures, reputational damage, legal liabilities, or regulatory sanctions3. Therefore, it is important to focus on identifying, assessing, and addressing unknown vulnerabilities when mitigating security risks associated with emerging technologies.
The other options are not as important as unknown vulnerabilities, because they are either more predictable, manageable, or specific. Compatibility with legacy systems is a technical issue that could affect the performance, functionality, or reliability of emerging technologies, but it is not a security risk per se. It could be resolved by testing, upgrading, or replacing legacy systems4. Application of corporate hardening standards is a security measure that could reduce the attack surface and improve the resilience of emerging technologies, but it is not a sufficient or comprehensive solution. It could be limited by the availability, applicability, or effectiveness of the standards. Integration with existing access controls is a security requirement that could prevent unauthorized or inappropriate access to emerging technologies, but it is not a guarantee of security. It could be challenged by the complexity, diversity, or dynamism of the access scenarios.
References = 1: Performing Risk Assessments of Emerging Technologies - ISACA 2: Assessing the Risk of Emerging Technology - ISACA 3: Factors Influencing Public Risk Perception of Emerging Technologies: A ... 4: CISM Review Manual 15th Edition, Chapter 3, Section 3.3 : CISM Review Manual
15th Edition, Chapter 3, Section 3.4 : CISM Review Manual 15th Edition, Chapter 3, Section 3.5

NEW QUESTION: 48
ACISO 了解到，第三方服務提供者並未向該組織通報影響該服務提供者資料中心的資料外洩事件。CISO 應先執行下列哪項操作？
A. 建議取消外包合約。

B. 請求對提供者的資料中心進行獨立審□。
C. 通知受影響的客□資料外洩。
D. 決定對組織的影響程度。
Answer: (SHOW ANSWER)
The CISO should first determine the extent of the impact to the organization by assessing the nature and scope of the data breach, the type and sensitivity of the data involved, the potential harm to the organization and its customers, and the legal and contractual obligations of the organization and the service provider. This will help the CISO to prioritize the appropriate actions and resources to respond to the incident and mitigate the risks. The other options are possible actions that the CISO may take after determining the impact, depending on the circumstances and the outcomes of the investigation. References = CISM Review Manual 15th Edition, page 2231; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1030

NEW QUESTION: 49
當資訊安全經理向高階管理層提交安全風險狀況的變更時，下列哪一項是最重要的？
A. 誤報數
B. 安全訓練測試結果
C. □業基準
D. 現有控制項的效能量測
Answer: (SHOW ANSWER)

NEW QUESTION: 50
在事件回應計畫的哪個階段確定根本原因？
A. 恢復
B. 吸取的教訓
C. 遏制
D. 根除
Answer: (SHOW ANSWER)
The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 51
在建立安全風險意識文化時，向員工傳達下列哪一項訊息最重要？
A. 個人資訊與敏感資訊需要不同的安全控制。
B. 員工存取應基於最小權限原則。
C. 了解資訊資□的價□對於風險管理至關重要。
D. 所有員工都有安全責任。

Answer: (SHOW ANSWER)

= The most important message to convey to employees in building a security risk-aware culture is that the responsibility for security rests with all employees, not just the information security function or the management. A security risk-aware culture is a collective mindset of the people in the organization working every day to protect the enterprise and its information assets from internal and external threats. A security risk- aware culture requires the workforce to know the security risks and the processes for avoiding or mitigating them, and to make thoughtful decisions that align with security policies and standards. A security risk-aware culture also incorporates a broader corporate culture of day-to-day actions that encourage employees to report security incidents, share security best practices, and participate in security awareness and training programs.

A security risk-aware culture helps to reduce the human factor that causes 90 percent of all cyberattacks, and to offset the impact of corrupted or lost data, decreased revenue, regulatory fines, and reputational damage. A security risk-aware culture turns people from assets that must be protected into assets that actively contribute to the cybersecurity and risk management posture and elevate security to being a business enabler rather than a business impediment123.

Personal information requires different security controls than sensitive information is a true statement, but it is not the most important message to convey to employees in building a security risk-aware culture. Personal information is any information that can identify or relate to a natural person, such as name, address, email, phone number, social security number, etc. Sensitive information is any information that is confidential, proprietary, or has a high value or impact to the organization, such as trade secrets, financial data, customer data, intellectual property, etc. Different types of information may have different legal, regulatory, contractual, or ethical obligations to protect them from unauthorized access, use, disclosure, modification, or destruction. Therefore, different security controls may be applied to personal and sensitive information based on their classification, such as encryption, access control, retention, disposal, etc. However, this message does not address the broader concept of security risk-aware culture, which is not limited to information classification and protection, but also encompasses the behaviors, attitudes, and values of the employees towards security.

Employee access should be based on the principle of least privilege is a good practice, but it is not the most important message to convey to employees in building a security risk-aware culture. The principle of least privilege states that users should only have the minimum level of access and permissions that are necessary to perform their job functions, and no more. This principle helps to reduce the risk of unauthorized or inappropriate actions, such as data leakage, fraud, sabotage, etc., by limiting the exposure and impact of user activities. However, this message does not capture the essence of security risk-aware culture, which is not only about access control, but also about the awareness, understanding, and commitment of the employees to security.

Understanding an information asset's value is critical to risk management is a valid point, but it is not the most important message to convey to employees in building a security risk-aware culture. Understanding an information asset's value is essential to determine the potential impact and

likelihood of a security risk, and to prioritize the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
However, this message does not reflect the holistic nature of security risk-aware culture, which is not only about risk assessment, but also about risk communication, risk treatment, and risk monitoring. References = Building a Culture of Security - ISACA2 The Risk-Conscious, Security-Aware Culture: The Forgotten Critical Security Control - Cisco3 CISM ITEM DEVELOPMENT GUIDE - ISACA4

NEW QUESTION: 52
下列哪一項是量子計算技術對資訊安全構成的最大威脅？
A. 量子電腦可以破解幾種現有的資料保密加密方案。
B. 量子電腦可以實現安全通信，但這只有少數負擔得起的人才能從中受益
C. 量子電腦可以透過極快的速度處理大型資料集來降低可用性。
D. 量子電腦能口模擬超越傳統運算能力的複雜物理系統。
Answer: (SHOW ANSWER)
The greatest threat posed by quantum computing is its potential to break widely used cryptographic algorithms (A), particularly public-key encryption schemes that rely on mathematical problems vulnerable to quantum algorithms. This directly threatens data confidentiality and long-term data protection. The other options describe secondary or non-security impacts. CISM recognizes cryptographic resilience as a core component of risk management and emphasizes the need for organizations to monitor emerging technologies that could invalidate existing controls. Quantum computing's impact on encryption represents a systemic risk to trust, privacy, and secure communications.
References: ISACA CISM Review Manual (Risk management-emerging technologies and cryptographic risk); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 53
下列哪一項主要受業務影響分析 (BIA) 的影響？
A. IT 策略
B. 復原策略
C. 風險緩解策略
D. 安全策略
Answer: (SHOW ANSWER)

NEW QUESTION: 54
事件回應團隊屬於哪種類型的控制？
A. 預防
B. 指令
C. 偵探
D. 修正

Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
下列哪一項最能支持增加資訊安全預算的商業案例？
A. 成本效益分析結果
B. 與同儕組織的資訊安全預算比較
C. 業務影響分析 (BIA) 結果
D. 資訊安全事件發生頻率
Answer: (SHOW ANSWER)
Cost-benefit analysis results are the best way to support the business case for an increase in the information security budget because they help to demonstrate the value and return on investment of the proposed security initiatives or projects. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or options, taking into account both quantitative and qualitative factors. A cost-benefit analysis helps to justify the need and feasibility of the security budget, as well as to prioritize the security spending based on the expected outcomes and impacts. Therefore, cost-benefit analysis results are the correct answer.
References:
https://www.cisa.gov/resources-tools/resources/business-case-security
https://www.cisa.gov/resources-tools/resources/isc-best-practices-making-business-case-security
https://risk3sixty.com/2020/09/21/how-to-build-a-business-case-for-security-initiatives-part-4/

NEW QUESTION: 56
某個組織決定外包 IT 營運。下列哪一項應該是資安經理的主要關注點？
A. 安全要求包含在供應商合約中
B. 審核外部安全審核結果。
C. 服務等級協定 (SLA) 符合營運標準。
D. 提供業務連續性應急計劃
Answer: (SHOW ANSWER)
Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations
https://www.sciencedirect.com/science/article/pii/S0378720616302166

NEW QUESTION: 57
恢復時間目標 (RTO) 最好由以下因素決定：

A. 業務經理
B. 業務連續性官員
C. 執行管理階層
D. 資料庫管理員 (DBA)。
Answer: (SHOW ANSWER)
Business managers are best suited to determine the recovery time objectives (RTOs) for their business processes and functions, as they have the knowledge and authority to assess the impact of downtime and the acceptable level of service continuity. RTOs are the maximum acceptable time that a business process or function can be disrupted before it causes significant harm to the organization's objectives, reputation, or compliance. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.2.1.11

NEW QUESTION: 58
如果滿足以下條件，資訊安全治理框架的有效性將得到最好的增強：
A. 顧問檢視資訊安全治理架構。
B. 管理階層提倡遵守法律和法規的文化。
C. 風險管理融入營運和策略活動。
D. 資訊系統審計員有權評估治理活動
Answer: (SHOW ANSWER)
The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk management is a key component of information security governance, which is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2:
Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

NEW QUESTION: 59

一個事件回應團隊最近遇到了一類不常見的網路事件。雖然團隊最終解決了問題，但識別問題耗費了大量時間。有什麼最佳方法可以確保將來更快地識別類似事件？

A. 為團隊建立績效指標

B. 進行事後審口

C. 實施 SIEM 解決方案

D. 執行威脅分析

Answer: (SHOW ANSWER)

Performing a post-incident review (also known as a lessons-learned session) is the best way to ensure similar incidents are identified and addressed more efficiently in the future. This review helps in understanding what went wrong, what went right, and how processes can be improved. The knowledge gained from the review can be incorporated into incident response plans and training.

"Post-incident reviews help determine root causes, assess the effectiveness of the response, and identify opportunities for improvement."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis Additionally, the ISACA CISM Practice Question Database emphasizes that post-incident reviews are essential for improving future response times and understanding patterns of threats.

NEW QUESTION: 60

IT 專案已經超出預算，後製中增加了太多安全控制措施。下列哪一項最有助於確保相關控制措施應用於專案？

Freecram.net

A. 在專案管理的各個階段涉及資訊安全

B. 在專案業務案例分析期間確定職責

C. 建立資料分類框架並將其提供給利害關係人

D. 為利害關係人提供最低資訊安全要求

Answer: (SHOW ANSWER)

The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

NEW QUESTION: 61

一家組織成功回應了一起資訊安全事件。然而，資訊安全經理發現回應團隊並未採取事件管理程序中規定的某些步驟。資安經理的第一步應該是什麼？

A. 檢討事件管理程序。

B. 從事件管理程序中刪除這些步驟。
C. 為事件回應團隊提供額外訓練。
D. 採訪事件回應團隊。
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 62
為了幫助用口應用與資料隱私監管相關的適當控制措施，與用口溝通最重要的是什麼？
A. 資料保護口品的特點
B. 滲透測試結果
C. 資料預存程序
D. 資料分類策略
Answer: (SHOW ANSWER)

NEW QUESTION: 63
某個組織正在將其事件回應能力與公有雲服務提供者進行調整。資安經理的首要行動應該是什麼？
A. 決定提供者事件回應團隊的技能組合。
B. 評估提供者的審核日誌記錄和監控控制。
C. 口看提供者的事件定義和通知標準。
D. 更新事件升級流程。
Answer: (SHOW ANSWER)
When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. References = CISM Review Manual, 16th Edition, page 1021 Reviewing the provider's incident definitions and notification criteria is the

FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

NEW QUESTION: 64
在發展安全事件的分類方法時，類別必須：
A. 符合業界標準。
B. 由事件處理程序建立。
C. 具有約定的定義。
D. 符合報告要求。
Answer: (SHOW ANSWER)
When developing a categorization method for security incidents, the categories must have agreed-upon definitions. This means that the categories should be clear, consistent, and understandable for all the parties involved in the incident response process, such as the incident handlers, the stakeholders, the management, and the external authorities. Having agreed-upon definitions for the categories can help to ensure that the incidents are classified and reported accurately, that the appropriate actions and resources are allocated, and that the communication and coordination are effective. Aligning with industry standards, creating by the incident handler, and aligning with reporting requirements are not mandatory for developing a categorization method for security incidents, although they may be desirable or beneficial depending on the context and objectives of the organization. Aligning with industry standards can help to adopt best practices and benchmarks for incident response, but it may not be feasible or suitable for all types of incidents or organizations. Creating by the incident handler can allow for flexibility and customization of the categories, but it may also introduce inconsistency and ambiguity if the definitions are not shared or agreed upon by others. Aligning with reporting requirements can help to comply with legal or contractual obligations, but it may not cover all the aspects or dimensions of the incidents that need to be categorized. References = CISM Review Manual, 16th Edition, pages 200-2011; CISM Review Questions, Answers & Explanations Manual,
10th Edition, page 822
When developing a categorization method for security incidents, the categories MUST have agreed-upon definitions. This is because having clear and consistent definitions for each category of incidents will help to ensure a common understanding and communication among the incident response team and other stakeholders. It will also facilitate the accurate and timely identification, classification, reporting and analysis of incidents. Having agreed-upon definitions will also help to avoid confusion, ambiguity and inconsistency in the incident management process

NEW QUESTION: 65
實現對資訊安全治理計畫的執行承諾的最重要要素是：

A. 定義的安全框架。
B. 流程改善模型
C. 已建立的安全性策略。
D. 確定的業務驅動因素。
Answer: (SHOW ANSWER)
The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

NEW QUESTION: 66
正確分類資訊資口的主要原因是確定：
A. 資口受損時對業務的影響。
B. 根據需要了解的使用者存取等級。
C. 使用基於風險的方法適當的加密強度。
D. 依照敏感度進行適當的保護。
Answer: D (LEAVE A REPLY)

NEW QUESTION: 67
在決定是否接受剩餘風險時，下列哪一項是最重要的標準？
A. 更換資口的成本
B. 額外緩解措施的成本
C. 年預期損失 (ALE)
D. 年發生率
Answer: (SHOW ANSWER)
= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one-year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk

event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk event occurring within a one-year period, and SLE is the estimated cost of a single occurrence of a risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance. Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
22, page 242

NEW QUESTION: 68
下列哪一項最能幫助組織評估雲端服務的安全狀況？
A. 業界同儕評審
B. 服務提供者證明
C. 滲透測試報告
D. 第三方審計報告
Answer: (SHOW ANSWER)
Third-party audit reports (D) provide the most reliable evaluation of a cloud provider's security posture because they offer independent assurance of control design and effectiveness. Peer reviews (A) and attestations (B) are less objective, while penetration test reports (C) focus narrowly on technical vulnerabilities. CISM emphasizes independent assurance mechanisms when assessing third-party security, particularly for cloud services.
References: ISACA CISM Review Manual (Governance-third-party assurance and cloud risk); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 69
下列哪一項是降低與自帶設備 (BYOD) 計劃相關的風險的最佳方法？
A. 為員工提供安全行動裝置實務的培訓。
B. 實施行動裝置政策和標準。
C. 實施行動裝置管理 (MDM) 解決方案。
D. 要求員工安裝有效的反惡意軟體應用程式。
Answer: (SHOW ANSWER)

NEW QUESTION: 70
隨著對遠端存取安全性的需求不斷增加，組織發現有必要快速轉向在家工作模式。應立即關注下列哪一項？
Freecram.net
A. 轉向零信任存取模型
B. 口用網路層級身分驗證
C. 增強網路回應能力

D. 加強端點安全

Answer: (SHOW ANSWER)

Strengthening endpoint security is the most immediate focus when shifting to a work-from-home model with an increased need for remote access security, as this reduces the risk of unauthorized access, data leakage, malware infection, and other threats that may compromise the confidentiality, integrity, and availability of the organization's information assets. Moving to a zero trust access model, enabling network-level authentication, and enhancing cyber response capability are also important, but not as urgent as strengthening endpoint security, as they require more time, resources, and planning to implement effectively. References = CISM Review Manual 2023, page 1561; CISM Review Questions, Answers & Explanations Manual 2023, page 302; ISACA CISM - iSecPrep, page 153

NEW QUESTION: 71

下列哪一項最能證明反網路釣魚活動是有效的？

A. 提高員工參加意識會議的程度

B. 收到的網路釣魚電子郵件數量減少

C. 改進了反網路釣魚活動的回饋

D. 已發生的事件數量減少

Answer: (SHOW ANSWER)

The ultimate goal of an anti-phishing campaign is to reduce the risk and impact of phishing attacks on the organization. Therefore, the most relevant and reliable indicator of the effectiveness of an anti-phishing campaign is the decreased number of incidents that have occurred as a result of phishing. This metric shows how well the employees have learned to recognize and report phishing emails, and how well the security controls have prevented or mitigated the damage caused by phishing.

References = Five Ways to Achieve a Successful Anti-Phishing Campaign; Don't click: towards an effective anti-phishing training. A comparative literature review; CISA, NSA, FBI, MS-ISAC Publish Guide on Preventing Phishing Intrusions

NEW QUESTION: 72

下列哪一項指標最能證明組織安全意識計畫的有效性？

A. 定期參加安全訓練的員工百分比

B. 向服務台報告的安全事件數量

C. 最終使用者口看的網路釣魚電子郵件數量

D. 感染惡意軟體的員工電腦和裝置的百分比

Answer: (SHOW ANSWER)

NEW QUESTION: 73

持續監控安全控制的主要目的是確保：

A. 控制間隙最小化。

B. 系統可用性。

C. 控制的有效性。
D. 符合合規性要求。
Answer: C (LEAVE A REPLY)
The primary purpose for continuous monitoring of security controls is to ensure the effectiveness of controls.
This involves regularly assessing the controls to ensure that they are meeting their intended objectives, and that any potential weaknesses are identified and addressed. Continuous monitoring also helps to ensure that control gaps are minimized, and that systems are available and aligned with compliance requirements.
The primary purpose of continuous monitoring of security controls is to ensure that the controls are operating effectively and providing adequate protection for the information assets. Continuous monitoring can also help to identify control gaps, ensure system availability, and support compliance requirements, but these are secondary benefits12 References = 1: SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, page 1-12: A Practical Approach to Continuous Control Monitoring, ISACA Journal, Volume 2, 2015, page 1.

NEW QUESTION: 74
從業務角度來看，事件回應計畫的最大好處在於：
A. 透過提供預先定義的回應程序來提高效率
B. 提高對破壞性事件的安全反應能力
C. 限制破壞性事件的負面影響
D. 確保符合監理要求
Answer: (SHOW ANSWER)
The greatest business benefit of an incident response plan is minimizing the negative impact of disruptive incidents on operations and reputation.
"The primary business objective of an incident response plan is to minimize the impact of incidents on business operations and assets."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Plan Objectives* ISACA practice questions reinforce that limiting impact is the key outcome from a business perspective.

NEW QUESTION: 75
某個組織的資訊安全團隊在最近的資訊安全指導委員會會議上提交了風險登記冊。委員會最該關注下列哪一項？
A. 未發現某些風險的所有者。
B. 業務應用程式的風險數量最多。
C. 風險緩解行動計畫沒有時間表。
D. 風險緩解行動計畫里程碑被延後。
Answer: (SHOW ANSWER)

The most concerning issue for the information security steering committee should be that no owners were identified for some risks in the risk register. This means that there is no clear accountability and responsibility for managing and mitigating those risks, and that the risks may not be properly addressed or monitored. The risk owners are the persons who have the authority and ability to implement the risk treatment options and to accept the residual risk. The risk owners should be identified and assigned for each risk in the risk register, and they should report the status and progress of the risk management activities to the information security steering committee.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Management, Subsection: Risk Register, Page 104.

NEW QUESTION: 76
當入侵偵測系統 (IDS) 報告基於外部網路的攻擊時，下列哪一項是檢口防火牆日誌的主要原因？
A. 驗證有效載荷簽名
B. 驗證事件
C. 檢口網路配置
D. 制定事件回應策略
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 77
新的資訊安全報告要求即將生效。下列哪一項應該是資安經理的首要行動？
A. 進行與不遵守新要求相關的成本效益分析。
B. 針對新需求進行差距評估。
C. 調口以確定新要求是否適用於該業務。
D. 通知高階管理層新的要求。
Answer: (SHOW ANSWER)
Before taking any compliance steps, the information security manager must first assess whether the regulation is applicable to the organization. This ensures resources are not spent unnecessarily.
"The applicability of legal, regulatory, and contractual requirements must be determined before initiating compliance activities."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Compliance*

NEW QUESTION: 78
下列哪一項是向高階管理層展示資訊安全控制有效性的最合適的指標？
A. 因惡意軟體感染而導致的停機
B. 網路掃描發現的安全漏洞數量
C. 已修補的伺服器百分比
D. 安全事件造成的年化損失
Answer: (SHOW ANSWER)
Annualized loss resulting from security incidents is the most appropriate metric to demonstrate the effectiveness of information security controls to senior management, as it quantifies the financial impact of security breaches on the organization's assets, operations, and reputation. This metric helps to communicate the value of security investments, justify the security budget, and prioritize the security initiatives based on the potential loss reduction. Annualized loss resulting from security incidents can be calculated by multiplying the annualized rate of occurrence (ARO) of an incident by the single loss expectancy (SLE) of an incident. ARO is the estimated frequency of an incident occurring in a year, and SLE is the estimated cost of an incident. For example, if an organization estimates that a ransomware attack may occur once every two years, and that each attack may cost $100,000 to recover, then the annualized loss resulting from ransomware attacks is $50,000 ($100,000 / 2).
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112; Key Performance Indicators for Security Governance, Part 1; Performance Measurement Guide for Information Security

NEW QUESTION: 79
資訊安全策略的首要目標應該是什麼？
A. 確保與業界最佳實務保持一致
B. 概述管理階層期望
C. 為了遵守監理要求
D. 詳細□明安全程序
Answer: (SHOW ANSWER)
The primary objective of an information security policy is to outline management expectations (B). In CISM governance, policies serve as high-level statements that define direction, intent, and accountability for information security. While alignment with best practices (A) and regulatory compliance (C) are important considerations, they are secondary to clearly communicating what management expects from the organization.
Detailing procedures (D) is not the role of policy; procedures translate policy into actionable steps. Clear policies establish authority and provide the foundation for standards, procedures, and enforcement.

References: ISACA CISM Review Manual (Governance-policy purpose and hierarchy); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 80

什麼時候是驗證生產系統的安全機制是否符合控制目標的最佳時間？

A. 品質和驗收檢口期間

B. 透過監控活動和自動化工具持續進行

C. 滲透測試建議的補救措施完成後

D. 在年度口部和合規審計期間

Answer: (SHOW ANSWER)

While audits and assessments provide periodic insights, the best time to verify that security mechanisms meet control objectives is continuously-through monitoring and automation. Continuous monitoring allows the organization to detect misconfigurations, anomalies, or control failures in real-time, significantly improving response capabilities. Modern environments, especially in production systems, require real-time feedback loops to maintain compliance and effectiveness due to rapidly evolving threats and configuration changes.

"Continuous monitoring provides assurance that controls are operating effectively in real time, enabling timely corrective actions."

- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Control Monitoring*

NEW QUESTION: 81

在確定備份頻率時最重要的是要考慮下列哪一項？

A. 最大可容忍中斷 (MTO)

B. 復原時間目標 (RTO)

C. 復原點目標 (RPO)

D. 允許的中斷視窗

Answer: (SHOW ANSWER)

NEW QUESTION: 82

下列哪一項指標提供了資訊安全治理與公司治理一致的最佳證據？

A. 與安全計畫相關的平均投資報酬率 (ROI)

B. 跨業務部門的平均安全事件數

C. 企業範圍口的安全事件的平均解決時間 (MTTR)

D. 為高風險資訊資口識別的漏洞數量

Answer: (SHOW ANSWER)

Average return on investment (ROI) associated with security initiatives is the best metric to provide evidence of alignment of information security governance with corporate governance because it demonstrates the value and benefits of security investments to the organization's strategic goals and objectives. Average number of security incidents across business units is not a good metric because it does not measure the effectiveness or efficiency of security initiatives or

their alignment with corporate governance. Mean time to resolution (MTTR) for enterprise-wide security incidents is not a good metric because it does not measure the impact or outcome of security initiatives or their alignment with corporate governance. Number of vulnerabilities identified for high-risk information assets is not a good metric because it does not measure the performance or improvement of security initiatives or their alignment with corporate governance. References: https://www.
isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security- investments https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the- effectiveness-of-information-security-governance

NEW QUESTION: 83
一家組織希望投資一項新興技術。在評估其影響時，資訊安全經理最應該考慮下列哪一項因素？
A. 系統相容性
B. 技術中的漏洞
C. 安全性配置
D. 業界對此技術的同儕審□
Answer: (SHOW ANSWER)

NEW QUESTION: 84
提供訊息本機加密的電子郵件軟體包的一個常見缺點是加密：
A. 無法加密附件
B. 無法跨□品域互通。
C. 密鑰長度不足。
D. 沒有密鑰恢復機制。
Answer: (SHOW ANSWER)
Email software packages that provide native encryption of messages use proprietary algorithms and formats that are not compatible with other email software packages. This means that the encryption cannot interoperate across product domains, and the recipients of encrypted messages must use the same email software package as the sender to decrypt and read the messages. This limits the usability and scalability of native encryption, and may also pose security risks if the encryption algorithms or formats are not well-tested or widely accepted. A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains1234. References = CISM Review Manual 15th Edition, page 206. The Top 10 Email Encryption Solutions In 2023 - Expert Insights2, The Best Email Encryption Services for 2023 | PCMag3, The Top 12 Email Encryption Services for 2023 - Right Inbox4.
A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

NEW QUESTION: 85
讓資訊安全經理在變革管理委員會任職的最重要原因是：
A. 識別資訊安全性策略的變更。
B. 確保更改經過測試。
C. 確保正確記錄變更。
D. 就與變更相關的風險提供建議。
Answer: (SHOW ANSWER)
The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2.
The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.
The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes.
Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities.

However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk. References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION: 86
一家企業希望將專有應用程式遷移到使用平台即服務 (PaaS) 模型的第三方雲端託管服務供應商。在選擇雲端服務供應商之前，該企業最需要確保的是什麼？
A. 雲端提供者可以滿足復原點目標 (RPO)。
B. 雲端提供者遵守適用的法規。
C. 雲端提供者的服務等級協定 (SLA) 包含可用性要求。
D. 託管合約包含終止條款。
Answer: B (LEAVE A REPLY)
When outsourcing to a cloud provider, regulatory compliance is paramount-especially with sensitive or proprietary applications. Non-compliance could result in legal penalties, fines, or reputational damage.
While RPOs, SLAs, and contract clauses are critical components of vendor risk management, ensuring adherence to relevant laws and industry regulations (such as GDPR, HIPAA, PCI DSS) is the first priority in cloud migration decisions.
"Prior to selecting a cloud provider, legal, regulatory, and contractual requirements must be reviewed to ensure alignment."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Considerations in Cloud Computing*

NEW QUESTION: 87
誰最適合確定資料庫中的資訊應如何分類？
A. 資料庫分析師
B. 資料庫管理員 (DBA)
C. 資訊安全分析師

D. 資料擁有者

Answer: (SHOW ANSWER)

= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements.

Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Data Classification, page 331

NEW QUESTION: 88

下列哪一項為資訊安全經理提供了有關組織回應網路攻擊的能力的最準確指示？

A. 事件響應計畫的演練

B. 黑盒滲透測試

C. 模擬網路釣魚練習

D. 紅隊演習

Answer: (SHOW ANSWER)

A red team exercise is a simulated cyber attack conducted by a group of ethical hackers or security experts (the red team) against an organization's network, systems, and staff (the blue team) to test the organization's ability to detect, respond, and recover from a real cyber attack. A red team exercise provides an information security manager with the most accurate indication of the organization's ability to respond to a cyber attack, because it mimics the tactics, techniques, and procedures of real threat actors, and challenges the organization' s security posture, incident response plan, and security awareness in a realistic and adversarial scenario12. A red team exercise can measure the following aspects of the organization's cyber attack response capability3:

The effectiveness and efficiency of the security controls and processes in preventing, detecting, and mitigating cyber attacks The readiness and performance of the incident response team and other stakeholders in following the incident response plan and procedures The communication and coordination among the internal and external parties involved in the incident response process The resilience and recovery of the critical assets and functions affected by the cyber attack The lessons learned and improvement opportunities identified from the cyber attack simulation The other options, such as a walk-through of the incident response plan, a black box penetration test, or a simulated phishing exercise, are not as accurate as a red team exercise in indicating the organization's ability to respond to a cyber attack, because they have the following limitations4 :

A walk-through of the incident response plan is a theoretical and hypothetical exercise that involves reviewing and discussing the incident response plan and procedures with the relevant stakeholders, without actually testing them in a live environment. A walk-through can help to familiarize the participants with the incident response roles and responsibilities, and to identify any gaps or inconsistencies in the plan, but it cannot measure the actual performance and effectiveness of the incident response process under a real cyber attack scenario.
A black box penetration test is a technical and targeted exercise that involves testing the security of a specific system or application, without any prior knowledge or access to its internal details or configuration. A black box penetration test can help to identify the vulnerabilities and weaknesses of the system or application, and to simulate the perspective and behavior of an external attacker, but it cannot test the security of the entire network or organization, or the response of the incident response team and other stakeholders to a cyber attack.
A simulated phishing exercise is a social engineering and awareness exercise that involves sending fake emails or messages to the organization's staff, to test their ability to recognize and report phishing attempts. A simulated phishing exercise can help to measure the level of security awareness and training of the staff, and to simulate one of the most common cyber attack vectors, but it cannot test the security of the network or systems, or the response of the incident response team and other stakeholders to a cyber attack.
References = 1: What is a Red Team Exercise? | Redscan 2: Red Team vs Blue Team: How They Differ and Why You Need Both | CISA 3: Red Team Exercises: What They Are and How to Run Them | Rapid7 4: What is a Walkthrough Test? | Definition and Examples | ISACA : Penetration Testing Types: Black Box, White Box, and Gray Box | CISA

NEW QUESTION: 89
將安全責任嵌入工作描述中非常重要，主要是因為它：
A. 支援存取管理。
B. 簡化安全意識計劃的發展。
C. 使安全性與人力資源 (HR) 職能保持一致。
D. 加強員工問責。
Answer: D (LEAVE A REPLY)
Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

NEW QUESTION: 90

下列哪一項對於傳達安全報告中的前瞻性趨勢最有效？

A. 關鍵控制指標 (KCI)

B. 關鍵風險指標 (KRI)

C. 關鍵績效指標 (KPI)

D. 關鍵目標指標 (KGI)

Answer: (SHOW ANSWER)

= Security reporting is the process of providing relevant and timely information on the status and performance of the information security program to the stakeholders. Security reporting should be aligned with the business objectives and risk appetite of the organization, and should provide meaningful insights and recommendations for decision making and improvement. Security reporting should also include forward- looking trends, which are projections or predictions of future events or conditions based on historical data, current situation, and external factors. Forward-looking trends can help the organization anticipate and prepare for potential risks and opportunities, and adjust their strategies and plans accordingly.

One of the most effective ways to communicate forward-looking trends within security reporting is to use key risk indicators (KRIs). KRIs are metrics that measure the level of exposure or likelihood of a risk event occurring, and provide early warning signals of potential changes in the risk profile. KRIs can help the organization monitor and manage the key risks that may affect the achievement of their objectives, and take proactive actions to mitigate or avoid them. KRIs can also help the organization identify emerging risks and trends, and evaluate the effectiveness of their risk treatment options. KRIs should be aligned with the risk appetite and tolerance of the organization, and should be regularly reviewed and updated to reflect the changing risk environment.

The other options are not the most effective ways to communicate forward-looking trends within security reporting. Key control indicators (KCIs) are metrics that measure the effectiveness and efficiency of the security controls implemented to reduce the impact or likelihood of a risk event. KCIs can help the organization assess and improve the performance of their security processes and activities, and ensure compliance with the security policies and standards. However, KCIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key performance indicators (KPIs) are metrics that measure the achievement of the security objectives and goals, and demonstrate the value and contribution of the information security program to the organization. KPIs can help the organization evaluate and communicate the results and outcomes of their security initiatives and projects, and align them with the business strategy and vision. However, KPIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. Key goal indicators (KGIs) are metrics that measure the progress and completion of the security goals and targets, and indicate the degree of success and satisfaction of the information security program. KGIs can help the organization track and report the status and milestones of their security plans and actions, and ensure alignment with the stakeholder expectations and requirements.

However, KGIs do not directly measure the level of exposure or likelihood of a risk event, and may not provide sufficient information on the future trends and scenarios. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 77-78, 81-821; CISM Online Review Course, Domain 3: Information Security Program Development and Management, Module 4: Information Security Program Resources, ISACA2

NEW QUESTION: 91
在定義如何分配資訊安全預算時，下列何者最重要？
A. 監理合規標準
B. 資訊安全策略
C. 資訊安全策略
D. 業務影響評估
Answer: (SHOW ANSWER)
Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are-shaping-up.html
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 92

當管理階層改變企業業務策略時，應使用下列哪一個流程來評估現有的資訊安全控制措施以及選擇新的資訊安全控制措施？

A. 設定管理

B. 風險管理

C. 存取控制管理

D. 變更管理

Answer: (SHOW ANSWER)

According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the organization's business strategy and objectives, as well as complying with applicable laws and regulations1.

The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.

The CISM Exam Content Outline also covers the topic of change management in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:

3.2.2 Change Management

3.2.3 Change Control

3.2.4 Change Implementation

3.2.5 Change Monitoring

I hope this answer helps you prepare for your CISM exam. Good luck! #

NEW QUESTION: 93

組織的品質流程可以透過提供以下口容來最好地支援安全管理：

A. 安全配置控制項。

B. 確保滿足安全要求。

C. 安全策略指導。

D. 安全系統文件的儲存庫。

Answer: (SHOW ANSWER)

= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct

security defects, measure security performance and effectiveness, and improve security practices and procedures. References = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

NEW QUESTION: 94
資訊安全經理在決定是否應儲存資料時要考慮下列哪一項最重要？
A. 業務需求
B. 資料保護法規
C. 資料儲存限制
D. 資料的類型和性質
Answer: (SHOW ANSWER)

NEW QUESTION: 95
下列哪一項是網路彈性策略的主要目標？
A. 業務連續性
B. 監理合規性
C. 員工意識
D. 行政支持
Answer: (SHOW ANSWER)
Business continuity is the primary objective of a cyber resilience strategy, as it aims to ensure that the organization can continue to deliver its essential products and services in the face of cyber disruptions, and recover to normal operations as quickly and effectively as possible. A cyber resilience strategy should align with the business continuity plan and support the organization's mission, vision, and values. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

NEW QUESTION: 96
某個組織已修復系統中的安全缺陷。接下來應該執行下列哪項操作？
A. 評估殘餘風險。
B. 與組織分享經驗教訓。
C. 更新系統文件。
D. 為滲透測試分配預算。
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after applying controls to mitigate the original risk. It is important to assess the residual risk after remediation to ensure that it is within the acceptable

level and tolerance of the organization. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 97
經過風險評估後，組織決定採用自帶設備(BYOD) 策略。資訊安全經理下一步該做什麼？
A. 制定個人設備政策
B. 實施行動裝置管理 (MDM) 解決方案
C. 制定針對 BYOD 意識的培訓
D. 定義控制要求
Answer: D (LEAVE A REPLY)
Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.
References:
https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating- effective-policies-and-mitigating
https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

NEW QUESTION: 98
下列哪一項能為資訊安全經理提供可能影響業務目標的新威脅和新興風險的最有用資訊？
A. 外部審計報告
B. 口部威脅分析報告
C. 口業威脅情報報告
D. 口部漏洞評估報告
Answer: (SHOW ANSWER)
An industry threat intelligence report (C) provides the most useful insight into new and emerging threats because it aggregates intelligence across organizations, sectors, and geographies. CISM emphasizes the importance of understanding the external threat landscape to anticipate risks that may not yet be visible internally. Audit reports (A) and vulnerability assessments (D) are retrospective and organization-specific.
Internal threat analysis (B) focuses on known issues rather than emerging trends. Threat intelligence supports proactive risk identification and helps align security strategy with evolving business risks.
References: ISACA CISM Review Manual (Risk management-threat intelligence, emerging risk identification); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 99
下列哪一項應該是向高階管理層提交的資訊安全計畫狀態報告的主要重點？

A. 提供資源如預期運作的證據
B. 驗證安全成本不超出預算
C. 證明風險已控制在所需水平
D. 確認組織遵守安全策略
Answer: (SHOW ANSWER)
The primary focus of a status report on the information security program to senior management is to demonstrate that the risk to the organization's information assets is managed at the desired level, in alignment with the business objectives and risk appetite. This can be achieved by providing relevant and meaningful metrics, indicators, and trends that show the performance, effectiveness, and value of the information security program, as well as the current and emerging risks and the corresponding mitigation strategies. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 100
在為資訊安全計畫建立支援時，下列哪一個元素最重要？
A. 資訊風險評估
B. 業務影響分析 (BIA)
C. 威脅分析
D. 辨識現有漏洞
Answer: (SHOW ANSWER)

NEW QUESTION: 101
伺服器遭到攻擊後，下列哪一項是最佳行動方案？
A. 口動事件回應。
B. 口看漏洞評估。
C. 進行安全審核。
D. 隔離系統。
Answer: (SHOW ANSWER)
Initiating incident response is the best course of action after a server has been attacked because it activates the incident response plan or process, which defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Reviewing vulnerability assessment is not a good course of action because it does not address the current attack or its impact, but rather evaluates the potential weaknesses or exposures of the server. Conducting a security audit is not a good course of action because it does not address the current attack or its impact, but rather verifies and validates the compliance or performance of the server's security controls or systems. Isolating the system is not a good course of action because it does not address the current attack or its impact, but rather stops or limits any communication or interaction with the server.
References: https://www.isaca.org/resources/isaca- journal/issues/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal /issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 102
下列哪一項是證明資訊安全策略與業務目標一致的最有效方法？
A. 平衡計分卡
B. 風險矩陣
C. 基準測試
D. 熱圖
Answer: (SHOW ANSWER)
The most effective way to demonstrate alignment of information security strategy with business objectives is to use a balanced scorecard. A balanced scorecard is a strategic management tool that translates the vision and mission of an organization into a set of performance indicators that measure its progress towards its goals. A balanced scorecard typically includes four perspectives: financial, customer, internal process, and learning and growth. Each perspective has a set of objectives, measures, targets, and initiatives that are aligned with the organization's strategy. A balanced scorecard helps to communicate, monitor, and evaluate the performance of the organization and its information security program in relation to its business objectives. A balanced scorecard also helps to identify and prioritize improvement opportunities, as well as to align the activities and resources of the organization with its strategy12.
The other options are not the most effective ways to demonstrate alignment of information security strategy with business objectives. A risk matrix is a tool that displays the likelihood and impact of various risks on a two-dimensional grid. A risk matrix helps to assess and prioritize risks, as well as to determine the appropriate risk response strategies. However, a risk matrix does not show how the information security strategy supports the business objectives, nor does it measure the performance or the value of the information security program3. Benchmarking is a process of comparing the performance, practices, or processes of an organization with those of other organizations or industry standards. Benchmarking helps to identify best practices, gaps, and areas for improvement, as well as to set realistic and achievable goals. However, benchmarking does not show how the information security strategy aligns with the business objectives, nor does it reflect the unique characteristics and needs of the organization4. A heat map is a graphical representation of data using colors to indicate the intensity or frequency of a variable. A heat map can be used to visualize the distribution, concentration, or variation of risks, controls, or incidents across different dimensions, such as business units, processes, or assets. A heat map helps to highlight the areas of high risk or low control effectiveness, as well as to facilitate decision making and resource allocation. However, a heat map does not show how the information security strategy contributes to the business objectives, nor does it measure the outcomes or the benefits of the information security program5. References = CISM Review Manual, 16th Edition | Print | English 2, Chapter 1: Information Security Governance, pages 28-29, 31-32, 34-35.
Balanced Scorecard - Wikipedia 1
Risk Matrix - Wikipedia 3
Benchmarking - Wikipedia 4

Heat map - Wikipedia 5

NEW QUESTION: 103
在向高階管理層提交的資訊安全狀態報告中，下列哪一項最重要？
A. 關鍵風險指標 (KRI)
B. 資訊安全政策審口
C. 資訊安全預算請求
D. 最近的安全事件列表
Answer: (SHOW ANSWER)
According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

NEW QUESTION: 104
組織允許在員工擁有的智慧型手機上儲存和使用其關鍵和敏感資訊。下列哪一項是最好的安全控制？
A. 建立遠端擦除權限
B. 進行安全意識培訓
C. 要求使用者備份組織的數據
D. 監控智慧型手機的使用頻率
Answer: (SHOW ANSWER)
The best security control for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones is establishing the authority to remote wipe. Remote wipe is a feature that allows an authorized administrator or user to remotely erase the data on a device in case of loss, theft, or compromise1. Remote wipe can help prevent unauthorized access or disclosure of the organization's information on employee-owned smartphones, as well as protect the privacy of the employee's personal data.
Remote wipe can be implemented through various methods, such as mobile device management (MDM) software, native device features, or third-party applications2. However, remote wipe requires the consent and cooperation of the employee, as well as a clear policy that defines the conditions and procedures for its use.
The other options are not the best security controls for an organization that permits the storage and use of its critical and sensitive information on employee-owned smartphones. Developing security awareness training is an important measure to educate employees about the security risks and responsibilities associated with using their own smartphones for work purposes, but it does not provide a technical or physical protection for the data on the devices3. Requiring the backup of the organization's data by the user is a good practice to ensure data availability and recovery in case of device failure or loss, but it does not prevent unauthorized access or

disclosure of the data on the devices4. Monitoring how often the smartphone is used is a possible way to detect abnormal or suspicious activities on the devices, but it does not prevent or mitigate the impact of a data breach on the devices. References: 4: Mobile Device Backup - NIST 3: Security Awareness Training - NIST
1: Remote Wipe - Lifewire 2: How Businesses with a BYOD Policy Can Secure Employee Devices - IBM :
Mobile Device Security Policy - SANS

NEW QUESTION: 105
下列哪一項對於確定是否遵守資訊安全政策最有幫助？
A. 指令控制
B. 修正控制
C. 偵探控制
D. 預防控制
Answer: (SHOW ANSWER)

NEW QUESTION: 106
進行事件後檢討的主要目標是：
A. 重新評估事件的影響。
B. 辨識漏洞。
C. 識別控制改進。
D. 確定根本原因。
Answer: (SHOW ANSWER)
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.
Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.
Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re- evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.
Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity,

or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.
Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. References = ISACA CISM: PRIMARY goal of a post-incident review should be to?
CISM Exam Overview - Vinsys
CISM Review Manual, Chapter 4, page 176
CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 107
制定業務連續性計畫 (BCP) 時應先執行下列哪項操作？
A. 口看目前的復原策略。
B. 檢視現有的網路保險範圍。
C. 定義組織策略。
D. 決定關鍵流程的優先順序。
Answer: (SHOW ANSWER)

NEW QUESTION: 108
在對一個關鍵系統進行資訊安全風險評估後，發現了幾個重大問題 下列哪一項對於資安經理來口最重要？
A. 風險被記錄在組織的風險登記冊中。
B. 風險已報告給業務部門的高階管理層。
C. 風險已升級至 IT 部門進行補救。
D. 風險已傳達至中央風險職能部門。
Answer: A (LEAVE A REPLY)
Entering identified risks into the organization's risk register ensures that they are documented, tracked, assigned, and addressed. Without recording in the risk register, there's no formal mechanism to manage, treat, or monitor the risk.

"The risk register is the central repository for tracking all known risks, their status, and treatment plans."
- CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, Section: Risk Response and Risk Register*

NEW QUESTION: 109
下列哪一項對於確保有效的事件回應至關重要？
A. 業務連續性計劃 (BCP)
B. 成本效益分析
C. 分類方案
D. 高階管理層支持
Answer: (SHOW ANSWER)
Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.
The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

NEW QUESTION: 110
下列哪一項是對面向公眾的 Web 伺服器的分散式拒絕服務 (DDoS) 攻擊造成的最大威脅？
A. 執行未經授權的命令
B. 阻止授權訪問
C. 竄改網站內容
D. 未經授權存取資源
Answer: (SHOW ANSWER)
Prevention of authorized access is the greatest threat posed by a distributed denial of service (DDoS) attack on a public-facing web server because it prevents legitimate users or customers from accessing the web services or resources, causing disruption, dissatisfaction, and potential loss of revenue or reputation. Execution of unauthorized commands is not a threat posed by a DDoS attack, but rather by a remote code execution (RCE) attack. Defacement of website

content is not a threat posed by a DDoS attack, but rather by a web application attack. Unauthorized access to resources is not a threat posed by a DDoS attack, but rather by a brute force attack or an authentication bypass attack. References: https://www.isaca.org/resources/isaca-journal/issues /2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016 /volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 111
下列哪一項對組織對新口業法規的回應影響最大？
A. 組織的控制目標
B. 組織的風險管理框架
C. 組織的風險偏好
D. 組織的風險控制基線
Answer: (SHOW ANSWER)
The most influential factor on an organization's response to a new industry regulation is the organization's risk appetite. This is because the risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives, and it guides the decision-making process for managing risks. The risk appetite also determines the extent to which the organization needs to comply with the new regulation, and the resources and actions required to achieve compliance. The risk appetite should be aligned with the organization's strategy, culture, and values, and it should be communicated and monitored throughout the organization.

NEW QUESTION: 112
當組織採用新興技術時，下列哪一項是資訊安全經理最重要的角色？
A. 了解對現有資源的影響
B. 評估使用相同技術的同儕組織受到的影響
C. 審口供應商合約和服務等級協定 (SLA)
D. 為最終使用者提供培訓，讓他們熟悉新技術
Answer: (SHOW ANSWER)

NEW QUESTION: 113
為了準備在涉及惡意軟體的事件後進行第三方取證調口，事件回應團隊應該：
A. 隔離受感染的系統。
B. 保留證據。
C. 對受感染的系統進行映像。
D. 清除惡意軟體。
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the incident response team should preserve the evidence as the first step to prepare for a third-party forensics investigation, as it helps to maintain the

integrity and admissibility of the evidence in a court of law. Preserving the evidence may include isolating and imaging the infected systems, but these are not the only actions required. Cleaning the malware may destroy or alter the evidence and should be avoided until the investigation is completed.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.6.2, page 165

NEW QUESTION: 114
若事件調□未能在事件回應計畫分配的時間□完成，事件回應團隊應採取下列哪一項措施？
A. 呼叫業務連續性計劃 (BCP)。
B. □動升級流程。
C. 聯絡危機管理團隊。
D. 繼續調□。
Answer: (SHOW ANSWER)

NEW QUESTION: 115
資訊安全經理認為資訊分類不當=有外洩風險。下列哪一項是資安經理的最佳行動？
A. 將此問題提交給□部稽核以尋求建議。
B. 將資料重新分類並提高安全等級以滿足業務風險。
C. 指示相關係統擁有者對資料進行重新分類。
D. 完成風險評估並將結果提交給資料擁有者。
Answer: (SHOW ANSWER)
= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.
If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach, as well as the cost and benefit of implementing additional

security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.
The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security manager. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701; CISM Online Review Course, Domain 3:
Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

NEW QUESTION: 116
下列哪一項定義了新開發的資訊系統最全面的安全要求？
A. 風險評估結果
B. 審計結果
C. 關鍵風險指標 (KRI)
D. 基線控制
Answer: (SHOW ANSWER)
Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance.
Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs)

are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. References = CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization." CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478:
"Baseline controls are the minimum security requirements that apply to all systems within the organization.
They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

NEW QUESTION: 117
下列哪一種備份方法需要最多時間來還原應用程式的資料？
A. 完整備份
B. 增量
C. 差分
D. 磁碟鏡像
Answer: (SHOW ANSWER)
= An incremental backup method only backs up the data that has changed since the last backup, whether it was a full or an incremental backup. This method requires the least amount of time and storage space for backup, but it requires the most time to restore data for an application. To restore data from an incremental backup, the latest full backup and all the subsequent incremental backups are needed. A full backup method backs up all the data in a system or an application at a point in time. This method requires the most amount of time and storage space for backup, but it requires the least time to restore data for an application. To restore data from a full backup, only the latest full backup is needed. A differential backup method backs up the data that has changed since the last full backup. This method requires more time and storage space for backup than the incremental method, but less than the full backup method. It also requires less time to restore data for an application than the incremental method, but more than the full backup method. To restore data from a differential backup, the latest full backup and the latest differential backup are needed. A disk mirroring method creates an exact copy of a disk on another disk in real time. This method provides the highest level of availability and fault tolerance, but it also requires twice the amount of disk space. To restore data from a disk mirroring method, the mirrored disk can be used as the primary disk in case of a failure. References = CISM Review Manual 15th Edition, page 201-202.
The method that requires the MOST time to restore data for an application is a Full Backup. Full backups contain all the data that is required to restore an application, but the process of restoring the data is the most time-consuming as it involves copying all the data from the backup to the application. Incremental backups only backup the changes made since the last backup, differential backups only backup changes made since the last full backup, and disk mirroring provides real-time data replication, so the data is immediately available.

NEW QUESTION: 118
在決定組織的風險處理方法時，下列何者是最佳策略？
A. 實施被視為速效措施的風險緩解控制措施
B. 優先考慮直接緩解組織最關鍵風險的控制措施
C. 根據風險承受能力提高現有控制措施的成熟度
D. 在所有組織部門實施一刀切的控制措施
Answer: (SHOW ANSWER)
Risk treatment should be prioritized based on risk criticality. Addressing the most severe and likely risks first ensures that resources are focused where they can have the greatest impact. "Risk treatment efforts should focus on the most significant risks first, based on likelihood and impact."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options*

NEW QUESTION: 119
如果民事訴訟是組織回應安全事件的目標，則主要步驟應該是：
A. 聯絡執法單位。
B. 記錄監管鏈。
C. 使用標準伺服器備份公用程式擷取證據。
D. 在安全區域重新口動受影響的電腦以搜尋證據。
Answer: (SHOW ANSWER)
Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court. The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12. Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server- backup utilities © is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody.
Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks involved in the incident, but it may also introduce changes or errors that

could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12.
Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files, or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4:
Information Security Incident Management (ISIM) [2022 update]2

NEW QUESTION: 120

資訊安全經理發現系統管理員沒有將伺服器管理員帳戶的使用者名稱變更為預設使用者名稱。業務經理已製定並批准了一項策略，要求進行這些變更。下列哪一項應該是資安經理的首要行動？

Freeclain.net

A. 將此要求納入資訊安全意識材料中
B. 執行政策遵從性評估
C. 確保已將該策略傳達給系統管理員。
Answer: (SHOW ANSWER)
The first course of action is to ensure the policy has been communicated to the system administrators (C).
CISM governance principles require that policies be formally communicated and understood before enforcement or compliance assessment occurs. Conducting assessments (B) or training (A) is ineffective if administrators are not aware of the policy requirements. Effective governance follows a sequence: approval # communication # implementation # monitoring and enforcement. Communication ensures accountability and supports consistent adoption of security requirements.
References: ISACA CISM Review Manual (Governance-policy lifecycle, communication and enforcement); CISM Exam Content Outline (Domain 2).

NEW QUESTION: 121
下列哪一項任務可以為新任命的資訊安全經理提供對組織現有安全態勢的最佳了解？
A. 審口政策和程序
B. 執行風險評估
C. 採訪業務經理和員工
D. 執行業務影響分析 (BIA)
Answer: (SHOW ANSWER)
Performing a risk assessment gives a holistic and objective understanding of the threats, vulnerabilities, and controls across the organization. It reveals actual risk exposures and the effectiveness of current controls, which directly reflect the organization's security posture.

"Risk assessments identify and evaluate risk and provide the basis for determining how those risks should be managed and mitigated."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment
According to ISACA's CISM Practice Question Database, performing a risk assessment is prioritized over reviewing documents or conducting interviews because it offers direct insight into current exposures and control effectiveness.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122
下列哪一項是製定資訊安全策略時要考慮的最重要的限制？
A. 法律和監管要求
B. 已建立的安全政策和標準
C. 符合國際安全標準
D. 資訊安全架構
Answer: (SHOW ANSWER)
Legal and regulatory requirements are the most important constraint to be considered when developing an information security strategy, as they define the minimum level of security that the organization must comply with to avoid legal sanctions, fines, or reputational damage. Legal and regulatory requirements may vary depending on the jurisdiction, industry, and type of data that the organization handles, and they may impose specific security controls, standards, or frameworks that the organization must follow. References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.2.1.11

NEW QUESTION: 123
以下人員中，誰最適合承擔應用程式中發現的風險？
A. 高階管理層
B. 資訊安全經理
C. 系統擁有者
D. 控制項擁有者
Answer: (SHOW ANSWER)

NEW QUESTION: 124
進行法醫調口時，下列何者最重要？

A. 分析系統口存
B. 記錄分析步驟
C. 擷取完整系統映像
D. 維護監理鏈
Answer: (SHOW ANSWER)
Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence. References = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

NEW QUESTION: 125
某組織的研究部門計劃將機器學習演算法應用於包含客口姓名和購買歷史記錄的大型資料集。個人資料外洩的風險被認為具有高影響力。在這種情況下，下列哪一項是最佳的風險處理選項？
A. 透過對資料集套用匿名化來降低風險。
B. 透過加密資料集中的客口名稱來降低風險。
C. 接受風險，因為好處超過了潛在的後果
D. 透過購買保險來轉移風險。
Answer: (SHOW ANSWER)

NEW QUESTION: 126
某個組織推出了新的自帶設備 (BYOD) 計劃。安全經理確定少數員工正在利用免費的雲端儲存服務透過行動裝置儲存公司資料。下列哪一項是最有效的行動方案？
A. 出於監控目的，允許暫時繼續該做法
B. 禁止員工遠端存取公司電子郵件和數據
C. 口動設備的遠端擦除
D. 評估提供安全解決方案的業務需求
Answer: D (LEAVE A REPLY)
The most effective course of action when employees are using free cloud storage services to store company data through their mobile devices is to assess the business need to provide a secure solution, such as a corporate-approved cloud service or a virtual desktop environment. Assessing the business need can help understand why employees are using free cloud storage services, what kind of data they are storing, and what are the security risks and requirements. Based on the assessment, the security manager can propose a secure solution that meets the business needs and complies with the BYOD policy. The other options, such as allowing the

practice to continue, disabling remote access, or initiating remote wipe, may not address the underlying business need or may cause disruption or data loss. References:
* https://www.digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing- breach
* https://news.microsoft.com/en-xm/2021/03/18/how-to-have-secure-remote-working-with-a-byod-policy/
* https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide- bring-your-own-device-byod

NEW QUESTION: 127
下列哪一項是商業影響分析 (BIA) 設計階段最重要的考量因素？
A. 選擇品質指標來監控業務績效
B. 估計端對端流程中斷的可能性
C. 取得儲備資金，為可能的企業倒閉做好準備
D. 確定業務營運的關鍵功能
Answer: (SHOW ANSWER)
The design phase of a BIA must begin with identifying critical business functions, since they determine:
Which systems/processes need protection
Recovery priorities
Acceptable downtime (RTO/MTD)
Without clearly defining what's critical, the BIA cannot guide resource allocation or continuity strategies effectively.
"A successful BIA must begin with identifying which business functions are critical to achieving organizational objectives."
- CISM Review Manual 15th Edition, Chapter 3: Business Continuity and Disaster Recovery, Section: BIA Methodology*

NEW QUESTION: 128
一位資訊安全經理獲悉即將生效的新資料保護法規。下列哪一項是管理不合規風險的最佳方法？
A. 與高階管理層協商最佳行動方案。
B. 實施一項工作計劃以遵守新立法。
C. 執行差距分析。
D. 了解不合規的代價。
Answer: (SHOW ANSWER)

NEW QUESTION: 129
下列哪一項應該是資訊安全事件回應流程的主要目標？
A. 進行事件分類
B. 與口部和外部各方溝通

C. 最大限度地減少對關鍵營運的負面影響

D. 將事件分類

Answer: C (LEAVE A REPLY)

The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents.

The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.

Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed.

However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.

Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.

Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION: 130

反向查找可用於防止成功：

Freecram.net

A. 拒口服務 (DoS) 攻擊

B. 會話駭客

C. 網路釣魚攻擊
D. 網際網路協定 (IP) 欺騙
Answer: (SHOW ANSWER)
Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

NEW QUESTION: 131
下列哪一項是資訊安全經理在回應可能擾亂業務的重大安全事件時最重要的行動方針？
A. 遵循升級流程。
B. 辨識妥協指標。
C. 通知執法單位。
D. 聯絡法醫調口員。
Answer: A (LEAVE A REPLY)
When responding to a major security incident that could disrupt the business, the information security manager's most important course of action is to follow the escalation process. The escalation process is a predefined set of steps and procedures that define who should be notified, when, how, and with what information in the event of a security incident. The escalation process helps to ensure that the appropriate stakeholders, such as senior management, business units, legal counsel, public relations, and external parties, are informed and involved in the incident response process. The escalation process also helps to coordinate the actions and decisions of the incident response team and the business continuity team, and to align the incident response objectives with the business priorities and goals. The escalation process should be documented and communicated as part of the incident response plan, and should be reviewed and updated regularly to reflect the changes in the organization's structure, roles, and responsibilities.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Incident Management and Response, video 32
Incident Response Models3

NEW QUESTION: 132
與雲端提供者一起制定事件回應策略時，下列何者是最重要的安全考量？
A. 升級流程
B. 技術能力
C. 復原時間目標（RTO）
D. 安全審計報告

Answer: (SHOW ANSWER)
Escalation processes ensure that the provider and the organization can coordinate quickly and effectively during incidents.
"A clearly defined escalation process ensures that incidents are handled swiftly and with the appropriate level of authority, particularly when working with cloud service providers."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Cloud and Outsourced Incident Response* ISACA practice questions reinforce that escalation processes are critical when collaborating with third parties in incident management.

NEW QUESTION: 133
關鍵系統之間的關係最好理解為
A. 評估關鍵績效指標 (KPI)
B. 執行業務影響分析 (BIA)
C. 發展系統分類方案
D. 評估復原時間目標 (RTO)
Answer: (SHOW ANSWER)
The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

NEW QUESTION: 134
在發現業務部門實施了新購買的應用程式並繞過變更管理流程後，資訊安全經理應該先執行下列哪項操作？
A. 修改採購流程。
B. 更新變更管理流程。
C. 與高階領導討論此問題。
D. 從生口中刪除應用程式。
Answer: (SHOW ANSWER)
An information security manager should first discuss the issue with senior leadership to escalate the problem and seek their support and guidance. Bypassing the change management process can introduce significant risks to the organization, such as unauthorized access, data loss, system instability, or compliance violations.
The information security manager should explain the potential impact and consequences of the incident, and recommend corrective actions to remediate the situation. The information security manager should also review the root cause of the incident and identify any gaps or weaknesses in the existing policies, procedures, or controls that allowed the business unit to implement the new application without proper authorization, testing, or documentation. The information security manager should then revise the procurement process, update the change management process, or implement other measures to prevent similar incidents from occurring in the future. Removing

the application from production may not be feasible or desirable, depending on the business needs and the severity of the risks involved. References = CISM Review Manual,
16th Edition, pages 100-1011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page
2692
Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 135
下列哪一項對於讓安全操作與 IT 治理架構保持一致最有幫助？
A. 安全風險評估
B. 安全操作程序
C. 資訊安全策略
D. 商業影響分析 (BIA)
Answer: (SHOW ANSWER)
An information security policy is the MOST helpful for aligning security operations with the IT governance framework because it defines the security objectives, principles, standards, and guidelines that guide the security operations activities and processes. An information security policy also establishes the roles and responsibilities, authorities and accountabilities, and reporting and communication mechanisms for security operations. An information security policy should be aligned with the IT governance framework, which provides the direction, structure, and oversight for the effective management and delivery of IT services and resources. An information security policy should also be consistent with the enterprise governance framework, which sets the vision, mission, values, and goals of the organization12. A security risk assessment (A) is helpful for identifying and evaluating the security risks that may affect the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A security risk assessment should be based on the information security policy, which defines the risk appetite, tolerance, and criteria for the organization12. A security operations program (B) is helpful for implementing and executing the security operations activities and processes that support the IT governance framework, but it is not the MOST helpful for aligning them. A security operations program should be derived from the information security policy, which provides the strategic direction and guidance for the security operations12. A business impact analysis (BIA) (D) is helpful for determining the criticality and priority of the business processes and functions that depend on the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A BIA should be conducted in accordance with the information security policy, which specifies the business continuity and disaster recovery requirements and objectives for the organization12. References = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2:
CISM Domain 1: Information Security Governance (ISG) [2022 update]2

NEW QUESTION: 136

在拒口服務（DoS）攻擊失敗後，已識別的弱點應該是：
A. 追蹤並報告直至最終解決
B. 如果發現類似的弱點，請記錄下來並重新檢口
C. 已記錄在安全意識計劃中
D. 不計成本，快速解決並消除
Answer: (SHOW ANSWER)
Any weaknesses identified, even after an unsuccessful attack, should be tracked and reported until they are fully resolved. This ensures accountability, remediation, and prevention of future incidents. Ignoring or delaying action increases exposure to future threats.
"All vulnerabilities must be tracked, assigned for remediation, and closed out following proper documentation and validation."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Remediation and Lessons Learned ISACA's guidance in the practice questions clearly recommends formal tracking and resolution of vulnerabilities as the best practice for ongoing security management.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137
下列哪一項對於減少分散式阻斷服務 (DDoS) 攻擊的影響最有效？
A. 對伺服器施加狀態限制。
B. 將站點分佈在多個 ISP 上。
C. 從源頭阻止攻擊。
D. 強化網路安全。
Answer: (SHOW ANSWER)
The answer to the question is B. Spread a site across multiple ISPs. This is because spreading a site across multiple Internet service providers (ISPs) can help to reduce the impact of a distributed denial of service (DDoS) attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. Spreading a site across multiple ISPs can also help to distribute the traffic load and balance the performance of the site, and to mitigate the effects of regional or network-specific outages or disruptions. Spreading a site across multiple ISPs can be done by using various techniques, such as anycast routing, content delivery networks (CDNs), or cloud-based services12.
Spreading a site across multiple ISPs can help to reduce the impact of a DDoS attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to

target and overwhelm a single point of failure. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; DDoS Attacks-A Cyberthreat and Possible Solutions2

NEW QUESTION: 138
一個組織最近更新並發布了其資訊安全政策和標準。資訊安全經理下一步該做什麼？
A. 進行風險評估。
B. 向利害關係人傳達變更。
C. 更新組織的風險登記冊。
D. 制定政策例外流程。
Answer: B (LEAVE A REPLY)
Communicating the changes to stakeholders is the next step after updating and publishing the information security policy and standards, as it ensures that the stakeholders are aware of the new or revised requirements, expectations and responsibilities, and can provide feedback or raise concerns if needed. Communication also helps to promote the acceptance and adoption of the policy and standards, and to reinforce the security culture and awareness within the organization. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

NEW QUESTION: 139
下列哪一項最能顯示組織已將資訊安全治理與公司治理結合？
A. 安全性能指標根據業務目標進行衡量。
B. 評估IT風險時根據業務損失來衡量影響。
C. 只要業務目標發生變化，就會檢視安全策略。
D. 安全供應商的服務等級是根據業務需求定義的。
Answer: A (LEAVE A REPLY)
Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives.
Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 140
對於需要高可用性的電子商務，下列哪項設計原則是最好的？
A. 手動故障轉移到另一個滿足使用者需求的電子商務網站
B. 單一入口點，允許快速接收和處理交易
C. 智慧型中間件，用於將交易從宕機系統引導至備用系統

D. 相鄰冷站點和具有關鍵資料鏡像副本的備用伺服器的可用性

Answer: (SHOW ANSWER)

Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention.
"Middleware solutions can provide automated failover capabilities, improving system resilience and availability."
- CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section:
Availability and Resilience*
Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

NEW QUESTION: 141

外包資訊安全管理時，下列何者是解決資料可用性問題的最佳方法？

A. 制定服務等級協定 (SLA)。

B. 制定應急計劃。

C. 規定保險要求。

D. 需要保密協議 (NDA)。

Answer: (SHOW ANSWER)

NEW QUESTION: 142

在為資訊安全計劃建立指標時，最好的方法是確定以下指標：

A. 減少資訊安全計畫支出。

B. 支持重大資訊安全措施。

C. 反映企業風險文化。

D. 展示安全計畫的有效性。

Answer: (SHOW ANSWER)

Metrics for an information security program should be aligned with the security objectives and strategy, and should demonstrate how well the program is performing in terms of reducing risk, enhancing security posture, and supporting business goals. Metrics that support major information security initiatives, reflect the corporate risk culture, or reduce information security program spending may be useful, but they are not the best approach for establishing metrics for the entire program.
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112

NEW QUESTION: 143

下列哪一項是有效資訊安全治理的最佳標誌？

A. 資訊安全被視為整個資訊安全團隊的責任。

B. 資訊安全控制指派給風險擁有者。

C. 資訊安全已融入公司治理。
D. 資訊安全治理是基於外部安全框架。
Answer: (SHOW ANSWER)
Information security governance (ISG) is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk1. Effective ISG ensures that information security is integrated into corporate governance and is considered an essential component of enterprise governance2. Information security is not just the responsibility of the information security team, but of all stakeholders in the organization3. Information security controls are not assigned to risk owners, but to control owners who are accountable for implementing and maintaining the controls4. Information security governance is not based on an external security framework, but on the organization's own objectives, risk appetite, and compliance requirements. References = 1: CISM Review Manual (Digital Version), page 3 2:
CISM Review Manual (Digital Version), page 4 3: CISM Review Manual (Digital Version), page 5 4: CISM Review Manual (Digital Version), page 14 : CISM Review Manual (Digital Version), page 16

NEW QUESTION: 144
下列哪一項對組織的資訊安全策略影響最大？
A. 組織的風險承受能力
B. 組織結構
C. 業界安全標準
D. 資訊安全意識
Answer: (SHOW ANSWER)
An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives.
Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.
The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.
An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission,

vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION: 145
從硬碟執行取證資料擷取時建立並外部儲存磁碟雜湊口的主要原因是：
A. 在分析過程中驗證機密性。
B. 發生意外變更時恢復原始資料。
C. 在分析過程中驗證完整性。
D. 在媒體發生故障時提供備份。
Answer: (SHOW ANSWER)
The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD-ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital evidence123 References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532: Guide to Computer Forensics and Investigations Fourth Edition, page 4-103:
Forensic disk acquisition over the network, Andrea Fortuna, 2018.
The main purpose of creating and storing an external disk hash value when performing forensic data acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

NEW QUESTION: 146
下列何者最能指導資訊安全計畫的開發與維護？
A. 業務影響評估
B. 全面的風險登記冊
C. 已建立的風險評估流程
D. 組織的風險偏好
Answer: (SHOW ANSWER)
According to the CISM Manual, the organization's risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives1. The organization's risk appetite should guide the development and maintenance of an information security program, as it determines the level of security controls, resources, and activities that are needed to protect the organization's assets and operations1.
The CISM Manual states that "the information security program should be aligned with the organization's risk appetite, which reflects its tolerance for risk and its strategic objectives" (IR 8288A)1. The information security program should also consider other factors that influence the

organization's risk appetite, such as its mission, vision, values, culture, stakeholders, regulations, standards, guidelines, and best practices1.
The CISM Manual also provides guidance on how to develop and maintain an information security program based on the organization's risk appetite. It recommends using a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that affect the organization's information assets1. It also suggests using a framework or model that supports the development of an information security program based on the organization's risk appetite (e.g., ISO/IEC 27001)1.
References: 1: IR 8288A - Information Security Program Development | CSRC NIST

NEW QUESTION: 147
在安裝具有入侵防禦功能以阻止惡意活動的新防火牆幾個月後，安裝後不久就發現了透過防火牆進入的漏洞。透過實施防火牆可以更早偵測到此漏洞：
A. 上網控制。
B. 包過濾。
C. 應用程式感知。
D. 日誌監控。
Answer: (SHOW ANSWER)

NEW QUESTION: 148
對於組織的安全控制來口，下列哪一項應該是最口得關注的？
A. 有些控制措施的執行超出了可接受的範圍。
B. 尚未實施任何關鍵控制指標 (KCI)。
C. 控制權所有權尚未更新。
D. 控制差距分析已過時。
Answer: (SHOW ANSWER)
Key Control Indicators (KCIs) are essential to measuring the effectiveness and performance of security controls. Without them:
The organization cannot assess if controls are working as intended
It's difficult to demonstrate due diligence
Risks may go unnoticed
While other answers point to operational concerns, the complete absence of KCIs presents a critical governance gap that compromises the organization's ability to monitor and manage control health.
"KCIs provide actionable metrics that support proactive control management and are fundamental to governance and assurance."
- CISM Review Manual 15th Edition, Chapter 1: Governance Metrics and Reporting*

NEW QUESTION: 149
下列哪一項是實施組織範圍口的安全意識計畫的最大好處？

A. 安全性策略提升。
B. 報告的安全事件較少。
C. 安全行為有改善。
D. 偵測到更多安全事件。
Answer: (SHOW ANSWER)
The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.
The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms. Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208. CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.
The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal, Volume 1,
2019, 1.

NEW QUESTION: 150
下列哪一項是在安全操作中使用 AI 工具的最大好處？
A. 快速偵測並回應威脅
B. 優先漏洞
C. 減少修補系統所需的時間和精力
D. 定義的風險承受能力
Answer: (SHOW ANSWER)

AI-driven tools enable real-time analysis, anomaly detection, and automated response, drastically reducing the time to identify and respond to threats. This capability is particularly effective against advanced persistent threats (APTs) and zero-day exploits.
"AI tools enhance security operations by enabling rapid threat detection and incident response, often before traditional tools can react."
- CISM Review Manual 15th Edition, Chapter 4: Security Operations and Threat Intelligence*
Other benefits (e.g., prioritization or patching) are secondary compared to the speed and precision of AI-based threat response.

NEW QUESTION: 151
當確定風險影響不重大且可能性很低時，下列何者是最適當的風險因應措施？
A. 避免
B. 接受
C. 轉移
D. 緩解
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 152
財務部門主管決定外包該組織的預算應用程序，並已確定潛在的提供者。IN 資安經理應先口動下列哪一項操作？
A. 確定新解決方案所需的安全控制
B. 審口提供者的災難復原計畫 (DRP)
C. 取得服務提供者託管環境的審核報告
D. 協調組織的角色和服務提供者的統計資料。
Answer: (SHOW ANSWER)
Before outsourcing any application or service, an information security manager should first determine the required security controls for the new solution, based on the organization's risk appetite, security policies and standards, and regulatory requirements. This will help to evaluate and select the most suitable provider, as well as to define the security roles and responsibilities, service level agreements (SLAs), and audit requirements. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 153
當外包事件回應功能時，下列何者最能讓組織滿足事件回應要求？
A. 需要全面的回應應用程式和工具
B. 包含服務等級協定 (SLA) 中的回應時間
C. 在服務等級協定 (SLA) 中加入稽核權條款
D. 與知名事件回應提供者簽約
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
在製定資訊安全政策時讓各個業務部門的利害關係人參與的主要原因是什麼？
A. 分擔解決安全漏洞的責任
B. 獲得整個組織對政策的接受
C. 減少 IT 部門的工作量
D. 降低政策制定的整體成本
Answer: (SHOW ANSWER)
Involving stakeholders from various business units promotes buy-in, relevance, and adherence. When users feel they've had input in shaping the policy, they're more likely to support and follow it.
Stakeholders also provide insights into business processes that help ensure policies are practical and tailored.
This collaboration enhances organizational alignment and ensures policies do not create unintended operational friction.
"Stakeholder involvement is key to ensuring that policies are practical, aligned with operations, and accepted throughout the organization."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Policy Development and Implementation*

NEW QUESTION: 155
下列哪一項是網路事件回應遏制階段最適當的行動？
A. 隔離受影響的系統以防止損害蔓延
B. 確定事件的最終根本原因
C. 緩解被利用的漏洞以防止未來發生事故
D. 從網路中刪除該事件的所有實例
Answer: (SHOW ANSWER)
The containment phase focuses on limiting the scope of the incident. Isolating affected systems immediately helps prevent propagation and further compromise.
"During the containment phase, isolating compromised systems is a key tactic to minimize further impact and enable safe recovery."
- CISM Review Manual 15th Edition, Chapter 4: Incident Response Life Cycle, Section: Containment Strategies*

NEW QUESTION: 156
在為新的雲端服務設計安全控制時，下列哪一項最重要？
A. 根據相關風險評估不同類型的部署模型
B. 了解將資源移轉到雲端的業務和 IT 策略
C. 定義事件回應策略以保護現場和雲端應用程式之間移動的數據
D. 執行業務影響分析 (BIA) 以收集制定恢復策略所需的信息
Answer: (SHOW ANSWER)
The most important factor when designing security controls for new cloud-based services is to understand the business and IT strategy for moving resources to the cloud. This will help to align the security controls with the business objectives, requirements, and risks, and to select the appropriate cloud service delivery and deployment models. The security controls should also be based on the shared responsibility model, which defines the roles and responsibilities of the cloud service provider and the cloud customer in ensuring the security of the cloud environment. Evaluating different types of deployment models, defining an incident response policy, and performing a business impact analysis are also important activities, but they should be done after understanding the business and IT strategy.
References = CISM Review Manual, 16th Edition eBook1, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 141-142.

NEW QUESTION: 157
從成功的惡意軟體攻擊中恢復後，惡意軟體的實例會繼續被發現。哪個階段的事件回應不成功？
A. 根除
B恢復
B. 經驗教訓回顧
C. 事件聲明
Answer: (SHOW ANSWER)
Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.
References:
* https://www.securitymetrics.com/blog/6-phases-incident-response-plan
* https://www.atlassian.com/incident-management/incident-response
* https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

NEW QUESTION: 158
在建立事件回應計畫時，建立安全事件的明確定義的主要好處是它有助於：
A. 對利害關係人的事件回應流程

B. 為事件回應團隊提供足⼝的人員和訓練。
C. 制定有效的升級和回應程序。
D. 使桌面測試更有效。
Answer: (SHOW ANSWER)
The primary benefit of establishing a clear definition of a security incident is that it helps to develop effective escalation and response procedures. A security incident is an event or an attempt that disrupts or threatens the normal operations, security, or privacy of an organization's information or systems1. A clear definition of a security in-cident helps to:
*Distinguish between normal and abnormal events, and between security-relevant and non-security-relevant events
*Determine the severity and impact of an incident, and the appropriate level of response
*Assign roles and responsibilities for incident detection, reporting, analysis, containment, eradication, recovery, and post-incident activities
*Establish criteria and thresholds for escalating incidents to higher authorities or external parties
*Define the communication channels and protocols for incident notification and coordina-tion
*Document the incident response process and procedures in a formal plan According to NIST, a clear definition of a security incident is one of the key compo-nents of an effective incident response capability2. The other options are not the prima-ry benefits of establishing a clear definition of a security incident. Communicating the incident response process to stakeholders is important, but it is not the main purpose of defining a security incident. Adequately staffing and training incident response teams is essential, but it depends on other factors besides defining a security inci-dent. Making tabletop testing more effective is a possible outcome, but not a direct benefit of defining a security incident. References: 2: NIST SP
800-61 Rev. 2 Computer Security Incident Handling Guide 1: NIST Glossary - Security Incident : What is a securi-ty incident? - TechTarget : 10 types of security incidents and how to handle them - TechTarget : 45 CFR § 164.304 - Definitions - Electronic Code of Federal Regulations

NEW QUESTION: 159
下列何者最能讓組織持續評估資訊安全風險態勢？
A. 定期檢討風險登記冊
B. 關鍵風險指標 (KRI)
C. 遵守⼝業法規
D. 高階主管的支持程度
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
為了克服安全是業務活動障礙的觀念，資訊安全經理必須：
A. 依靠高階管理層來加強安全性。
B. 提升安全的相關性與貢獻。
C. 專注於合規性。

D. 重申安全的必要性。

Answer: (SHOW ANSWER)

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security to the organization's goals and objectives. Security is not only a technical function, but also a business enabler that supports the organization's strategy, vision, and mission. By promoting the relevance and contribution of security, the information security manager can demonstrate the value and benefits of security to the stakeholders, such as increasing customer trust, enhancing reputation, reducing costs, improving efficiency, and complying with regulations. Promoting the relevance and contribution of security can also help the information security manager to build relationships and partnerships with the business units, and to align the security program with the business needs and expectations. Promoting the relevance and contribution of security can also help the information security manager to foster a positive security culture and awareness within the organization, and to encourage the adoption and support of security policies and practices.

The other options are not the best ways to overcome the perception that security is a hindrance to business activities. Relying on senior management to enforce security is not the best way, because it may create a sense of coercion and resentment among the employees, and may undermine the credibility and authority of the information security manager. Focusing on compliance is not the best way, because it may create a false sense of security and satisfaction, and may neglect the other aspects and dimensions of security, such as risk management, value creation, and innovation. Reiterating the necessity of security is not the best way, because it may not address the root causes and factors of the negative perception, and may not provide sufficient evidence and justification for the security investments and decisions. References = CISM Review Manual,

16th Edition, ISACA, 2020, pp. 13-14, 23-241; CISM Online Review Course, Domain 1: Information Security Governance, Module 1: Information Security Governance Overview, ISACA2

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security. By demonstrating the value that security brings to the organization, including protecting assets and supporting business objectives, the information security manager can help to change the perception of security from a hindrance to a critical component of business success.

Relying on senior management to enforce security, focusing on compliance, and reiterating the necessity of security are all important elements of a comprehensive security program, but they do not directly address the perception that security is a hindrance to business activities. By promoting the relevance and contribution of security, the information security manager can help to align security with the overall goals and objectives of the organization, and foster a culture that values and supports security initiatives.

NEW QUESTION: 161

在提出資訊安全策略時，為了獲得高階領導的支持，下列哪一項最重要？

A. 此策略符合管理階層可接受的風險水準。

B. 此策略解決了無效的資訊安全控制問題。
C. 此策略符合口業基準和標準。
D. 此策略涉及組織成熟度和威脅環境。
Answer: (SHOW ANSWER)
The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat environment is not a very important factor because it does not indicate how the strategy will advance or adapt the organization's security posture or resilience. References: https://www.isaca.org/resources /isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems https://www.isaca. org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and- objectives

NEW QUESTION: 162
多個關鍵系統已被惡意軟體入侵。下列哪一項是根除此事件的最佳策略？
A. 執行惡意軟體掃描
B. 重新建構系統
C. 阻止對受影響系統的訪問
D. 執行漏洞評估
Answer: (SHOW ANSWER)
Reimaging the systems (B) is the most reliable method to eradicate malware because it ensures complete removal of malicious code, including hidden persistence mechanisms. Malware scanning (A) may miss advanced threats, while blocking access (C) is a containment action, not eradication. Vulnerability assessments (D) help identify weaknesses but do not remove existing malware. CISM incident management guidance prioritizes thorough eradication to prevent reinfection and restore system integrity.
References: ISACA CISM Review Manual (Incident management-eradication strategies); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 163
下列哪一項最能顯示組織擁有成熟的資訊安全文化？
A. 所有員工都必須接受資訊安全訓練。

B. 記錄並傳達組織的資訊安全策略。
C. 首席資訊安全長 (CISO) 定期與董事會互動。
D. 員工在做決策時始終考慮風險。
Answer: (SHOW ANSWER)
The BEST indication that an organization has a mature information security culture is when its staff consistently consider risk in making decisions. When an organization's staff understands the risks associated with their actions and are empowered to make risk-informed decisions, it indicates that the organization has a mature information security culture.
According to the Certified Information Security Manager (CISM) Study Manual, "A mature information security culture exists when the people within the organization understand and appreciate the risks associated with information and technology and when they take steps to manage those risks on a daily basis." While information security training, documented information security policies, and regular interaction between the chief information security officer (CISO) and the board are all important components of a mature information security culture, they are not sufficient on their own. It is only when staff consistently consider risk in making decisions that an organization's information security culture can be considered mature.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 151-152.

NEW QUESTION: 164
下列哪一項最能幫助使用者從勒索軟體或惡意軟體攻擊中復原？
A. 事件回應計劃
B. 頻繁的系統備份
C. 定期防毒更新
D. 最終使用者意識培訓
Answer: (SHOW ANSWER)
Frequent system backups (B) are the most effective means of recovery from ransomware or malware attacks. CISM emphasizes resilience and recoverability as critical aspects of incident management. While incident response plans (A), antivirus updates (C), and awareness training (D) help prevent or manage incidents, they do not guarantee restoration of data or systems. Reliable, tested backups allow organizations to restore operations without paying ransoms or suffering permanent data loss.
References: ISACA CISM Review Manual (Incident management-recovery and resilience); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 165
下列哪一項是加強事件回應團隊訓練的最佳方法？
A. 執行事件後檢討。
B. 建立事件關鍵績效指標 (KPI)。
C. 與組織單位進行訪談。

D. 參與緊急應變活動。

Answer: (SHOW ANSWER)

Performing post-incident reviews is the best way to enhance training for incident response teams because it allows them to identify the strengths and weaknesses of their response, learn from the lessons and best practices, and implement corrective actions and improvement plans for future incidents. Post-incident reviews also help to evaluate the effectiveness and efficiency of the incident response process and procedures, and to update them as needed.

References: The CISM Review Manual 2023 states that "post-incident reviews are an essential part of the incident response process" and that "they provide an opportunity to assess the performance of the incident response team, identify areas for improvement, and document lessons learned and best practices" (p. 191).

The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Performing post-incident reviews is the best way to enhance training for incident response teams, as it enables them to learn from their experience and improve their skills and knowledge" (p. 97).

NEW QUESTION: 166

下列哪份文件應包含服務恢復的初始優先順序？

A. IT 風險分析

B. 威脅評估

C. 業務影響分析 (BIA)

D. 業務流程圖

Answer: (SHOW ANSWER)

A business impact analysis (BIA) is the document that should contain the initial priori-tization of recovery of services. A BIA is a process of identifying and analyzing the po-tential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:

*Identifying the critical business functions and processes that support the organization's mission and objectives.

*Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.

*Assessing the potential impacts of disruptions to each function or process, such as finan-cial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatis-faction, etc.

*Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.

*Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.

A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or re-covery of critical business functions and processes in the event of a disruption2. The other options are not documents that should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3.
A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes. References: 1:
Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process map-ping - Wikipedia

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 167
事件回應團隊由一群經驗豐富的人員組成，在第一次演習中哪種類型的演習對團隊最有利？
A. 紅隊練習
B. 黑盒滲透測試
C. 災難復原練習
D. 桌上練習
Answer: (SHOW ANSWER)
= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low- cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills,

and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.
A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A disaster recovery exercise © is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high- risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

NEW QUESTION: 168
下列何者最能實現風險和控制所有權的分配？
A. 與業界認可的控制框架保持一致
B. 採用風險管理框架
C. 獲得高階管理層的支持
D. 制定資訊安全策略
Answer: C (LEAVE A REPLY)
Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their

roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.
References:
* https://www.protechtgroup.com/en-au/blog/risk-control-management
* https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_risk_ownership_right.ashx
* https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

NEW QUESTION: 169
下列哪一項是防止口部威脅的最佳方法？
A. 實施嚴格的安全性原則和密碼控制。
B. 進行全組織範圍的安全意識訓練。
C. 對所有存取活動實施日誌記錄。
D. 強制職責分離與最小特權存取。
Answer: (SHOW ANSWER)

NEW QUESTION: 170
在以下情況中，如果第三方提供者發生資訊安全事件，誰對資料遺失負責？
A. 資訊安全經理
B. 託管資料的服務供應商
C. 事件回應團隊
D. 業務資料擁有者
Answer: D (LEAVE A REPLY)
The business data owner is accountable for data loss in the event of an information security incident at a third- party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third- party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan.
References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and- custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident- response-lessons-learned

NEW QUESTION: 171

將事件分類標準納入事件回應計畫的最大好處是什麼？
A. 監控和控制事件管理成本的能力
B. 更清楚了解中斷的影響
C. 有效保護資訊資口
D. 恢復資源的最佳化分配
Answer: (SHOW ANSWER)
The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

NEW QUESTION: 172
高可用性系統中發現了新的風險。最佳處理方案是：
A. 執行緩解控制的成本效益分析
B. 建議企業主接受風險
C. 制定並實施計劃以減輕已識別的風險
D. 評估並確定已識別風險的優先級
Answer: (SHOW ANSWER)
The best first step is to evaluate and prioritize the risk to determine the appropriate treatment strategy before implementing mitigation.
"Once risks are identified, they should be evaluated and prioritized to determine the best response (mitigation, transfer, acceptance, or avoidance)."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*
ISACA practice questions confirm the need for evaluation and prioritization before taking further action.

NEW QUESTION: 173
下列哪一項是幫助確保資訊安全計畫與組織目標一致的最佳方法？
A. 建立資訊安全指導委員會。
B. 採用以流程為基礎的方法進行資訊資口分類。
C. 利用業界認可的風險管理架構。
D. 為董事會高階主管提供安全意識培訓。
Answer: (SHOW ANSWER)
The best way to help ensure alignment of the information security program with organizational objectives is A: Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by:

Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators Allocating and prioritizing the resources and budget for information security initiatives and projects Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

NEW QUESTION: 174
事件管理團隊收到可疑安全事件的警報。在將可疑事件歸類為安全事件之前，安全經理最重要的是：
A. 通知業務流程擁有者。
B. 遵循業務連續性計劃 (BCP)。
C. 進行事件取證分析。
D. 遵循事件回應計畫。
Answer: (SHOW ANSWER)
= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =
* 1: CISM Review Manual 15th Edition, page 199-2004
* 2: CISM Practice Quiz, question 1011
* 3: Computer Security Incident Handling Guide5, page 2-3

NEW QUESTION: 175
下列哪一項是製定有效資訊安全策略最重要的投入？
A. 業務流程與需求
B. 風險與業務影響評估
C. 明確定義的安全性策略和程序
D. 目前與所需的安全狀態
Answer: (SHOW ANSWER)

NEW QUESTION: 176
在企業中部署自帶裝置 (BYOD) 行動程式時，下列哪一項是資訊安全經理面臨的主要挑戰？
A. 行動應用程式控制
B. 裝置安全性不一致
C. 設定管理
D. 最終使用者接受度
Answer: (SHOW ANSWER)
Inconsistent device security is the primary challenge for an information security manager when deploying a bring your own device (BYOD) mobile program in an enterprise because it increases the risk of data breaches and compromises. A BYOD mobile program allows employees to use their personal devices, such as smartphones, tablets, or laptops, to access the organization's network, applications, and data. However, personal devices may have different operating systems, versions, configurations, and security settings than the organization's standard devices. Moreover, personal devices may not be updated regularly, may have unauthorized or malicious apps installed, or may not have adequate protection against malware or theft.
Inconsistent device security makes it difficult for the information security manager to enforce and monitor the security policies and controls across all devices, as well as to ensure compliance with the regulatory requirements for data privacy and security. Therefore, inconsistent device security is the correct answer.
References:
https://simplemdm.com/blog/challenges-of-bring-your-own-device-byod-policy/
https://www.timedoctor.com/blog/byod-pros-and-cons/
https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf

NEW QUESTION: 177
一位金融公司高層對最近不斷增加的網路攻擊感到擔憂，需要採取行動降低風險。組織最好的回應方式是：
A. 增加事件回應團隊的預算和人員配置水準。
B. 實施入侵偵測系統（IDS）。
C. 重新驗證風險並將其降低至可接受的水平。
D. 測試業務連續性計劃 (BCP)。
Answer: (SHOW ANSWER)
The best response for the organization to reduce risk from increasing cyberattacks is to revalidate and mitigate risks to an acceptable level. This means that the organization should review its current risk profile, identify any new or emerging threats, vulnerabilities, or impacts, and evaluate the effectiveness of its existing controls and countermeasures. Based on this analysis, the organization should implement appropriate risk treatment strategies, such as avoiding, transferring, accepting, or reducing the risks, to achieve its desired risk appetite and tolerance. The organization should also monitor and review the risk situation and the implemented controls

on a regular basis, and update its risk management plan accordingly. This approach is consistent with the ISACA Risk IT Framework, which provides guidance on how to align IT risk management with business objectives and value12.
The other options are not the best responses because they are either too narrow or too reactive. Increasing budget and staffing levels for the incident response team may improve the organization's ability to respond to and recover from cyberattacks, but it does not address the root causes or the prevention of the attacks.
Implementing an intrusion detection system (IDS) may enhance the organization's detection and analysis capabilities, but it does not guarantee the protection or mitigation of the attacks. Testing the business continuity plan (BCP) may verify the organization's readiness and resilience to continue its critical operations in the event of a cyberattack, but it does not reduce the likelihood or the impact of the attack. References = Risk IT Framework 1 CISM Review Manual, 16th Edition | Print | English 2, Chapter 3: Information Risk Management, pages 97-98, 103-104, 107-108, 111-112.

NEW QUESTION: 178
在規劃與業務相關的資訊安全計畫時，下列哪些來源最有用？
A. 安全風險登記冊
B. 資訊安全政策
C. 業務影響分析 (BIA)
D. 企業架構 (EA)
Answer: (SHOW ANSWER)
A business-aligned information security program is one that supports the organization's business objectives and aligns the information security strategy with the business functions. A business impact analysis (BIA) is a process that identifies the critical business processes, assets, and functions of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA helps to prioritize the information security requirements and controls that are needed to protect the organization's critical assets and functions from various threats and risks. Therefore, a BIA is one of the most useful sources when planning a business-aligned information security program. References = CISM Review Manual 15th Edition, page 254; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 229.
The most useful source when planning a business-aligned information security program is a Business Impact Analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to an organization's operations, and helps to identify the security controls and measures that should be implemented to reduce the impact of those disruptions. The BIA should include an assessment of the organization's information security posture, including its security policies, risk register, and enterprise architecture. With this information, organizations can develop an information security program that is aligned to the organization's business objectives.

NEW QUESTION: 179
業務連續性計劃（BCP）應包含：

A. 硬體和軟體清單。
B. 有關根除活動的資訊。
C. 口動標準。
D. 資料恢復程序。
Answer: (SHOW ANSWER)

NEW QUESTION: 180
下列哪一項是實施全面資訊安全管理系統的最佳理由？
A. 確保與組織策略持續保持一致
B. 獲得高階管理層對資訊安全計畫的支持
C. 支持關鍵風險指標 (KRI) 的識別
D. 促進遵守外部監理要求
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition, the primary objective of an information security management system (ISMS) is to align the information security strategy with the business strategy and ensure that information security objectives are consistent with the business objectives1. This helps the organization to achieve its goals and protect its information assets from threats and risks.
References = 1: CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, page 11.

NEW QUESTION: 181
一個組織正計劃外包其災難復原活動的執行。外包協議中包含下列哪一項最重要？
A. 定義何時應宣布災難
B. 定期測試備份的要求
C. 復原時間目標 (RTO)
D. 災難復原溝通計劃
Answer: (SHOW ANSWER)
The most important thing to include in the outsourcing agreement for disaster recovery activities is the recovery time objectives (RTOs). RTOs are the maximum acceptable time frames within which the critical business processes and information systems must be restored after a disaster or disruption. RTOs are based on the business impact analysis (BIA) and the risk assessment, and they reflect the business continuity requirements and expectations of the organization. By including the RTOs in the outsourcing agreement, the organization can ensure that the service provider is aware of and committed to meeting the agreed service levels and minimizing the downtime and losses in the event of a disaster. The other options are not as important as the RTOs, although they may be relevant and useful to include in the outsourcing agreement depending on the scope and nature of the disaster recovery services. References = CISM Review Manual 15th Edition, page 2471; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1033

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 182
一名員工點擊了電子郵件中的惡意鏈接，導致公司資料外洩 未來減輕這種風險的最佳方法是什麼？
A. 進行網路釣魚意識訓練。
B. 實作紀律程序。
C. 建立可接受的使用政策。
D. 評估並更新垃圾郵件過濾規則。
Answer: (SHOW ANSWER)
Phishing awareness training is the best way to mitigate the risk of employees clicking on malicious links in emails, as it educates them on how to recognize and avoid phishing attempts. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 179, section 4.3.2.2.

NEW QUESTION: 183
下列哪一項是記錄防火牆活動最重要的原因？
A. 指標報告
B. 入侵防禦
C. 事件調口
D. 防火牆調整
Answer: (SHOW ANSWER)

NEW QUESTION: 184
下列哪一項期望結果最能支持投資新安全計畫的決定？
A. 增強的安全監控和報告
B. 降低控制複雜性
C. 增強的威脅偵測能力
D. 降低組織風險
Answer: (SHOW ANSWER)
The reduction of organizational risk is the desired outcome that best supports a decision to invest in a new security initiative. The organizational risk is the level of exposure or uncertainty that the organization faces in achieving its objectives. The organizational risk is influenced by various

factors, such as the threat landscape, the vulnerability of the assets, the impact of the incidents, and the effectiveness of the controls. The information security manager should evaluate the organizational risk and propose security initiatives that can reduce the risk to an acceptable level. The security initiatives should be aligned with the business goals, the risk appetite, and the available resources of the organization. The security initiatives should also provide a positive return on investment (ROI) or value for money (VFM) for the organization. The reduction of organizational risk is the ultimate goal and benefit of any security initiative, as it enhances the security posture, performance, and resilience of the organization. Enhanced security monitoring and reporting, reduced control complexity, and enhanced threat detection capability are all possible outcomes of security initiatives, but they are not the best ones to support a decision to invest in a new security initiative. These outcomes are more specific and technical, and they may not directly relate to the business objectives or the risk appetite of the organization. These outcomes are also intermediate or enabling, rather than final or ultimate, as they may not necessarily lead to the reduction of organizational risk. For example, enhanced security monitoring and reporting may improve the visibility and awareness of the security status, but it may not prevent or mitigate the incidents. Reduced control complexity may simplify the security management and maintenance, but it may not address the emerging or evolving threats. Enhanced threat detection capability may increase the speed and accuracy of identifying the attacks, but it may not reduce the impact or the likelihood of the attacks. Therefore, the reduction of organizational risk is the best outcome to support a decision to invest in a new security initiative, as it demonstrates the value and effectiveness of the security initiative for the organization. References = CISM Review Manual 2023, page 40 1; CISM Practice Quiz 2

NEW QUESTION: 185
下列哪一個角色主要負責確保 IT 控制的運作有效性？
A. 風險所有者
B. 控制測試儀
C. IT 合規領導者
D. 資訊安全經理
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition1, the information security manager is responsible for ensuring that the information security program supports the organization's objectives and aligns with applicable laws and regulations. The information security manager is also responsible for overseeing the implementation and maintenance of effective IT controls, as well as monitoring and reporting on their performance.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 1, page 10.

NEW QUESTION: 186
下列哪一項是確保符合密碼標準的最佳方法？
A. 實現密碼同步軟體
B. 使用密碼破解軟體

C. 自動執行密碼語法規則
D. 使用者意識計劃
Answer: (SHOW ANSWER)
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.
Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for
2020 - Auth0 2: Password synchronization - Wikipedia 3:

NEW QUESTION: 187
事件回應團隊應在下列哪個階段記錄消除導致事件的威脅所需的操作？
A. 事件後審□
B. 根除
C. 遏制
D. 標識
Answer: (SHOW ANSWER)
The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2.
The other phases of incident response are:
Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.

Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.
Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2:
What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

NEW QUESTION: 188
在證明組織資訊安全計畫投資合理性的提案中包含下列哪一項是最重要的？
A. 漏洞掃描結果
B. 競爭對手基準分析
C. 之前的安全預算
D. 業務需求
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Justifying investments in information security requires aligning proposals with business objectives to gain management approval.
A). Vulnerability scan results: These provide technical insights but are insufficient for high-level justification.
B). Competitor benchmark analysis: While useful, this is less relevant than demonstrating direct alignment with organizational needs.
C). Previous security budget: Historical data may provide context but does not justify future needs.
D). Business requirements: This is the BEST answer because aligning security investments with business objectives demonstrates the value and necessity of the program to stakeholders.
Reference: CISM Job Practice Area 1 (Information Security Governance) focuses on aligning security initiatives with business goals to secure buy-in.

NEW QUESTION: 189
針對組織外部 Web 應用程式的滲透測試顯示了多個漏洞。下列哪一項是最令人擔憂的？
A. 滲透測試前未簽署參與規則表
B. 口部測試未發現漏洞
C. 漏洞是由於使用者驗收測試 (UAT) 不足所引起的
D. 其中一個漏洞的利用程式碼已公開
Answer: (SHOW ANSWER)
Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web

application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.
References:
* https://www.imperva.com/learn/application-security/penetration-testing/
* https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web- application-for-vulnerabilities/

NEW QUESTION: 190
資安經理發現安全風險沒有及時處理。下列哪一項
A. 定期提供有關風險當前狀態的最新資訊。
B. 定期重新執行風險分析。
C. 為每個風險分配風險負責人
D. 建立緩解控制措施來管理風險。
Answer: (SHOW ANSWER)
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References:
https://support.microsoft.com/en-us/office/secure- messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com /searchsecurity/definition/digital-signature

NEW QUESTION: 191
在呼叫中心，進行社會工程的最佳理由是：
A. 確定接受額外安全訓練的候選人。
B. 最小化成功攻擊的可能性。
C. 為資訊安全計畫取得資金。
D. 改進密碼策略。
Answer: (SHOW ANSWER)
The best reason to conduct a social engineering test in a call center is to identify candidates for additional security training because it helps to assess the level of awareness and skills of the call center staff in recognizing and resisting social engineering attacks, and provide them with the necessary training or education to improve their security posture. Minimizing the likelihood of successful attacks is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. Gaining funding for information security initiatives is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of

conducting such a test. Improving password policy is not a reason to conduct a social engineering test, but rather a possible outcome or benefit of conducting such a test. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration- testing

NEW QUESTION: 192
下列哪一項是成熟資訊安全計畫的最佳標誌？
A. 安全事件已妥善管理。
B. 安全支出低於預算。
C. 安全資源最佳化。
D. 安全審核結果減少。
Answer: (SHOW ANSWER)
A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human, financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

NEW QUESTION: 193
下列哪一項是製定戰略資訊安全決策的最佳方法？
A. 建立定期的資訊安全狀態報告。
B. 建立資訊安全指導委員會。
C. 建立業務部門安全工作小組。
D. 建立定期的高階管理層會議。
Answer: (SHOW ANSWER)
= According to the CISM Review Manual (Digital Version), page 9, an information security steering committee is a group of senior managers from different business units and functions who provide guidance and oversight for the information security program. An information security steering committee is the best approach to make strategic information security decisions because it can:
Ensure alignment of information security strategy with business objectives and risk appetite1 Facilitate communication and collaboration among different stakeholders and promote information security awareness and culture2 Provide direction and support for information security initiatives and projects3 Monitor and review the performance and effectiveness of the information security

program4 Resolve conflicts and issues related to information security policies and practices5 Establishing regular information security status reporting, business unit security working groups, and periodic senior management meetings are useful activities for information security management, but they are not sufficient to make strategic information security decisions without the involvement and guidance of an information security steering committee. References = 1: CISM Review Manual (Digital Version), page
9 2: 1 3: 2 4: 3 5: 4
An Information Security Steering Committee is a group of stakeholders responsible for providing governance and guidance to the organization on all matters related to information security. The committee provides oversight and guidance on security policies, strategies, and technology implementation. It also ensures that the organization is in compliance with relevant laws and regulations. Additionally, it serves as a forum for discussing security-related issues and ensures that security is taken into account when making strategic decisions.

NEW QUESTION: 194
下列誰的意見對於資訊安全戰略的發展最為重要？
A. 進程擁有者
B. 最終用口
C. 安全架構師。
D. 公司審計師
Answer: (SHOW ANSWER)
Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them.
Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information

security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to. Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. References = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

NEW QUESTION: 195
下列哪一項是建立風險意識文化的最佳方法？
A. 確保及時記錄和傳達威脅。
B. 定期測試安全控制的合規性。
C. 定期更改風險意識訊息。
D. 建立員工風險通報管道。
Answer: (SHOW ANSWER)

NEW QUESTION: 196
高階管理層希望徹底測試關鍵任務系統的災難復原計畫 (DRP)。
下列哪一項可以提供最可靠的結果？
A. 模擬測試
B. 結構化演練
C. 完全中斷測試
D. 平行測試
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 197
下列哪一項對於制定符合業務需求的經濟高效的資訊安全策略最有幫助？
A. 與業界同業進行基準比較
B. 資訊資口分類
C. 制定政策標準
D. 強制保留數據
Answer: (SHOW ANSWER)

NEW QUESTION: 198
在為計算設施選擇共用備用位置時，下列哪一項是最重要的考量因素？
A. 組織的風險承受能力
B. 組織的使命
C. 資源可用性
D. 事件回應團隊培訓
Answer: (SHOW ANSWER)
The organization's risk tolerance is the most important factor to consider when choosing a shared alternate location for computing facilities, as it determines the acceptable level of risk exposure and the required recovery time objective (RTO) for the organization. A shared alternate location is a facility that is used by multiple organizations for disaster recovery purposes, and it may have limited resources, availability, and security. Therefore, the organization must assess its risk tolerance and ensure that the shared alternate location can meet its recovery requirements and protect its information assets.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291; CISM Online Review Course, Module 4, Lesson 3, Topic 22; BCMpedia, Alternate Site3

NEW QUESTION: 199
當組織的關鍵第三方提供者之一遭遇資料外洩時，資訊安全經理應先採取下列哪項行動？
A. 通知公共關係官員。
B. 監控第三方的回應。
C. 呼叫事件回應計畫。
D. 通知客口違規狀況。
Answer: (SHOW ANSWER)
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

NEW QUESTION: 200
在收購的盡職調查階段，資訊安全經理最重要的行動方針是：
A. 執行風險評估
B. 執行差距分析
C. 檢討資訊安全政策
D. 檢討安全意識狀況
Answer: (SHOW ANSWER)

During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.
"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence
ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

NEW QUESTION: 201
下列哪一項是資訊安全經理在收到有關新的網路安全威脅的資訊後最重要的行動方針？
A. 更新日誌監控的關聯規則以偵測可能出現的威脅。
B. 檢視企業架構 (EA) 中是否有威脅所利用的漏洞。
C. 評估新威脅一旦成為現實對組織的影響。
D. 立即向高階管理層報告威脅，以便做出明智的決定。
Answer: (SHOW ANSWER)

NEW QUESTION: 202
新任命的資安經理被要求更新所有五年或更長時間不變的安全相關政策和程序。接下來該做什麼？
A. 根據最佳業務實務進行更新。
B. 對目前 IT 環境進行風險評估。
C. 了解目前的業務方向。
D. 清點並檢視目前的安全策略。
Answer: (SHOW ANSWER)
The next step for the information security manager should be to inventory and review the current security policies to understand the existing security requirements, controls, and gaps. This will help to identify the areas that need to be updated, revised, or replaced to align with the current business needs and objectives, as well as the legal and regulatory requirements. Updating the policies in accordance with the best business practices, performing a risk assessment of the current IT environment, or gaining an understanding of the current business direction are important activities, but they should be done after reviewing the current security policies.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Policies, Standards, Procedures and Guidelines, Subsection: Information Security Policies, Page 28.

NEW QUESTION: 203
在回應備受矚目的安全事件時，資安經理發現目前事件回應計畫存在一些缺陷。什麼時候是更新計畫的最佳時間？
A. 回應事件時

B. 桌面練習期間
C. 事件後審口期間
D. 風險重新評估後
Answer: (SHOW ANSWER)
During post-incident review is the best time to update the incident response plan after observing several deficiencies in the current plan while responding to a high-profile security incident. A post-incident review is a process of analyzing and evaluating the incident response activities, identifying the lessons learned, and documenting the recommendations and action items for improvement. Updating the incident response plan during post-incident review helps to ensure that the plan reflects the current best practices, addresses the gaps and weaknesses, and incorporates the feedback and suggestions from the incident response team and other stakeholders. Therefore, during post-incident review is the correct answer.
References:
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response- plan
https://www.integrify.com/blog/posts/incident-response-plan-need-an-update/

NEW QUESTION: 204
在商業提案中，潛在供應商提倡通過國際安全標準認證，作為其安全能力的衡量標準。
在依賴此認證之前，最重要的是資訊安全經理確認：
A. 使用目前國際標準來評估安全流程。
B. 認證在整個合約有效期間口保持有效。
C. 認證範圍與所提供的服務有關。
D. 認證可以擴展到涵蓋客口的業務。
Answer: (SHOW ANSWER)
Before relying on a vendor's certification for international security standards, such as ISO/IEC 27001, it is most important that the information security manager confirms that the certification scope is relevant to the service being offered. The certification scope defines the boundaries and applicability of the information security management system (ISMS) that the vendor has implemented and audited. The scope should cover the processes, activities, assets, and locations that are involved in delivering the service to the client. If the scope is too narrow, too broad, or not aligned with the service, the certification may not provide sufficient assurance of the vendor's security capability and performance.
The current international standard was used to assess security processes (A) is an important factor, but not the most important one. The information security manager should verify that the vendor's certification is based on the latest version of the standard, which reflects the current best practices and requirements for information security. However, the standard itself is generic and adaptable, and does not prescribe specific security controls or solutions. Therefore, the

certification does not guarantee that the vendor has implemented the most appropriate or effective security processes for the service being offered.
The certification will remain current through the life of the contract (B) is also an important factor, but not the most important one. The information security manager should ensure that the vendor's certification is valid and up to date, and that the vendor maintains its compliance with the standard throughout the contract period.
However, the certification is not a one-time event, but a continuous process that requires periodic surveillance audits and recertification every three years. Therefore, the certification does not ensure that the vendor's security capability and performance will remain consistent or satisfactory for the duration of the contract.
The certification can be extended to cover the client's business (D) is not a relevant factor, as the certification is specific to the vendor's ISMS and does not apply to the client's business. The information security manager should not rely on the vendor's certification to substitute or supplement the client's own security policies, standards, or controls. The information security manager should conduct a due diligence and risk assessment of the vendor, and establish a clear and comprehensive service level agreement (SLA) that defines the security roles, responsibilities, expectations, and metrics for both parties.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, page 142-1431

NEW QUESTION: 205
某部門報告稱，某項安全控制措施已失效。下列哪一項是資安經理的最佳應對措施？
A. 評估控制狀態。
B. 替換控制項。
C. 向管理階層報告失敗。
D. 檢口縱深防禦。
Answer: (SHOW ANSWER)
Upon learning a control is ineffective, the first action should be to assess the state of the control to verify the issue, determine its root cause, and assess the risk exposure. The CISM Review Manual emphasizes that assessment comes before taking further steps like replacement or escalation, as it informs appropriate, risk- based action.
Reference:ISACA CISM Review Manual, 16th Edition, Page 131-132, "Control Assessment and Continuous Improvement".

NEW QUESTION: 206
當業務案例符合以下條件時，使用業務案例來獲取資訊安全投資資金是最有效的：
A. 將資訊安全政策和標準轉化為業務需求。
B. 將投資與組織的策略計畫連結起來。
C. 根據組織策略重新調整資訊安全目標。

D. 以清楚的語言闡明管理階層的意圖和資訊安全指令。
Answer: (SHOW ANSWER)

NEW QUESTION: 207
一個組織正在製定提高安全意識的策略。在製定該策略時，下列何者最為重要？
A. 組織成熟度
B. 實施成本
C. 組織文化
D. 交付的技術解決方案
Answer: (SHOW ANSWER)
Organizational culture (C) is the most important factor when developing a security awareness strategy because culture determines how messages are received, accepted, and acted upon. CISM emphasizes that awareness programs must be tailored to the organization's values, behaviors, leadership tone, and risk mindset. Even well-funded programs or advanced delivery platforms will fail if they do not align with how employees think and work. Organizational maturity (A) and cost (B) influence scope and pacing, while technical delivery methods (D) are implementation details. A culture-aware approach ensures that security awareness drives behavioral change, which is the ultimate goal of awareness initiatives.
References: ISACA CISM Review Manual (Program management-security culture, awareness and training); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 208
下列哪一項是資訊安全治理職能的主要職責？
A. 管理資訊安全意識培訓
B. 定義安全性策略以支援組織計劃
C. 確保對使用新興技術的解決方案提供足口的支持
D. 就風險偏好和承受能力的最佳水準向高階管理層提供建議
Answer: (SHOW ANSWER)
Defining security strategies to support organizational programs is a primary responsibility of the information security governance function, as it involves providing strategic direction for security activities and ensuring that objectives are achieved. According to ISACA, information security governance is a subset of corporate governance that provides guidance for aligning information security with business objectives, managing information security risks, and using information resources responsibly12.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12

NEW QUESTION: 209
應定期執行業務影響分析 (BIA)，主要目的是：
A. 驗證環境變化的漏洞。

B. 分析資口的重要性。
C. 檢口是否符合規定。
D. 驗證控制的有效性。
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12.
According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations ©, as these are not the primary purposes of a BIA.
References: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

NEW QUESTION: 210
對組織而言，下列何者對於決定資訊安全治理的有效性最為重要？
A. 程序指標
B. 關鍵風險指標 (KRI)
C. 風險登記冊
D. 安全策略
Answer: (SHOW ANSWER)
Program metrics measure the effectiveness of governance processes and provide a basis for continuous improvement and informed decision-making.
"Metrics are essential for evaluating governance performance, demonstrating effectiveness, and identifying areas for improvement."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Monitoring and Metrics* ISACA's practice questions confirm that program metrics are key to evaluating governance effectiveness.

NEW QUESTION: 211
下列何者最能保證第三方託管服務提供者能口滿足可用性要求？
A. 審計權條款
B. 第三方的事件回應計劃
C. 服務等級協定 (SLA)
D. 第三方的業務連續性計劃 (BCP)
Answer: (SHOW ANSWER)

A Service Level Agreement (SLA) is the contractual document that specifies and guarantees the availability levels the third-party hosting provider must meet. It provides the clearest and most enforceable commitment to availability.
"SLAs establish measurable commitments that can be monitored and enforced, providing a high level of assurance that service availability will meet business requirements."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Outsourcing and Third-Party Management* ISACA's practice questions highlight SLAs as the most direct and reliable assurance for third-party service availability.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 212
一名事故處理人員正在準備硬碟的取證影像。為了證明該影像與原始影像完全一致，必須進行下列哪一項操作？
A. 對影像使用與原始影像相同的硬體。
B. 執行檔案數量的手動驗證。
C. 複製前加密並備份硬碟。
D. 對原始影像和影像進行數位雜湊處理。
Answer: (SHOW ANSWER)

NEW QUESTION: 213
為了有效管理組織的資訊安全風險，最重要的是：
A. 將風險管理職責分配給經驗豐富的顧問。
B. 定期辨識並修正新的系統漏洞。
C. 建立並傳達風險承受能力。
D. 針對同儕組織對風險情境進行基準測試。
Answer: C (LEAVE A REPLY)
To effectively manage an organization's information security risk, it is most important to establish and communicate risk tolerance, which is the level of risk that the organization is willing to accept or bear. By establishing and communicating risk tolerance, the organization can align its risk management strategy and objectives with its business goals and values, and ensure that the risk management activities and decisions are consistent and appropriate across the organization.

References: The CISM Review Manual 2023 defines risk tolerance as "the acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives" and states that
"the information security manager should assist the enterprise in establishing and communicating its risk tolerance, and ensure that the risk management process is aligned with the enterprise's risk tolerance" (p. 94).
The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Establish and communicate risk tolerance is the correct answer because it is the most important factor to effectively manage an organization's information security risk, as it helps to define the scope, direction, and priorities of the risk management process, and to ensure that the risk management activities and decisions are consistent and appropriate across the organization" (p. 29). Additionally, the article Risk Tolerance: The Forgotten Factor from the ISACA Journal 2019 states that "risk tolerance is the key factor that influences the risk management process and outcomes" and that "risk tolerance should be established and communicated by the organization's senior management and board of directors, and should reflect the organization's strategy, culture, and governance" (p. 1)1

NEW QUESTION: 214
在分配風險責任人時，最重要的考慮因素是確保責任人：
A. 對風險處理和相關控制活動有足口的了解。
B. 決策權與風險資源配置能力。
C. 有足口的時間有效監控和管理風險。
D. 支持決策的風險溝通和報告技能。
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation = The risk owner is the person or entity with the accountability and authority to manage a risk. The risk owner should have the decision-making authority and the ability to allocate resources for risk treatment and related control activities. The risk owner should also be responsible for monitoring and reporting on the risk, but these are not the most important considerations when assigning a risk owner. The risk owner may not have adequate knowledge of risk treatment and related control activities, but can delegate or consult with experts as needed. The risk owner should also have sufficient time for managing the risk effectively, but this is not a prerequisite for assigning a risk owner.
References =
* CISM Review Manual 15th Edition, page 76
* CISM Practice Quiz, question 4171

NEW QUESTION: 215
一家組織正在向零信任架構轉型。下列哪一項是資訊安全經理向董事會傳達此轉型影響的最佳方法？
A. 展示核心零信任邏輯元件的圖表，以協助視覺化架構變化

B. 在口部入口網站中總結培訓計劃和最終用口回饋，並將連結發送到公告板
C. 準備一份關於零信任實施的報告，其中包括狀態儀表板和時間表
D. 概述在降低風險和改變使用者體驗方面的業務影響
Answer: (SHOW ANSWER)
Senior leadership needs to understand how Zero Trust supports risk reduction and business needs.
Communicating the impact on risk reduction and user experience aligns security initiatives with business goals.
"Communicating how security initiatives support business objectives and risk reduction is critical for gaining senior management support."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment*

NEW QUESTION: 216
當需要實施對業務影響重大的新監管要求時，對於在嚴格監管的市場中運作的組織來口，最重要的考慮因素是什麼？
A. 建立補償控制
B. 進行差距分析
C. 聘請外部審計
D. 實施強而有力的監控控制
Answer: (SHOW ANSWER)

NEW QUESTION: 217
資訊安全經理在完成與服務提供者的合約談判中扮演什麼角色？
A. 對外包流程進行風險分析
B. 取得提供者的安全標準認證
C. 更新外包流程的安全標準
D. 確保包含定期審核的條款
Answer: (SHOW ANSWER)
The role of the information security manager in finalizing contract negotiations with service providers is to ensure that the outsourcing process is aligned with the organization's information security policies, standards, and objectives. One of the key aspects of this process is to perform a risk analysis on the outsourcing process, which involves identifying, assessing, and mitigating the potential threats and vulnerabilities that may arise from outsourcing activities. A risk analysis can help the information security manager to determine the appropriate level of security controls and requirements for the outsourced process, as well as to monitor and evaluate its performance and compliance. A risk analysis can also help to avoid or minimize legal, financial, reputational, or operational risks associated with outsourcing1. References = CISM Review Manual (Digital Version), Chapter 6: Information Security Program Management CISM Review Manual (Print Version), Chapter 6: Information Security Program Management

NEW QUESTION: 218
下列何者最能幫助組織有效管理新出現的網路風險？
A. 定期口部和外部審核
B. 明確的職責範圍
C. 足口的網路預算分配
D. 網路安全政策
Answer: (SHOW ANSWER)
Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 219
當需要連續正常運作時間時，哪種方法是評估備用處理站點有效性的最佳方法？
A. 平行測試
B. 全中斷測試
C. 模擬測試
D. 桌上型測試
Answer: (SHOW ANSWER)
A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required. A parallel test involves processing the same transactions or data at both the primary and the alternate site simultaneously, and comparing the results for accuracy and consistency. A parallel test can validate the functionality, performance, and reliability of the alternate site without disrupting the normal operations at the primary site. A parallel test can also identify and resolve any issues or discrepancies between the two sites before a real disaster occurs. A parallel test can provide a high level of assurance and confidence that the alternate site can support the organization's continuity requirements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP) Testing, page 1861; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 56, page 522.
A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required because it involves processing data at both the primary and alternate sites simultaneously without disrupting the normal operations1. A full interruption test would cause downtime and potential loss of data or revenue2. A simulation test would not provide

a realistic assessment of the alternate site's capabilities3. A tabletop test would only involve a discussion of the procedures and scenarios without actually testing the site4.
1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM - ISACA Certified Information Security Manager Exam Prep - NICCS 3: Prepare for the ISACA Certified Information Security Manager Exam: CISM ... 4: CISM: Certified Information Systems Manager | Official ISACA ... - NICCS

NEW QUESTION: 220
在評估新興風險的影響時，下列何者最具挑戰性？
A. 新興風險的複雜性
B. 與新興風險相關的數據不足
C. 過時的風險管理策略
D. 缺乏進行風險評估的資源
Answer: B (LEAVE A REPLY)
The greatest challenge in assessing emerging risk is insufficient data (B). Emerging risks, by definition, lack historical incidents, loss data, and proven impact metrics, making accurate assessment difficult. CISM emphasizes that uncertainty and data scarcity are inherent challenges in emerging risk management.
Complexity (A) and resource constraints (D) are common issues, but without sufficient data, even skilled analysts and mature processes struggle to estimate likelihood and impact. An outdated strategy (C) affects overall effectiveness but does not specifically hinder impact assessment as much as data scarcity does.
References: ISACA CISM Review Manual (Risk management-emerging risks, uncertainty, and assessment challenges); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 221
下列何者最有利於安全計畫的有效策略調整？
A. 業務策略定期更新
B. 程序和標準由部門主管批准。
C. 由第三方定期進行安全審核。
D. 組織單位對優先事項做出貢獻並達成一致
Answer: (SHOW ANSWER)
Organizational units contribute to and agree on priorities is the best way to facilitate effective strategic alignment of security initiatives because it ensures that the security initiatives are aligned with the business goals and objectives, supported by relevant stakeholders, and prioritized based on risk and value. The business strategy is periodically updated is not sufficient to facilitate effective strategic alignment of security initiatives because it does not involve collaboration or communication between different organizational units.
Procedures and standards are approved by department heads is not sufficient to facilitate effective strategic alignment of security initiatives because it does not reflect the strategic direction or vision of the organization.

Periodic security audits are conducted by a third-party is not sufficient to facilitate effective strategic alignment of security initiatives because it does not address the planning or implementation of security initiatives. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align- security-initiatives-with-business-goals-and-objectives https://www.isaca.org/resources/isaca-journal/issues /2015/volume-1/how-to-measure-the-effectiveness-of-information-security-governance

NEW QUESTION: 222
在下列人員中，誰最有能力對基於風險偏好的風險接受決策負責？
A. 資訊安全經理
B. 首席風險長 (CRO)
C. 資訊安全指導委員會
D. 風險負責人
Answer: (SHOW ANSWER)
The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.
References = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

NEW QUESTION: 223
資訊安全團隊必須獲得資訊安全指導委員會的批准才能實施金鑰控制。下列哪一項是協助委員會做出此決定的最重要的資訊？
A. 風險評估
B. 商業案例
C. 安全架構
D. IT 策略
Answer: (SHOW ANSWER)

NEW QUESTION: 224
對潛在網路重新配置的風險評估結果表明，敏感資料很可能受到損害。資訊安全經理的最佳行動方案是什麼？
A. 建議額外的網路分段。
B. 尋求獨立意見以確認調口結果。
C. 確定與現有法規的一致性。
D. 向主要利害關係人報告調口結果。

Answer: (SHOW ANSWER)
The information security manager's best course of action is to report the findings of the risk assessment to the key stakeholders, such as senior management, business owners, and regulators. This will ensure that the stakeholders are aware of the potential impact of the risk and can make informed decisions on how to address it. The other options are possible actions to take after reporting the findings, but they are not the best course of action in this scenario.
References = CISM Domain 2: Information Risk Management (IRM) [2022 update] (section: Information Risk Response) and CISM ITEM DEVELOPMENT GUIDE - ISACA (page 6, item example 2)

NEW QUESTION: 225
下列哪一項對於確定組織應實施哪些資訊安全策略最有幫助？
A. 風險評估
B. 業務影響分析 (BIA)
C. 漏洞評估
D. 業界最佳實踐
Answer: (SHOW ANSWER)
Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes1. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance2.
Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.
A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses3. A risk assessment helps to determine the following aspects of information security policies:
The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.
The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses.
The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.
The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.
The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations:

A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.
A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls.
Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.
References = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page
30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

NEW QUESTION: 226
下列哪一項是針對分散式阻斷服務 (DDoS) 攻擊的可行遏制策略？
A. 阻止攻擊者使用的 IP 位址
B. 重定向攻擊者的流量
C. 停用攻擊者利用的防火牆連接埠。
D. 關閉受影響的伺服器
Answer: (SHOW ANSWER)
Redirecting the attacker's traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker's traffic is a technique that involves changing the DNS settings or routing tables to send the attacker's traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker's behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server.

Redirecting the attacker's traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker's traffic is the correct answer.
References:
* https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation-strategy
* https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy
* https://www.cloudflare.com/learning/ddos/glossary/sinkholing/.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 227
組織口部報告了一起安全事件。資訊安全經理應何時聯絡資訊所有者？
A. 事件被遏制後
B. 事件緩解後
C. 事件確認後
D. 記錄潛在事件後
Answer: (SHOW ANSWER)
The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 228
下列哪一項是確保業務連續性計劃 (BCP) 最新的最佳方法？
A. 管理業務流程變更。
B. 定期更新業務影響分析 (BIA)。
C. 進行定期測試。
D. 口看並更新緊急聯絡人清單。
Answer: (SHOW ANSWER)
Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide

feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.
References: The CISM Review Manual 2023 states that "testing is a critical component of the BCP process" and that "testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations" (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update" (p. 98). Additionally, the article Business Continuity Planning: Testing an Organization's Plan from the ISACA Journal 2019 states that "testing is essential to ensure that the BCP is current and effective" and that "testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks" (p. 1)

NEW QUESTION: 229
管理層宣布收購一家新公司。母公司的資訊安全經理擔心，存取權限衝突可能會導致兩家公司整合期間關鍵資訊暴露。為了最好地解決這個問題，資訊安全經理應該：
A. 在進行收購整合時檢口存取權限。
B. 執行存取權限的風險評估。
C. 升級對管理存取權衝突的擔憂。
D. 實施一致的存取控制標準。
Answer: B (LEAVE A REPLY)
Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. References: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful post-merger integration

NEW QUESTION: 230
一個組織即將收購一個競爭對手的組織。在購買之前進行資訊安全盡職調查的主要原因是：
A. 確定安全風險。
B. 評估整合安全部門運作的能力。
C. 確保符合國際標準。
D. 評估安全策略和標準。
Answer: (SHOW ANSWER)
Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value, reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnair

NEW QUESTION: 231
在一次資訊安全審計中，發現IT人員在配置和管理IT系統時沒有遵循既定標準。下列哪一項是防止此類事件再次發生的最佳方法？
A. 提供年度資訊安全意識培訓
B. 定期進行漏洞掃描
C. 實施嚴格的變更控制流程
D. 更新配置基線
Answer: (SHOW ANSWER)
A strict change control process (C) is the most effective preventive measure because it embeds compliance with standards into the system lifecycle and operational workflow. If staff are deviating from configuration
/management standards, the core issue is often lack of enforced process controls: undocumented changes, rushed fixes, inconsistent approvals, or missing validation. Formal change management ensures changes are requested, risk-assessed, approved by authorized parties, tested, implemented, and reviewed, with traceability and accountability. Annual awareness training (A) helps general understanding but is weaker than a control that prevents and detects unauthorized deviations. Vulnerability scanning (B) is detective and may identify weaknesses after the fact, but it does not ensure standards are followed. Updating configuration baselines (D) is valuable, but without change control, baselines can still be bypassed. In CISM program management, the best answer typically emphasizes repeatable, auditable processes that reduce human error and enforce governance.
References: ISACA CISM Review Manual (Program management-control implementation, change control governance, assurance and compliance); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 232
下列哪一項提供了最好的證據來證明最近建立的資訊安全計畫是有效的？
A. 報告的事件數量增加
B. 定期傳達 IT 平衡計分卡。
C. 高階管理層報告的垃圾郵件減少。
D. 與 IT 事件相關的工單數量保持一致
Answer: (SHOW ANSWER)
The number of reported incidents has increased is the best evidence that a recently established information security program is effective because it indicates that the organization has improved its detection and reporting capabilities and has raised awareness among employees about security issues. Regular IT balanced scorecards are communicated is not a good evidence because it does not measure the actual performance or outcomes of the security program. Senior management has reported fewer junk emails is not a good evidence because it does not reflect the overall security posture or maturity of the organization. The number of tickets associated with IT incidents have stayed consistent is not a good evidence because it does not show any improvement or reduction in security incidents or risks. References:
https://www.isaca.org/resources/isaca- journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004
https://www.isaca.org/resources/isaca-journal/issues/2014/volume-6/how-to-measure-the-effectiveness-of- your-information-security-management-system

NEW QUESTION: 233
與業界同行製定資訊安全溝通計畫時，下列何者應該是重點考量？
A. 透過自動化流程降低與資訊共享相關的成本
B. 確保資訊口詳細，以便其他組織使用
C. 平衡資訊共享的好處和敏感資訊共享的弊端
D. 每當分享與事件相關的資訊時通知法律部門
Answer: (SHOW ANSWER)

NEW QUESTION: 234
下列哪一項應該是資訊安全計畫的主要結果？
A. 策略調整
B. 風險消除
C. 降低成本
D. 減少威脅
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, strategic alignment is the primary outcome of an information security program1. Strategic alignment means that the information security program supports and is tailored to the organization's objectives and

business strategy1. It also means that the information security program is aligned with other assurance functions, such as physical, human resources, quality, and IT1.
The CISM Review Manual (Digital Version) also states that strategic alignment is essential for achieving a competitive advantage, enhancing customer trust, reducing legal and regulatory risks, and improving organizational performance1. Strategic alignment requires effective communication and collaboration among all stakeholders, including senior management, information owners, information security managers, information security steering committees, and external partners1.
The CISM Exam Content Outline also covers the topic of strategic alignment in Domain 3 - Information Security Program Development and Management (33% exam weight)2. The subtopics include:
3.2.1 Information Security Strategy
3.2.2 Information Security Governance
3.2.3 Information Security Risk Management
3.2.4 Information Security Compliance
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 235
經驗豐富的資訊安全經理加入新組織，首先對所有關鍵IT 流程進行審核。下列哪一項有關漏洞管理計畫的調口結果最口得關注？
A. 未及時記錄並解決已識別的漏洞。
B. 已識別的漏洞不會在意識計劃中發布和傳達。
C. 漏洞由口部員工而非外部顧問識別。
D. 已識別的漏洞數量超過業界基準。
Answer: (SHOW ANSWER)

NEW QUESTION: 236
誰負責批准資訊安全治理框架？
A. 董事會
B. 首席資訊安全長 (CISO)
C. 企業風險委員會
D. 資訊長 (CIO)
Answer: (SHOW ANSWER)
The board of directors is ultimately responsible for the governance of the organization, including the approval of the information security governance framework and the oversight of its implementation and performance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 2: Establish and Maintain an Information Security Governance Framework, Section:
Roles and Responsibilities of Senior Management and the Board of Directors1

NEW QUESTION: 237

一家金融機構的管理階層接受了營運風險，導致關鍵監控流程暫時停用。對於這種情況，資安經理最關心的是下列哪一項？

A. 對合規風險的影響。

B. 無法確定短期影響。

C. 對風險文化的影響。

D. 偏離風險管理最佳實踐

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation = The impact on the risk culture is the greatest concern for the information security manager, because it reflects the attitude and behavior of the organization towards risk management. If management accepts an operational risk that compromises a critical monitoring process, it may indicate a lack of awareness, commitment, or accountability for risk management. This may erode the trust and confidence of the stakeholders, regulators, and customers, and expose the organization to further risks. The impact on compliance risk, the inability to determine short-term impact, and the deviation from risk management best practices are also important, but they are secondary to the impact on the risk culture.

References = CISM Review Manual 15th Edition, page 48. CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question ID 421.

NEW QUESTION: 238

一家組織發現其員工在識別和報告網路安全事件方面存在不足。儘管提供了培訓材料，但員工仍缺乏興趣。下列哪一項是資安經理的最佳行動方案？

A. 阻止網路訪問，直到安全意識培訓完成。

B. 進行企業網路安全風險評估。

C. 獲得關鍵利害關係人和領導階層的支持。

D. 發送一封電子郵件，要求對員工進行培訓。

Answer: C (LEAVE A REPLY)

Leadership support reinforces the importance of security awareness and motivates employees to engage with training.

"Security awareness programs are most effective when they have visible support from senior management, reinforcing their importance."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training*

NEW QUESTION: 239

事件後檢討的主要目標應該是：

A. 確定策略變更以防止再次發生。

B. 決定如何改善事件處理流程。

C. 確定事件對企業造成的成本。

D. 確定事件發生的原因。

Answer: (SHOW ANSWER)

The primary goal of a post-incident review is to identify areas for improvement in the incident handling process. The focus is on evaluating the effectiveness of incident response procedures, technical controls, communication channels, coordination among teams, documentation, and any other relevant aspects. The post- incident review should also provide recommendations for corrective actions, preventive measures, and lessons learned that can help reduce the likelihood and impact of future incidents12. References = CISM Review Manual 15th Edition, page 1251; CISM Item Development Guide, page 72

NEW QUESTION: 240

當資安經理得知某個業務部門正在繞過現有控制措施以提高營運效率時，他應該採取的第一步行動是什麼？

FreeCram.net

A. 向高階管理層報告不合規情況。

B. 評估不合規的風險。

C. 口動事件回應計畫。

D. 評估可能的補償控制。

Answer: B (LEAVE A REPLY)

Assessing the risk of noncompliance ensures that decisions are based on an understanding of the business impact and security implications.

"Before reporting or remediating, it is critical to assess the risk associated with the control bypass to make informed decisions."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment*

NEW QUESTION: 241

下列哪一項對勒索軟體事件後關鍵系統和資料的恢復提出了最大的挑戰？

A. 傳輸中的備份資料缺乏加密

B. 未定義或未記錄的備份保留策略

C. 備份作業的警報配置無效

D. 資料備份無法使用或損壞

Answer: (SHOW ANSWER)

A ransomware incident is a type of cyberattack that encrypts the victim's data and demands a ransom for its decryption. Ransomware can cause significant disruption and damage to critical systems and data, as well as financial losses and reputational harm. To recover from a ransomware incident, the organization needs to have reliable and accessible backups of its data, preferably in an encrypted format. However, if the backups are unavailable or corrupt, the organization will face a major challenge in restoring its data and operations. Therefore, option D is the most challenging factor for the recovery of critical systems and data following a ransomware incident. References = CISA MS-ISAC Ransomware Guide1, page 9; How to Write an Incident Response Plan for Ransomware Recovery2.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 242
更新密碼標準後，資訊安全經理會收到各種應用程式管理員的警告，他們支援的應用程式無法執行這些標準。資安經理的首要行動應該是：
A. 實施補償控制。
B. 評估更換應用程式的成本。
C. 確定潛在影響。
D. 重新評估標準。
Answer: (SHOW ANSWER)

NEW QUESTION: 243
最近的審計發現，組織的新使用者帳口設定不統一。下列哪一項對於資訊安全經理審口最重要？
A. 自動化控制
B. 安全性策略
C. 指南
D. 標準
Answer: (SHOW ANSWER)
Standards are the most important thing to review, as they define the specific and mandatory requirements for setting up new user accounts, such as the naming conventions, access rights, password policies, and expiration dates. Standards help to ensure consistency, security, and compliance across the organization's information systems and users. If the standards are not followed, the organization may face increased risks of unauthorized access, data breaches, or audit failures.
References = CISM Review Manual 2022, page 341; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.32; CISM 2020: IT Security Policies; Information Security Policy, Standards, and Guidelines

NEW QUESTION: 244
管理階層審口了已識別的風險並確定風險低於定義的風險偏好後，下列哪一項是最佳行動方案？
A. 接受
B. 避免
C. 轉移
D. 緩解

Answer: A (LEAVE A REPLY)
When a risk is determined to be below the organization's risk appetite, the most appropriate course of action is to formally accept the risk. Risk acceptance is a valid and cost-effective strategy when the impact and likelihood are within acceptable limits, and the cost of mitigation outweighs the potential loss.
"Risk acceptance is an appropriate response when the level of residual risk is within the organization's defined risk tolerance and appetite."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Avoidance, transfer, or mitigation may be overreactions that waste resources in this context.

NEW QUESTION: 245
及時宣布災難的主要目標是：
A. 確保業務管理階層參與復原過程。
B. 評估並修正災難復原過程的缺陷。
C. 保護重要的實體資口免於進一步損失。
D. 確保組織基本服務的連續性。
Answer: (SHOW ANSWER)
The primary objective of timely declaration of a disaster is to ensure the continuity of the organization's essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan (DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

NEW QUESTION: 246
在執行業務影響分析 (BIA) 時，誰應負責確定初始復原時間目標(RTO)？
A. 外部顧問
B. 資訊擁有者
C. 資訊安全經理
D. 業務連續性協調員
Answer: (SHOW ANSWER)
Information owners are responsible for determining the initial recovery time objective (RTO) for their information assets and processes, as they are the ones who understand the business requirements and impact of a disruption. An external consultant may assist in conducting the business impact analysis (BIA), but does not have the authority to decide the RTO. An information security manager may provide input on the security aspects of the RTO, but does not

have the business perspective to determine the RTO. A business continuity coordinator may facilitate the BIA process and ensure the alignment of the RTO with the business continuity plan, but does not have the ownership of the information assets and processes. References = CISM Review Manual 15th Edition, page 202.
When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the BIA and should be determined in cooperation with the information owners. The RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

NEW QUESTION: 247
為了優先回應事件，應先執行下列哪項操作？
A. 分類
B. 分析
C. 遏制
D. 升級
Answer: (SHOW ANSWER)

NEW QUESTION: 248
下列哪一項是辨識資訊安全環境變化最有效的方法？
A. 業務影響分析 (BIA)
B. 年度風險評估
C. 定期滲透測試
D. 持續監控
Answer: (SHOW ANSWER)
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

NEW QUESTION: 249
下列哪一項是記錄整個組織報告的資訊安全事件的最重要原因？
A. 評估組織的安全狀況。
B. 支持安全方面的商業投資。
C. 辨識未緩解的風險。
D. 防止事件再發生。

Answer: (SHOW ANSWER)

NEW QUESTION: 250

一個組織發現，處理即時視覺資料的伺服器可能容易受到勒索軟體攻擊的橫向移動階段的影響。下列哪一種控制措施最能緩解此漏洞？

Freecram.net

A. 網路分段

B. 資料遺失防護 (DLP)

C. 傳輸中的資料加密

D. 入侵偵測系統 (IDS)

Answer: (SHOW ANSWER)

Network segmentation is the most effective control to prevent lateral movement. In ransomware attacks, attackers often breach one endpoint and move laterally across the network to reach critical assets.

Segmentation limits this movement by isolating systems into different zones or subnets, thereby reducing the attack surface and preventing unauthorized internal traversal.

DLP and encryption are primarily focused on data protection, not internal network movement.

IDS can detect intrusions but does not prevent movement like segmentation does.

"Network segmentation limits the scope of access for compromised systems and is a key strategy in preventing lateral movement in an attack."

- CISM Review Manual 15th Edition, Chapter 3: Information Security Architecture, Section: Network Security* Real-world example: "In the NotPetya and WannaCry incidents, poor internal segmentation allowed malware to propagate rapidly."

NEW QUESTION: 251

下列何者最有利於及時有效地回應事件？

A. 呼叫事件回應計畫時通知利害關係人

B. 評估受損資口的風險

C. 將事件的嚴重程度進行分類

D. 將滲透測試結果納入事件回應計劃

Answer: (SHOW ANSWER)

NEW QUESTION: 252

下列哪一種方法是證明資訊安全計畫提供適當覆蓋範圍的最佳方法？

A. 安全風險分析

B. 差距評估

C. 成熟度評估

D. 漏洞掃描報告

Answer: (SHOW ANSWER)

A gap assessment is the best way to demonstrate that an information security program provides appropriate coverage, as it compares the current state of the information security program with the desired state based on the organization's objectives, policies, standards, and regulations. A

gap assessment can identify the strengths and weaknesses of the information security program, as well as the areas that need improvement or alignment.
A gap assessment can also provide recommendations and action plans to close the gaps and achieve the desired level of information security coverage.
The other options are not as good as a gap assessment, as they do not provide a comprehensive and holistic view of the information security coverage. Security risk analysis is a process to identify and evaluate the risks to the information assets and the impact of potential threats and vulnerabilities. It can help to prioritize and mitigate the risks, but it does not measure the compliance or performance of the information security program.
Maturity assessment is a process to measure the level of maturity of the information security program based on a predefined model or framework. It can help to benchmark and improve the information security program, but it does not account for the specific needs and expectations of the organization. Vulnerability scan report is a document that shows the results of a scan on the network or system to identify the existing or potential vulnerabilities. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1015.
CISM domain 3: Information security program development and management [2022 update], Infosec Certifications, 2.

NEW QUESTION: 253
一個組織正在實施資訊安全治理框架。為了向利害關係人傳達該計劃的有效性，最重要的是建立：
A. 控制自我評估 (CSA) 過程。
B. 自動向利害關係人報告。
C. 安全性策略的監控程序。
D. 每個里程碑的指標。
Answer: (SHOW ANSWER)
= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress, performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.
The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self- assessment (CSA) process is a technique to involve the staff in

assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.
CISM domain 1: Information security governance [Updated 2022], Infosec, 1.
Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

NEW QUESTION: 254
一個組織剛剛將其備份功能更新為新的基於雲端的解決方案。下列哪項測試能最有效地驗證此變更是否如預期運作？
A. 模擬測試
B. 平行測試
C. 桌上型測試
D. 黑盒測試
Answer: (SHOW ANSWER)

NEW QUESTION: 255
當選擇緩解風險處理方法時，下列哪一個角色負責有效實施所選的處理方法？
A. 風險所有者
B. 控制擁有者
C. 業務系統擁有者
D. 應用程式擁有者
Answer: (SHOW ANSWER)
The control owner is the individual accountable for implementing and managing specific controls that mitigate risks. While the risk owner is responsible for the overall risk and decision-making, it

is the control owner who ensures the selected mitigation is effectively implemented and maintained.
"The control owner is responsible for ensuring that the control is properly designed, implemented, and operating effectively."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment
ISACA practice questions stress this distinction: the control owner is tasked with the execution of mitigation strategies.

NEW QUESTION: 256
將惡意軟體事件分類時，應先執行下列哪一步？
A. 包含受影響的系統
B. 保留取證影像
C. 將備份與生口進行比較
D. 移除惡意軟體
Answer: (SHOW ANSWER)
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 257
下列哪一項是組織資訊安全狀態的最佳指標？
A. 入侵偵測日誌分析
B. 控制審核
C. 威脅分析
D. 滲透測試
Answer: (SHOW ANSWER)
A controls audit is the best indicator of an organization's information security status, as it provides an independent and objective assessment of the design, implementation, and effectiveness of the information security controls. A controls audit can also identify the strengths and weaknesses of

the information security program, as well as the compliance with the policies, standards, and regulations. A controls audit can cover various aspects of information security, such as governance, risk management, incident management, business continuity, and technical security. A controls audit can be conducted by internal or external auditors, depending on the scope, purpose, and frequency of the audit.
The other options are not as good as a controls audit, as they do not provide a comprehensive and holistic view of the information security status. Intrusion detection log analysis is a technique to monitor and analyze the network or system activities for signs of unauthorized or malicious access or attacks. It can help to detect and respond to security incidents, but it does not measure the overall performance or maturity of the information security program. Threat analysis is a process to identify and evaluate the potential sources, methods, and impacts of threats to the information assets. It can help to prioritize and mitigate the risks, but it does not verify the adequacy or functionality of the information security controls. Penetration test is a simulated attack on the network or system to evaluate the vulnerability and exploitability of the information security defenses. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1012.

NEW QUESTION: 258
下列哪一項對於在組織口建立 4 種強大的資訊安全文化最重要？
A. 整個組織口成熟的資訊安全意識培訓
B. 嚴格要求員工遵守組織安全政策
C. IT 環境的開發與營運中嵌入的安全控制
D. 高階管理層批准資訊安全政策
Answer: (SHOW ANSWER)
= Mature information security awareness training across the organization is the most important factor for building a robust information security culture, because it helps to educate and motivate the employees to understand and adopt the security policies, procedures, and best practices that are aligned with the organizational goals and values. Information security awareness training should be tailored to the specific roles, responsibilities, and needs of the employees, and should cover the relevant topics, such as:
The importance and value of information assets and the potential risks and threats to them The legal, regulatory, and contractual obligations and compliance requirements related to information security The organizational security policies, standards, and guidelines that define the expected and acceptable behaviors and actions regarding information security The security controls and tools that are implemented to protect the information assets and how to use them effectively and efficiently The security incidents and breaches that may occur and how to prevent, detect, report, and respond to them The security best practices and tips that can help to enhance the security

posture and culture of the organization Information security awareness training should be delivered through various methods and channels, such as:
Online courses, webinars, videos, podcasts, and quizzes that are accessible and interactive Classroom sessions, workshops, seminars, and simulations that are engaging and practical Posters, flyers, newsletters, emails, and social media that are informative and catchy Games, competitions, rewards, and recognition that are fun and incentivizing Information security awareness training should be conducted regularly and updated frequently, to ensure that the employees are aware of the latest security trends, challenges, and solutions, and that they can demonstrate their knowledge and skills in a consistent and effective manner.
Mature information security awareness training can help to create a positive and proactive security culture that fosters trust, collaboration, and innovation among the employees and the organization, and that supports the achievement of the strategic objectives and the mission and vision of the organization.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 144-146, 149-150.

NEW QUESTION: 259
實施標準安全配置的主要目標是什麼？
A. 保持靈活的方法來減輕不受支援的系統的潛在風險。
B. 最大限度地減少管理和監控不受支援的系統的營運負擔。
C. 控制漏洞並減少配置變更帶來的威脅。
D. 比較支援和不支援的系統之間的配置。
Answer: (SHOW ANSWER)
The primary objective of implementing standard security configurations is to control vulnerabilities and reduce threats from changed configurations. Standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices. By implementing standard security configurations, the organization can ensure that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected. This can help to prevent or mitigate potential security incidents caused by misconfigurations, unauthorized modifications, or malicious attacks.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should establish and implement standard security configurations for information systems and devices, and monitor and review the security configuration on a regular basis and take corrective actions when deviations or violations are detected" (p.
138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Control vulnerabilities and reduce threats from changed configurations is the correct answer because it is the primary objective of implementing standard security configurations, as it helps to maintain the security posture and functionality of information systems and devices, and to prevent or mitigate potential security incidents caused by

misconfigurations, unauthorized modifications, or malicious attacks" (p. 63). Additionally, the article Standard Security Configurations from the ISACA Journal 2017 states that "standard security configurations are the baseline settings and parameters that define the desired security level and functionality of information systems and devices" and that "standard security configurations can help to control vulnerabilities and reduce threats from changed configurations by ensuring that the information systems and devices are configured in a consistent and secure manner, and that any deviations or changes from the standard are detected and corrected" (p. 1)

NEW QUESTION: 260

下列何者最能顯示資訊安全治理架構已成功實施？

A. 框架協調口部和外部資源。

B. 此框架可讓安全流程與業界最佳實務保持一致。

C. 此架構協調安全組織口的管理和其他功能。

D. 該框架包括商業現成的安全解決方案。

Answer: A (LEAVE A REPLY)

The best indicator that an information security governance framework has been successfully implemented is A: The framework aligns internal and external resources. This is because the framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities.

The framework should ensure that the information security strategy, policies, and objectives are aligned with the business goals, stakeholder expectations, and regulatory requirements. The framework should also enable the effective allocation and coordination of internal and external resources, such as people, processes, technology, and finances, to support the information security program and its activities. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 49, page 14

NEW QUESTION: 261

資訊安全經理希望記錄詳細口明使用者工作站所需的最低安全控制的要求。下列哪一項資源最適合此目的？

A. 指南

B. 政策

C. 程式

D. 標準

Answer: (SHOW ANSWER)

Standards are detailed statements of the minimum requirements for hardware, software, or security configurations. They are used to define the minimum security controls required for user workstations. References = CISM Review Manual, 16th Edition, page 69.

NEW QUESTION: 262
下列哪一項對於確定組織業務職能的重要性最有幫助？
A. 災難復原計畫 (DRP)
B. 業務影響分析 (BIA)
C. 業務連續性計劃 (BCP)
D. 安全評估報告 $AR）
Answer: (SHOW ANSWER)
Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.
References:
* https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez
* https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business-continuity- Understanding-impact-criticality

NEW QUESTION: 263
下列哪一項是有效災難復原規劃流程的最佳指標？
A. 每次事件後都會進行事件後檢討。
B. 復原時間目標 (RTO) 比復原點目標 (RPO) 短。
C. 任何已宣布的災難都需要熱點站點。
D. 在整個災難復原過程中維護監管鏈。
Answer: (SHOW ANSWER)

NEW QUESTION: 264
一家全球性組織正在組建一支事件回應團隊。該組織希望讓總部隨時了解所有事件，並希望能□對廣泛分佈的事件做出統一的回應。下列哪一項最能支持這些目標？
A. 虛擬事件回應團隊
B. 分散式事件回應團隊
C. 外包事件回應團隊
D. 集中事件回應團隊
Answer: (SHOW ANSWER)
A centralized incident response team ensures consistent communication, coordination, and a unified approach to managing incidents across the organization.
"A centralized incident response team provides a consistent and coordinated approach to incident handling and ensures that management is kept informed."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Organization Models*

NEW QUESTION: 265
在製定資訊安全計畫的關鍵績效指標 (KPI) 時，下列哪一項是最重要的考量因素？
A. 與財務報告保持一致
B. 與業務計劃保持一致
C. 與口業框架保持一致
D. 與風險偏好保持一致
Answer: (SHOW ANSWER)
Explore
The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain - Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

NEW QUESTION: 266
下列哪一項是業務影響分析(BIA)的主要結果？
A. 簡化事件分類與實施事件回應程序
B. 技術安全控制與安全文化提升的預算分配
C. 確保符合行業特定法規並改善業務流程
D. 識別關鍵業務功能並決定復原工作的優先順序
Answer: (SHOW ANSWER)
The primary outcome of a BIA is the identification of critical business functions and prioritization of recovery efforts (D). CISM defines the BIA as the foundation for continuity and resilience planning, providing insight into impact, recovery priorities, and tolerable downtime. The other options represent secondary or unrelated benefits.
References: ISACA CISM Review Manual (Program management-BIA purpose and outcomes); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 267
下列哪一種設備放置在非軍事區 (DMZ) 會被視為最嚴重的暴露？
A. 郵件中繼伺服器
B. 資料庫伺服器
C. 應用程式伺服器
D. 代理伺服器
Answer: (SHOW ANSWER)

NEW QUESTION: 268
資訊安全經理正在向高階管理層報告風險登記冊中的未清項目。關於這些風險，下列哪一項對於溝通最重要？
A. 責任實體
B. 關鍵風險指標 (KRIS)
C. 補償控制
D. 潛在的業務影響
Answer: D (LEAVE A REPLY)
The most important information to communicate with regard to the open items from the risk register to senior management is the potential business impact of these risks. The potential business impact is the estimated consequence or loss that the organization may suffer if the risk materializes or occurs. The potential business impact can be expressed in quantitative or qualitative terms, such as financial, operational, reputational, legal, or strategic impact. Communicating the potential business impact of the open items from the risk register helps senior management to understand the severity and urgency of these risks, and to prioritize the risk response actions and resources accordingly. Communicating the potential business impact also helps senior management to align the risk management objectives and activities with the business objectives and strategies, and to ensure that the risk appetite and tolerance of the organization are respected and maintained.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Reporting, page 1012.

NEW QUESTION: 269
組織使用的安全標準已經過認證機構的重大修訂。希望維持其認證的組織將不再使用舊版的標準。下列哪一項應該是第一個行動方案？
A. 評估維持認證的成本。
B. 口看新標準對業務的適用性。
C. 修改政策以確保滿足新要求。
D. 向高階領導傳達新標準。
Answer: (SHOW ANSWER)

Reviewing the new standard for applicability to the business is the first course of action, as it helps to understand the changes, gaps, and impacts of the revision on the organization's security posture, compliance status, and business objectives. Evaluating the cost of maintaining the certification, modifying policies to ensure new requirements are covered, and communicating the new standard to senior leadership are important steps, but they should be done after reviewing the new standard for applicability to the business.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.2

NEW QUESTION: 270
事件分類對於評估下列哪一項最重要？
A. 適當的溝通管道
B. 所需資源的分配
C. 風險嚴重性和事件優先級
D. 回應和遏制要求
Answer: (SHOW ANSWER)
The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation.
The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence the allocation of resources, the response and containment requirements, and the communication channels, but they are not the primary purpose of categorization.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

NEW QUESTION: 271
某個組織發現了大量似乎未使用的舊資料。資訊安全經理接下來應該執行下列哪一項操作？
A. □□記錄保留政策。
B. 更新意識和培訓計畫。
C. 實作媒體清理程式。
D. □□備份和復原策略。
Answer: (SHOW ANSWER)
The next thing that the information security manager should do after identifying a large volume of old data that appears to be unused is to consult the record retention policy. The record retention policy is a document that defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes. By consulting the record retention policy, the information security manager can determine if the old data is still

required to be stored, archived, or disposed of, and how to do so in a secure and compliant manner.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 272
下列哪一項是評估與使用軟體即服務 (SaaS) 供應商相關的風險的最佳方法？
A. 驗證合約中是否包含資訊安全要求。
B. 向供應商請求客口參考。
C. 請供應商完成資訊安全問卷。
D. 檢視供應商獨立控制報告的結果。
Answer: (SHOW ANSWER)
Reviewing the results of the vendor's independent control reports is the best way to assess the risk associated with using a SaaS vendor because it provides an objective and reliable evaluation of the vendor's security controls and practices. Independent control reports, such as SOC 2 or ISO 27001, are conducted by third-party auditors who verify the vendor's compliance with industry standards and best practices. These reports can help the customer identify any gaps or

weaknesses in the vendor's security posture and determine the level of assurance and trust they can place on the vendor.
Verifying that information security requirements are included in the contract is a good practice, but it does not provide sufficient assurance that the vendor is actually meeting those requirements. The contract may also have limitations or exclusions that reduce the customer's rights or remedies in case of a breach or incident.
Requesting customer references from the vendor is not a reliable way to assess the risk associated with using a SaaS vendor because the vendor may only provide positive or biased references that do not reflect the true experience or satisfaction of the customers. Customer references may also not have the same security needs or expectations as the customer who is conducting the assessment.
Requiring vendors to complete information security questionnaires is a useful way to gather information about the vendor's security policies and procedures, but it does not provide enough evidence or verification that the vendor is actually implementing and maintaining those policies and procedures. Information security questionnaires are also subject to the vendor's self-reporting and interpretation, which may not be accurate or consistent. References = CISM Review Manual 15th Edition, page 144 SaaS Security Risk and Challenges - ISACA1 SaaS Security Checklist & Assessment Questionnaire | LeanIX2 Risk Assessment Guide for Microsoft Cloud3

NEW QUESTION: 273
當出現以下情況時，重新評估風險最為關鍵：
A. 抵制實施緩解控制措施。
B. 更新安全性報告的管理請求。
C. 安全性策略的變更。
D. 威脅情勢改變。
Answer: (SHOW ANSWER)
= Reevaluation of risk is a vital aspect of the risk management process that helps organizations to identify and analyze new or evolving threats, vulnerabilities, and impacts on their assets, and implement the necessary controls to mitigate them. Reevaluation of risk is most critical when there is a change in the threat landscape, which refers to the external and internal factors that influence the likelihood and severity of potential attacks on the organization's information assets. A change in the threat landscape may be caused by various factors, such as technological innovations, geopolitical events, cybercrime trends, regulatory changes, or organizational changes. A change in the threat landscape may introduce new risks or alter the existing risk profile of the organization, requiring a reassessment of the risk appetite, tolerance, and strategy. Reevaluation of risk helps the organization to adapt to the changing threat landscape and ensure that the information security program remains effective, efficient, and aligned with the business objectives.
References =
* CISM Review Manual 15th Edition, page 1131
* CISM Domain 2: Information Risk Management (IRM) [2022 update]2

* Reevaluation of Risk | CISM Exam Question Answer | ISACA3

NEW QUESTION: 274
某個組織因未通知可能危及客口資料的重大安全漏洞而受到監管機構的處罰。下列哪一項最可能需要審口和更新，以防止將來出現類似的處罰？
A. 事件回應訓練計劃
B. 資訊安全政策與程序
C. 業務連續性計劃 (BCP)
D. 事件溝通計劃
Answer: (SHOW ANSWER)

NEW QUESTION: 275
事後審口發現用口錯誤導致了重大違規行為。在審核過程中確定下列哪一項最重要？
A. 違規發生的時間和地點
B. 使用者先前造成的事件的證據
C. 使用者錯誤的根本原因
D. 針對使用者錯誤的適當紀律程序
Answer: (SHOW ANSWER)
The underlying reason for the user error is the most important factor to determine during the post-incident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents. References = CISM Review Manual 2023, page
1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

NEW QUESTION: 276
某組織正計劃將網路管理外包給服務提供者。在合約中包含下列哪一項是減輕資訊安全風險最有效的方法？
A. 定期資訊安全意識的要求
B. 審計權條款
C. 服務等級協定 (SLA)
D. 遵守公司安全政策的要求

Answer: (SHOW ANSWER)
The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.
References = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NEW QUESTION: 277
以下人員中，誰最適合批准具體的資訊安全風險處理方案？
A. 風險所有者
B. 資訊安全經理
C. 風險管理主管
D. 高階管理層
Answer: (SHOW ANSWER)
The risk owner (A) is best positioned to approve specific risk treatment options because they are accountable for the business process or asset affected by the risk and ultimately bear the consequences of that decision. CISM clearly distinguishes between roles that advise on risk (e.g., information security manager, risk management function) and those that own and accept risk. Senior management (D) defines risk appetite and tolerance, but day-to-day treatment decisions are delegated to risk owners within those boundaries. Approving treatment options requires an understanding of operational impact, cost, and business value-making the risk owner the appropriate authority.
References: ISACA CISM Review Manual (Risk management-risk ownership, accountability, and risk response); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 278
哪種類型的計劃主要旨在減少可能發生的安全事件的潛在影響？
A. 安全意識計劃
B. 災難復原計畫 (DRP)
C. 事件回應計劃
D. 業務連續性計劃 (BCP)
Answer: (SHOW ANSWER)

NEW QUESTION: 279
一家擁有多家商店的零售商新任命的資訊安全經理發現 HVAC（暖氣 通風和空調）供應商可以遠端存取商店，以實現即時監控和設備診斷 下列哪一項應該是資訊安全經理的首要行動方案？
A. 對供應商進行滲透測試。

B. 審口供應商的技術安全控制
C. 口看供應商合約
D. 斷開即時訪問
Answer: (SHOW ANSWER)
Reviewing the vendor contract should be the information security manager's first course of action when discovering an HVAC vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. The vendor contract should specify the terms and conditions of the vendor's access to the retailer' s network, such as the scope, purpose, duration, frequency, and method of access. The vendor contract should also define the roles and responsibilities of both parties regarding security, privacy, compliance, liability, and incident response. Reviewing the vendor contract will help the information security manager to understand the contractual obligations and expectations of both parties, and to identify any gaps or issues that need to be addressed or resolved1. The other options are not the first course of action for the information security manager when discovering an HVAC vendor has remote access to the stores. Conducting a penetration test of the vendor may be a useful way to assess the vendor's security posture and potential vulnerabilities, but it should be done with the vendor's consent and cooperation, and after reviewing the vendor contract2.
Reviewing the vendor's technical security controls may be a necessary step to verify the vendor's compliance with security standards and best practices, but it should be done after reviewing the vendor contract and in accordance with the agreed-upon audit procedures3. Disconnecting the real-time access may be a drastic measure that could disrupt the vendor's service delivery and violate the vendor contract, unless there is a clear and imminent threat or breach that warrants such action. References: 1: Vendor Access: Addressing the Security Challenge with Urgency - BeyondTrust 2: Penetration Testing - NIST 3: Reduce Risk from Third Party Access | BeyondTrust : Third-Party Vendor Security Risk Management & Prevention

NEW QUESTION: 280
成功控制勒索軟體事件後，應先執行下列哪一項操作？
A. 通知相關利害關係人。
B. 進行法醫分析。
C. 恢復受影響的系統。
D. 執行所學到的經驗教訓。
Answer: (SHOW ANSWER)

NEW QUESTION: 281
在建立向資訊安全戰略委員會報告的指標時，最重要的考慮因素是什麼？
A. 開髮用於傳達指標的儀表板
B. 就指標的基線口達成一致
C. 根據業界標準對指標的預期口進行基準測試
D. 使指標與組織文化保持一致
Answer: D (LEAVE A REPLY)

The most important consideration when establishing metrics for reporting to the information security strategy committee is D. Aligning the metrics with the organizational culture. This is because the metrics should reflect the values, beliefs, and behaviors of the organization and its stakeholders, and support the achievement of the strategic objectives and goals. The metrics should also be relevant, meaningful, and understandable for the intended audience, and provide clear and actionable information for decision making. The metrics should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 5, page 3

NEW QUESTION: 282
預算有限的小型組織僱用了一位新的資訊安全經理，他發現同一位T 員工被分配了系統管理員、安全管理員、資料庫管理員(DBA) 和應用程式管理員的職責。佳行動方針是什麼？
A. 自動化使用者設定活動。
B. 嚴格控制使用者配置活動。
C. 實施對 IT 管理員活動的監控。
D. 正式記錄 IT 管理員活動。
Answer: (SHOW ANSWER)

NEW QUESTION: 283
實施資料遺失防護 (DLP) 技術時，第一步應該是什麼？
A. 將組織的資料分類。
B. 執行成本效益分析。
C. 對候選供應商進行盡職調口。
D. 建立業務案例。
Answer: (SHOW ANSWER)

NEW QUESTION: 284
下列哪一項是遵守與個人資訊保護相關的新全球法規的最佳方式？
A. 執行風險處理計畫。
B. 審口與供應商的合約和工作口明書 (SOW)。
C. 實施資料區域化控制。
D. 確定控制項的目前狀態和所需狀態。
Answer: (SHOW ANSWER)
The best way to achieve compliance with new global regulations related to the protection of personal information is to determine the current and desired state of controls, as this helps the information security manager to identify the gaps and requirements for compliance, and to prioritize and implement the necessary actions and measures to meet the regulatory standards. The current state of controls refers to the existing level of protection and compliance of the

personal information, while the desired state of controls refers to the target level of protection and compliance that is required by the new regulations. By comparing the current and desired state of controls, the information security manager can assess the maturity and effectiveness of the information security program, and plan and execute a risk treatment plan to address the risks and issues related to the protection of personal information. Executing a risk treatment plan, reviewing contracts and statements of work (SOWs) with vendors, and implementing data regionalization controls are also important, but not as important as determining the current and desired state of controls, as they are dependent on the outcome of the gap analysis and the risk assessment, and may not be sufficient or appropriate to achieve compliance with the new regulations. References = CISM Review Manual 2023, page 491; CISM Review Questions, Answers & Explanations Manual 2023, page 352; ISACA CISM - iSecPrep, page 203

NEW QUESTION: 285
下列哪一項是成功實施零信任的最重要因素？
A. 優先選擇經過滲透測試的網絡
B. 專注於記錄和監控使用者行為
C. 對架構的策略點數進行認證與授權
D. 了解網路的每個元件
Answer: (SHOW ANSWER)
Zero Trust requires granular authentication and authorization at every critical juncture. It assumes no implicit trust within the network and enforces strict access control.
"Zero Trust is based on continuous authentication and authorization at all strategic control points." - CISM Review Manual 15th Edition, Chapter 3: Security Architecture, Section: Zero Trust Principles*

NEW QUESTION: 286
企業安全技術投資的建議應主要基於：
A. 遵守國際標準
B. 財務資源的可用性
C. 組織的風險承受能力
D. 與業務需求保持一致
Answer: (SHOW ANSWER)
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1, "Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance."1 The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security investments should be, as they can help protect the organization's assets and reputation from potential threats.

References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 287
在製定資訊安全策略的背景下，以下哪一項提供了最有用的輸入來確定或
A. 安全預算
B. 風險登記冊
C. 風險評分
D. 法律法規
Answer: (SHOW ANSWER)
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with- business-goals-and-objectives

NEW QUESTION: 288
在建立執行資訊安全計畫策略的路線圖後，資訊安全經理下一步該執行下列哪項操作？
A. 取得執行董事會對策略的共識。
B. 檢口與業務目標的一致性。
C. 定義組織風險承受能力。
D. 制定專案計劃來實施該策略。
Answer: (SHOW ANSWER)

The next thing that an information security manager should do after creating a roadmap to execute the strategy for an information security program is D. Develop a project plan to implement the strategy. This is because a project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. A project plan can help the information security manager to organize, coordinate, monitor, and control the activities and resources required to execute the strategy and achieve the desired outcomes. A project plan can also facilitate communication, collaboration, and reporting among the project team, stakeholders, and sponsors. A project plan is a detailed document that outlines the scope, objectives, deliverables, milestones, tasks, resources, roles, responsibilities, risks, and dependencies of the implementation process. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.2, page 1281; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 74, page 19

NEW QUESTION: 289
實施最小權限原則主要需要確定：
A. 工作職責
B. 資料擁有者
C. 主要風險因子。
D. 驗證控制
Answer: (SHOW ANSWER)
Implementing the principle of least privilege primarily requires the identification of job duties. Job duties are the specific tasks and responsibilities that an individual performs as part of their role in the organization. By identifying the job duties, the organization can determine the minimum access privileges necessary for each individual to perform their assigned function, and nothing more. This helps to reduce the risk of unauthorized access, misuse, or compromise of information and resources. The principle of least privilege is a key security principle that states that every module (such as a user, a process, or a program) must be able to access only the information and resources that are necessary for its legitimate purpose12.
The other options are not the primary factors that require identification for implementing the principle of least privilege. Data owners are the individuals or entities that have the authority and responsibility to define the classification, usage, and protection of data. Data owners may be involved in granting or revoking access privileges to data, but they are not the ones who identify the job duties of the data users. Primary risk factors are the sources or causes of potential harm or loss to the organization. Primary risk factors may influence the level of access privileges granted to users, but they are not the ones who define the job duties of the users.
Authentication controls are the mechanisms that verify the identity of users or systems before granting access to resources. Authentication controls may enforce the principle of least privilege, but they are not the ones who determine the job duties of the users. References = Principle of least privilege What Is the Principle of Least Privilege and Why is it Important? - F5 1
4

NEW QUESTION: 290
對於新聘用的負責識別和解決網路漏洞的資訊安全經理來說，下列哪一項是最佳起點？
A. 控制分析
B. 新興風險審口
C. 滲透測試
D. 流量監控
Answer: (SHOW ANSWER)
The best starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities is C. Penetration testing. This is because penetration testing is a method of simulating real-world attacks on a network to evaluate its security posture and identify any weaknesses or gaps that could be exploited by malicious actors. Penetration testing can help the information security manager to assess the effectiveness of the existing controls, prioritize the remediation efforts, and demonstrate compliance with the relevant standards and regulations. Penetration testing can also provide valuable insights into the network architecture, configuration, and behavior, as well as the potential impact and likelihood of different types of attacks.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 50, page 14

NEW QUESTION: 291
在以下情況下，事件回應團隊的效率將達到最高：
A. 根據吸取的經驗教訓更新事件回應流程。
B. 事件回應團隊成員是經過訓練的安全人員。
C. 事件回應團隊定期開會審口日誌檔案。
D. 使用安全資訊和事件監控 (SIEM) 系統來識別事件。
Answer: (SHOW ANSWER)

NEW QUESTION: 292
平衡記分卡最有效地實現資訊安全：
A. 專案管理
B. 治理。
C. 性能。
D. 風險管理。
Answer: (SHOW ANSWER)
A balanced scorecard most effectively enables information security govern-ance. Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress

of an organization toward its strategic goals. It typically includes four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:
*Align information security objectives with business objectives and communicate them to senior management and other stakeholders
*Monitor and report on the effectiveness and efficiency of information security processes and controls
*Identify and prioritize improvement opportunities and corrective actions
*Demonstrate the value and benefits of information security investments
*Foster a culture of security awareness and continuous learning
Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality.
A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Per-formance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement.
Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment.
References: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per- formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders:
Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

NEW QUESTION: 293
在新系統的實施過程中，下列哪個流程可以主動最大限度地減少中斷 未經授權的變更和錯誤的可能性？
A. 設定管理
B. 密碼管理
C. 變更管理
D. 版本管理
Answer: (SHOW ANSWER)
Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively

minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION: 294
資訊安全經理確定新發布的行業要求的安全標準存在大量例外。接下來應該執行下列哪項操作？
A. 記錄風險接受情形。
B. 修改組織的安全性策略。
C. 評估不合規的後果。
D. 進行資訊安全審核。
Answer: (SHOW ANSWER)
Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done. These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it. References = CISM Review Manual
2023, page 43 1; CISM Practice Quiz 2

NEW QUESTION: 295
在調口資訊安全事件時，應分享事件的詳細資訊：
A. 廣泛地表現出正面的意圖。
B. 僅限管理階層。
C. 僅根據需要，
D. 僅限口部稽核。
Answer: (SHOW ANSWER)
When investigating an information security incident, details of the incident should be shared only as needed, according to the principle of least privilege and the need-to-know basis. This means that only the authorized and relevant parties who have a legitimate purpose and role in the incident response process should have access to the incident information, and only to the extent that is necessary for them to perform their duties.
Sharing incident details only as needed helps to protect the confidentiality, integrity, and availability of the incident information, as well as the privacy and reputation of the affected individuals and the organization.
Sharing incident details only as needed also helps to prevent unauthorized disclosure, modification, deletion, or misuse of the incident information, which could compromise the investigation, evidence, remediation, or legal actions.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, page 2311; CISM Review Questions, Answers & Explanations Manual,
10th Edition, Question 49, page 462.

NEW QUESTION: 296
一家軟體供應商宣布存在一個零日漏洞，該漏洞會暴露組織的關鍵業務系統。供應商已發布緊急補丁。下列哪一項應該是資訊安全管理者主要關注的問題？
A. 修補程式的文檔
B. 實施控制的資源可用性
C. 能口在部署之前測試補丁
D. 事件回應計畫的充分性
Answer: (SHOW ANSWER)

NEW QUESTION: 297
在將受影響的系統恢復在線之前，在事件回應過程的恢復階段完成以下哪一項是最重要的？
A. 高階管理層報告的文檔復原步驟。
B. 擷取並儲存受影響系統的取證影像。
C. 記錄並關閉安全事件票證。
D. 測試並驗證受感染的系統是否乾淨。
Answer: (SHOW ANSWER)

NEW QUESTION: 298
當組織計劃使用第三方雲端運算服務進行關鍵業務流程時，資訊安全經理首先應該做什麼？
A. 分析業務需求。
B. 執行差距分析。
C. 執行風險評估。
D. 標識要託管的資料。
Answer: (SHOW ANSWER)

NEW QUESTION: 299
當新的資訊安全經理正在為不受監管的組織制定資訊安全策略時，請口看以下哪一項最有幫助？
A. 管理階層的業務目標與目標
B. 其他非監理公司的策略
C. 風險評估結果
D. 業界最佳實務與控制建議
Answer: (SHOW ANSWER)
When a new information security manager is developing an information security strategy for a non-regulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

NEW QUESTION: 300
組織內部網路的定期漏洞掃描發現許多使用者工作站都有未打補丁的軟體版本。資訊安全經理幫助高階管理層了解相關風險的最佳方法是什麼？
Freecram.net
A. 將風險的影響納入常規指標。
B. 建議安全指導委員會進行審口。
C. 定期更新風險評估
D. 直接向高階主管發送定期通知
Answer: (SHOW ANSWER)

Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact.
References: https://www.isaca.
org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-security-investments
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of- your-information-security-management-system

NEW QUESTION: 301
在確認特權使用者對安全應用程式進行未經授權的修改後，資訊安全經理應先執行下列哪項操作？
A. 報告與違反政策相關的風險。
B. 強制執行安全性配置並要求復原變更。
C. 實施補償控制來解決風險。
D. 實施特權存取管理系統。
Answer: (SHOW ANSWER)
The first thing that an information security manager should do upon confirming a privileged user's unauthorized modifications to a security application is to enforce the security configuration and require the change to be reverted. This is because the unauthorized modification may have compromised the security of the application and the data it protects, and may have violated the security policies and standards of the organization. By enforcing the security configuration and requiring the change to be reverted, the information security manager can restore the security posture of the application and prevent further unauthorized modifications.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should monitor and review the security configuration of information systems on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Enforcing the security configuration and requiring the change to be reverted is the correct answer because it is the most immediate and effective action to address the unauthorized modification and to maintain the security of the application" (p. 63). Additionally, the Effective Interactive Privileged Access Review article from the ISACA Journal 2018 states that "any

unauthorized changes to the production environment should be reverted back to the original state and the incident should be reported to the appropriate authority" (p. 4)1.

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 302
下列哪一項最有利於有效的事件回應測試？
A. 包含測試中的所有業務部門
B. 模擬真實的測試場景
C. 每季檢討一次測試結果
D. 重大業務變更後的測試
Answer: (SHOW ANSWER)
Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective testing is to simulate realistic test scenarios that reflect the most likely or critical threats and vulnerabilities that could cause an incident, and the most relevant or significant impacts and consequences that could result from an incident. Simulating realistic test scenarios can help to evaluate the adequacy, accuracy, and applicability of the incident response plan, procedures, roles, and resources, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the incident response process. Simulating realistic test scenarios can also help to enhance the skills, knowledge, and experience of the incident response team and the organization, as well as to improve the communication, coordination, and collaboration among the stakeholders involved in the incident response process. Simulating realistic test scenarios can also help to measure and report the effectiveness and efficiency of the incident response process, and to provide feedback and recommendations for improvement and optimization. References = CISM Review Manual 15th Edition, page 2401; CISM Practice Quiz, question 1362

NEW QUESTION: 303
下列哪一項是有效資訊安全指標最重要的特徵？
A. 此指標經常向高階管理層報告。
B. 此指標將組織的固有風險與其風險偏好進行比較。

C. 此指標直接對應到口業風險管理框架。
D. 此指標表示相對於風險承受能力的剩餘風險。
Answer: (SHOW ANSWER)

NEW QUESTION: 304
為了支持有效的風險決策，下列何者最重要？
A. 已建立的風險域
B. 風險報告程序
C. 由中階管理人員組成的審計委員會
D. 明確定義且經過批准的控制措施
Answer: (SHOW ANSWER)
To support effective risk decision making, it is most important to have risk reporting procedures in place.
Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid- level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION: 305
下列哪一個角色最適合在年度使用者訪問審核期間驗證使用者存取要求？
A. 存取管理器
B. IT 總監
C. 系統管理員
D. 企業主
Answer: (SHOW ANSWER)
The business owner is the best suited role to validate user access requirements during an annual user access review, because the business owner is responsible for determining the business needs and objectives of the users, as well as defining the appropriate access rights and privileges for each user role. The business owner is also accountable for ensuring that the user access is aligned with the organization's policies and standards, and that the user access review is conducted effectively and efficiently1. The access manager, the IT director, and the system administrator are not as suitable as the business owner, because they are more involved in the technical and operational aspects of user access management, rather than the business aspects.
References = Effective User Access Reviews

NEW QUESTION: 306
下列哪一項對於確定是否接受關鍵安全系統的殘餘風險最有幫助？
A. 可用的年度預算
B. 緩解控制措施的成本效益分析
C. 復原時間目標 (RTO)
D. 最大可容忍中斷 (MTO)
Answer: (SHOW ANSWER)
Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk events." CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise." CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

NEW QUESTION: 307

一家組織正在進行一項安全意識培訓計畫。然而，員工參與度在過去一年中一直在下降，而來自電子郵件的惡意軟體和網路釣魚事件數量卻在不斷增加。資訊安全經理的最佳應對方案是什麼？

A. 向高階管理層報告調口結果並提出建議。

B. 在電子郵件系統中實施網路釣魚報告工具。

C. 每次訓練課程後都包含定期的網路釣魚活動。

D. 要求所有員工必須參加訓練計畫。

Answer: (SHOW ANSWER)

If participation in security awareness training is decreasing while incidents are rising, making the training program mandatory for all employees is the best course of action. The CISM Review Manual notes that mandatory training ensures organizational-wide coverage and directly addresses the lack of participation, which is likely contributing to increased incidents. Reference:ISACA CISM Review Manual, 16th Edition, Page 220-221, "Awareness and Training - Ensuring Coverage".

NEW QUESTION: 308

一家線上銀行發現正在進行的成功網路攻擊。銀行應該首先：

A. 隔離受影響的網段。

B. 向董事會報告根本原因。

C. 評估個人識別資訊 (PII) 是否受到洩漏。

D. 關閉整個網路。

Answer: (SHOW ANSWER)

The online bank should first isolate the affected network segment, as this is the most effective way to contain the attack and prevent it from spreading to other parts of the network or compromising more data or systems.

Isolating the affected network segment also helps to preserve the evidence and facilitate the investigation and recovery process. Reporting the root cause to the board of directors, assessing whether personally identifiable information (PII) is compromised, and shutting down the entire network are not the first actions that the online bank should take, as they may not be feasible or appropriate at the time of the attack, and may cause more disruption, confusion, or damage to the business operations and reputation. References = CISM Review Manual 2023, page 1641; CISM Review Questions, Answers & Explanations Manual 2023, page 362; ISACA CISM - iSecPrep, page 213

NEW QUESTION: 309

一個組織正在經歷數位轉型過程，這將IT 組織置於一個不熟悉的風險環境中。資訊安全經理的任務是領導 IT 風險管理流程。下列哪一項應被給予最高優先權？

A. 風險識別

B. 控制差距分析

C. 關鍵風險指標 KRI）的設計

D. 風險處理方案的選擇

Answer: (SHOW ANSWER)
= Identification of risk is the first and most important step in the IT risk management process, especially when the organization is undergoing a digital transformation that introduces new technologies, processes, and business models. Identification of risk involves determining the sources, causes, and potential consequences of IT-related risks that may affect the organization's objectives, assets, and stakeholders. Identification of risk also helps to establish the risk context, scope, and criteria for the subsequent risk analysis, evaluation, and treatment. Without identifying the risks, the information security manager cannot effectively assess the risk exposure, prioritize the risks, implement appropriate controls, monitor the risk performance, or communicate the risk information to the relevant parties.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, page 841; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question
34, page 352.

NEW QUESTION: 310
一個業務部門最近將組織新的強密碼策略整合到其業務應用程式中，要求使用者每 30 天重置一次密碼。服務台現在充斥著密碼重置請求。下列哪一項是資安經理解決這種情況的最佳行動方案？
A. 升等至高階管理層。
B. 提供最終使用者培訓。
C. 進行業務影響分析 (BIA)。
D. 繼續執行該政策。
Answer: (SHOW ANSWER)

NEW QUESTION: 311
在決定大型組織資料中心的業務連續性策略時，下列哪一項最有用？
A. 利害關係人回饋分析
B. 業務連續性風險分析
C. 事件根本原因分析
D. 商業影響分析 (BIA)
Answer: (SHOW ANSWER)
According to the CISM Review Manual, a business impact analysis (BIA) is the most useful tool when determining the business continuity strategy for a large organization's data center, as it helps to identify and prioritize the critical business processes and resources that depend on the data center, and the impact of their disruption or loss. A BIA also provides the basis for defining the recovery time objectives (RTOs) and recovery point objectives (RPOs) for the data center, which guide the selection of the appropriate business continuity strategy.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.5.2, page 1511.

NEW QUESTION: 312

一名員工剛剛報告丟失了包含公司資訊的個人行動裝置。資訊安全經理應該先執行下列哪一項操作？

A. 口動事件回應。

B. 停用遠端

C. 口動設備重設。

D. 進行風險評估。

Answer: (SHOW ANSWER)

Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage.

According to ISACA, incident management is one of the key processes for information security governance.

Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan. References: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

NEW QUESTION: 313

下列哪一項對於指導綜合資訊安全計畫的開發和管理最重要？

A. 採用資訊安全計畫管理最佳實踐

B. 實施政策和程序來解決資訊安全策略

C. 使組織的業務目標與 IT 目標一致

D. 建立並維護資訊安全治理框架

Answer: (SHOW ANSWER)

An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified. References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 314

與白盒控制測試相比，執行黑盒控制測試的主要優點是：

A. 減少潛在的生口問題。

B. 需要較少的 IT 人員準備。

C. 模擬現實世界的攻擊。
D. 辨識更多威脅。
Answer: (SHOW ANSWER)
The primary advantage of performing black-box control tests as opposed to white-box control tests is that they simulate real-world attacks. Black-box control tests are a software testing methodology in which the tester analyzes the functionality of an application without a thorough knowledge of its internal design. Conversely, in white-box control tests, the tester is knowledgeable of the internal design of the application and analyzes it during testing. By performing black-box control tests, the tester can mimic the perspective and behavior of an external attacker who does not have access to the source code or the implementation details of the application.
This way, the tester can evaluate how the application responds to different inputs and scenarios, and identify any vulnerabilities or errors that may affect its functionality or security. The other options are not the primary advantage of performing black-box control tests, although they may be some benefits or drawbacks depending on the context. Causing fewer potential production issues is not necessarily true, as black-box control tests may still introduce errors or disruptions to the application if not performed carefully. Requiring less IT staff preparation is not always true, as black-box control tests may still require a lot of planning and documentation to ensure adequate test coverage and quality. Identifying more threats is not necessarily true, as black-box control tests may miss some threats that are hidden in the internal logic or structure of the application.

NEW QUESTION: 315
組織□報告了安全事件，資訊安全經理應何時聯繫資訊所有者？
A. 事件緩解後
B. 事件得到確認後。
C. 潛在事件被切換後
D. 事件被遏制後
Answer: (SHOW ANSWER)
= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

NEW QUESTION: 316
員工安全意識培訓計畫結束後，預期結果應該是什麼？

A. 傳入電子郵件中偵測到的病毒數量減少
B. 報告的社會工程攻擊減少
C. 報告的社會工程嘗試增加
D. 使用者報告的誤報事件增加
Answer: (SHOW ANSWER)
This outcome indicates that the employees are more aware of the signs and techniques of social engineering and are able to report them to the appropriate authorities. This also helps to prevent successful attacks and reduce the impact of potential breaches.
References: The CISM Review Manual 2023 states that "security awareness training should include information on how to identify and report social engineering attempts" and that "the effectiveness of security awareness training can be measured by the number and quality of reported incidents" (p. 121). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "An increase in reported social engineering attempts is the best indicator that the security awareness training program has been effective, as it shows that the employees are more vigilant and proactive in detecting and reporting such attempts" (p. 45).

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 317
應用程式開發部門主管已決定接受最近評估中發現的風險。儘管監管部門要求實施這些建議，但不會實施任何建議。資訊安全經理下一步該怎麼做？
A. 審口風險監控計畫。
B. 正式記錄該決定。
C. 審口規定。
D. 建議風險管理團隊。
Answer: D (LEAVE A REPLY)
Since the identified risks are subject to regulatory requirements, and cannot simply be accepted without oversight, the information security manager should escalate the issue to the risk management team or higher authority to ensure proper governance.
"When risk acceptance contradicts regulatory requirements, it must be escalated to senior management or the risk function for resolution."
- CISM Review Manual 15th Edition, Chapter 1: Governance Responsibilities, Section: Risk Governance and Oversight*

NEW QUESTION: 318
下列何者最能讓資訊安全經理確定組織資訊安全策略的全面性？
A. 口部安全審核
B. 外部安全審核
C. 組織風險偏好
D. 商業影響分析 (BIA)
Answer: (SHOW ANSWER)
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

NEW QUESTION: 319
下列哪一項是針對惡意口部人員洩漏機密資訊最有效的防禦措施？
A. 定期審核存取控制
B. 招募員工時進行嚴格的背景調口
C. 提示終止程序
D. 基於角色的存取控制 (RBAC)
Answer: (SHOW ANSWER)
role-based access control (RBAC) is the most effective defense against malicious insiders compromising confidential information, as it helps to limit the access of users to the information and resources that are necessary for their roles and responsibilities. RBAC also helps to enforce the principle of least privilege, which reduces the risk of unauthorized or inappropriate access, disclosure, modification, or destruction of information by insiders. RBAC also facilitates the monitoring and auditing of user activities and access rights.
References = Malicious insiders | Cyber.gov.au, Insider Threat Mitigation Guide - CISA, Malicious Insiders:
Types, Indicators & Common Techniques - Ekran System

NEW QUESTION: 320
一位資訊安全經理正在更新組織的事件回應計畫。下列哪一項是驗證IT和業務部門提供的流程和程序是否完整、準確且所有負責團隊均知曉的最佳方法？
Freecram.net
A. 與利害關係人一起檢視測試目標。
B. 進行資料外洩事件桌面演習。
C. 進行事件回應計畫調口。

D. 檢視資料外洩事件分類步驟。

Answer: (SHOW ANSWER)

Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.

Reference:ISACA CISM Review Manual, 16th Edition, Page 295, "Testing and Validating Incident Response Plans".

NEW QUESTION: 321

滿足下列哪一項安全目標最能確保資訊免於未經授權的外洩？

A. 完整性

B. 真實性

C. 保密性

D. 不可否認性

Answer: (SHOW ANSWER)

Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References: https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

NEW QUESTION: 322

回應勒索軟體攻擊時的主要考慮因素應是確保：

A. 備份可用。

B. 已套用最新補丁。

C. 勒索軟體攻擊已被遏制

D. 企業可以經營

Answer: (SHOW ANSWER)

Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.

References:
https://www.cisa.gov/stopransomware/ransomware-guide
https://csrc.nist.gov/Projects/ransomware-protection-and-response
https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

NEW QUESTION: 323
下列哪一項是在製定資訊安全計畫時考慮組織文化的最重要原因？
A. 它有助於加快資訊安全預算的批准。
B. 安全事件對整個組織口生不利影響。
C. 它幫助組織滿足合規性要求。
D. 組織中的每個人都對資訊安全負責。
Answer: (SHOW ANSWER)

NEW QUESTION: 324
為了確保事件得到適當的個人回應，下列哪一項對於包含在事件回應計畫中最重要？
A. 事件回應團隊所需的技能
B. 協助處理事件的外部資源列表
C. 服務等級協定 (SLA)
D. 詳細的事件通知流程
Answer: (SHOW ANSWER)
A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right people are involved in the incident response, that the incident is handled in a timely and efficient manner, and that the relevant information is shared with the appropriate parties. Skills required for the incident response team, a list of external resources to assist with incidents, and service level agreements (SLAs) are also important elements of an incident response plan, but they are not as critical as the incident notification process. Skills required for the incident response team describe the competencies and qualifications of the team members, but they do not specify who should be notified or involved in the incident response. A list of external resources to assist with incidents provides a directory of external parties that can provide support or expertise in the incident response, but it does not define the criteria or process for engaging them. Service level agreements (SLAs) define the expectations and obligations of the service providers and the service recipients in the incident response, but they do not detail the steps or procedures for notifying or escalating incidents. References = CISM Review Manual, 16th Edition, pages 191-1921; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 662

NEW QUESTION: 325
哪種類型的系統最能有效地根據影響對網路事件進行優先排序並追蹤直至其結束？

A. 安全資訊與事件管理 (SIEM)
B. 擴充偵測與回應（XDR）
C. 端點偵測與回應（EDR）
D. 網路入侵偵測系統 (NIDS)
Answer: (SHOW ANSWER)
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

NEW QUESTION: 326
在開發儲存高度機密資料的關鍵系統時，資訊安全經理應主要注意下列哪一項？
A. 減少偵測到的漏洞數量
B. 確保剩餘風險的大小是可接受的
C. 避免已識別的系統威脅
D. 符合監理要求
Answer: (SHOW ANSWER)
The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable. Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

NEW QUESTION: 327
誰負責確保採取適當的控制措施來解決資訊系統的機密性和可用性？
A. 業務經理
B. 高階管理層
C. 資訊安全經理

D. 資訊擁有者
Answer: (SHOW ANSWER)

NEW QUESTION: 328
基於 Web 應用程式的資料輸入功能已外包給將在遠端站點工作的第三方服務提供者 下列哪一個問題是資訊安全經理最關心的問題？
A. 應用程式未使用安全通訊協定
B. 應用程式配置了限制性存取控制
C. 業務流程只有一級錯誤檢口
D. 不強制執行基於伺服器的惡意軟體防護
Answer: (SHOW ANSWER)
Server-based malware protection is not enforced is the issue that would be of GREATEST concern to an information security manager, as it exposes the web-based application and its data to potential threats from malicious software that can compromise the confidentiality, integrity, and availability of the information.
Server-based malware protection is a security control that monitors and blocks malicious activities on the server where the application runs, such as viruses, worms, trojans, ransomware, etc. Without server-based malware protection, the web-based application may be vulnerable to attacks that can damage or destroy the data stored on the server, or disrupt the normal functioning of the application. The other issues are also important, but not as critical as server-based malware protection. The application does not use a secure communications protocol may expose sensitive data in transit to eavesdropping or interception by unauthorized parties. The application is configured with restrictive access controls may limit the access rights of legitimate users to authorized resources, but it does not prevent unauthorized users from accessing them through other means. The business process has only one level of error checking may result in incorrect or inconsistent data entry or processing, but it does not guarantee data quality or accuracy. References = CISM Review Manual, 16th Edition, page 1751; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 812

NEW QUESTION: 329
某機構近期購買了網路安全保險，此前其董事會表達了對潛在安全漏洞的擔憂。透過這項應對措施，該機構：
A. 已避免與安全漏洞相關的風險
B. 可以安全地降低其口部安全支出
C. 最終仍需對違規行為的影響負責
D. 已實施冗餘控制措施以防止違規行為
Answer: (SHOW ANSWER)
Even with cybersecurity insurance, the organization remains ultimately accountable for the impact of a breach (C). Insurance represents risk transfer, not risk elimination or avoidance. CISM clearly states that accountability for risk cannot be transferred; only financial impact may be partially offset. Insurance does not justify reducing security controls (B) and does not constitute redundant

controls (D). Avoidance (A) would require eliminating the risky activity entirely. Management must continue to manage, monitor, and mitigate risk in line with appetite, regardless of insurance coverage.
References: ISACA CISM Review Manual (Risk management-risk response strategies, risk transfer); CISM Exam Content Outline (Domain 1).

NEW QUESTION: 330
當威脅情報報告顯示針對該行業的大量勒索軟體攻擊時，下列哪一項是資訊安全經理的最佳行動方案？
A. 增加系統備份的頻率。
B. 檢口緩解安全控制措施。
C. 將威脅通知員工。
D. 評估組織的風險。
Answer: (SHOW ANSWER)
The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance.
A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness.
The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat © is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. References = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

NEW QUESTION: 331

新任資安經理發現組織傾向於使用短期解決方案來解決問題。無法有效追蹤資源分配和支出，且無法保證滿足合規性要求。首先該做什麼來扭轉這種由下而上的安全方法？
A. 創建資訊安全指導委員會。
B. 建立審計委員會。
C. 進行威脅分析。
D. 實施資訊安全意識培訓計畫。
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 332
作為事件回應活動的一部分，開始復原過程的最佳時間是：
A. 根除階段已完成
B. 事件回應小組已成立
C. 根本原因已確定
D. 事件管理員已宣布此事件
Answer: (SHOW ANSWER)
Recovery should not begin until the eradication phase is complete, meaning all malicious activity, malware, or unauthorized access has been removed. Starting recovery too early may reintroduce threats or result in re- infection.
"Recovery begins after eradication is complete, ensuring a clean environment for restoring services."
- CISM Review Manual 15th Edition, Chapter 4: Incident Response Lifecycle, Section: Recovery Phase*

NEW QUESTION: 333
下列哪一項是決定事件回應計畫有效性的最佳方法？
A. 口看先前的審核報告
B. 進行桌面練習
C. 根據最佳實踐對計劃進行基準測試
D. 執行滲透測試
Answer: (SHOW ANSWER)

A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

NEW QUESTION: 334
當滲透測試發現由於防火牆配置不正確而導致安全漏洞時，資訊安全經理應採取下列哪項最佳行動？
A. 確保制定具有里程碑的計劃。
B. 實施分散式阻斷服務 (DDoS) 控制。
C. 與事件回應團隊合作。
D. 定義新的關鍵績效指標 (KPI)。
Answer: (SHOW ANSWER)
A penetration test is a proactive way to identify and remediate security vulnerabilities in a network. When a penetration test reveals a security exposure due to a firewall that is not configured correctly, the information security manager's best course of action is to ensure a plan with milestones is developed to address the issue.
This plan should include the root cause analysis, the corrective actions, the responsible parties, the deadlines, and the verification methods. This way, the information security manager can ensure that the security exposure is resolved in a timely and effective manner, and that the firewall configuration is aligned with the security policy and the business objectives.
References =
CISM Review Manual (Digital Version), page 193: "The information security manager should ensure that a plan with milestones is developed to address the issues identified during the penetration test." How to configure a network firewall: Walkthrough: "A good network firewall is essential. Learn the basics of configuring a network firewall, including stateful vs. stateless firewalls and access control lists in this episode of Cyber Work Applied." Which of the following is the BEST way to evaluate whether the information security program aligns with corporate governance?
A). Survey mid-level management.
B). Analyze industry benchmarks.
C). Conduct a gap analysis.
D). Review internal audit reports.

NEW QUESTION: 335
員工點擊釣魚郵件中的鏈接，引發勒索軟體攻擊下列哪一項應該屬於資訊安全？
A. 擦除受影響的系統。

B. 通知口部法律顧問。
C. 通知高階管理層。
D. 隔離受影響的端點。
Answer: (SHOW ANSWER)
Isolating the impacted endpoints is the best course of action for the information security manager after an employee clicked on a link in a phishing email, triggering a ransomware attack because it prevents the ransomware from spreading to other systems or devices on the network, and minimizes the damage or disruption caused by the attack. Wiping the affected system is not a good course of action because it may destroy any evidence or data that could be used for investigation or recovery. Notifying internal legal counsel is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Notifying senior management is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. References: https://www.isaca.org/resources/isaca-journal/issues
/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 336
在風險已被隔離並已執行取證流程的違規事件之後，接下來應該執行下列哪項操作？
A. 將 Web 伺服器置於隔離區。
B. 從上次驗證的備份重建伺服器。
C. 有組織地關閉伺服器。
D. 使用原始媒體中的相關補丁重建伺服器。
Answer: (SHOW ANSWER)
= After a breach where the risk has been isolated and forensic processes have been performed, the next step should be to rebuild the server from the last verified backup. This will ensure that the server is restored to a known and secure state, and that any malicious code or data that may have been injected or compromised by the attacker is removed. Rebuilding the server from the original media may not be sufficient, as it may not include the latest patches or configurations that were applied before the breach. Placing the web server in quarantine or shutting it down may not be feasible or desirable, as it may disrupt the business operations or services that depend on the server. Rebuilding the server from the last verified backup is the best option to resume normal operations while maintaining security. References = CISM Review Manual 15th Edition, page 118: "Recovery is the process of restoring normal operations after an incident. Recovery activities may include rebuilding systems, restoring data, applying patches, changing passwords, and testing functionality." Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2014 &

2015, snippet: "Restore from backup. If you have a backup of your system from before the breach, wipe your system clean and restore from backup. This will ensure that any backdoors or malware installed by the hackers are removed."

NEW QUESTION: 337
當未知惡意軟體感染組織的關鍵系統時，應先觸發下列哪一項？
A. 事件回應計劃
B. 災難復原計畫 (DRP)
C. 業務連續性計劃 (BCP)
D. 漏洞管理計劃
Answer: (SHOW ANSWER)
The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization' s critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage.
References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons- learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 338
下列哪一項最能顯示最近在整個組織口進行的資訊安全意識活動的有效性？
A. 安全事件數量減少
B. 安全事件升級的頻率增加
C. 減少安全事件的影響
D. 報告的安全事件數量增加
Answer: (SHOW ANSWER)
The best indicator of the effectiveness of a recent information security awareness campaign delivered across the organization is the increase in the number of reported security incidents. This means that the employees have become more aware of the security threats and issues, and have learned how to recognize and report them to the appropriate authorities. Reporting security incidents is a vital part of the incident response process, as it helps to identify and contain the incidents, prevent further damage, and initiate the recovery actions. Reporting security incidents also helps to collect and analyze the incident data, which can be used to improve the security

controls and policies, and to prevent or mitigate similar incidents in the future. An increase in the number of reported security incidents shows that the awareness campaign has successfully raised the level of security knowledge, attitude, and behavior among the employees, and has encouraged them to take an active role in protecting the organization's information assets.
References =
CISM Review Manual 15th Edition, page 1631
Measuring and Evaluating the Effectiveness of Security Awareness Improvement Methods2 Developing metrics to assess the effectiveness of cybersecurity awareness program3 How to build a successful information security awareness programme - BCS4 How to Increase Cybersecurity Awareness - ISACA5

NEW QUESTION: 339
下列何者是組織文化對資訊安全計畫有效性的主要影響？
A. 文化塑造了資訊安全行為。
B. 文化定義了專案實施所需的責任。
C. 文化有助於確定資訊安全控制的預算。
D. 只要遵守資訊安全控制，文化的影響就很小。
Answer: (SHOW ANSWER)
A culture that supports security encourages behaviors that protect information assets.
"Organizational culture has a significant impact on how employees approach security, influencing their behavior and adherence to policies."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture*

NEW QUESTION: 340
下列哪一項是資訊安全經理在應用程式開發中的主要角色？
A. 確保將安全性整合到系統開發生命週期 (SDLC) 中
B. 確保符合業界最佳實踐
C. 確保實施企業安全控制
D. 確保控製程式解決業務風險
Answer: (SHOW ANSWER)
According to the CISM Review Manual, one of the primary roles of the information security manager in application development is to ensure that security is integrated into the SDLC. This means that security requirements, design, testing, deployment, and maintenance are all considered and addressed throughout the application development process. By doing so, the information security manager can help to prevent or mitigate security risks, ensure compliance with standards and regulations, and improve the quality and reliability of the application1 The other options are not as accurate as ensuring security is integrated into the SDLC. Ensuring compliance with industry best practices is a secondary role of the information security manager in application development, as it involves following established guidelines and frameworks for secure application development. However, compliance alone does not guarantee that security is

actually implemented in the application. Ensuring enterprise security controls are implemented is a tertiary role of the information security manager in application development, as it involves applying existing policies and procedures for managing and monitoring security activities across the organization. However, enterprise controls alone do not ensure that security is tailored to the specific needs and context of each application. Ensuring control procedures address business risk is a quaternary role of the information security manager in application development, as it involves identifying and assessing potential threats and vulnerabilities that could affect the business objectives and operations of each application. However, business risk alone does not ensure that security measures are aligned with the value proposition and benefits of each application1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 30-31...

NEW QUESTION: 341
資安經理指出，在記錄票證後，幫助台沒有適當升級安全事件下列哪一項是解決此問題的最佳自動化控制？
A. 在口明台工作流程中實施自動漏洞掃描
B. 將所有安全事件的預設設定變更為最高優先權
C. 將自動化服務等級協定 (SLA) 報告整合到幫助台票務系統中
D. 將事件回應工作流程整合到幫助台票務系統中
Answer: (SHOW ANSWER)
The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities.
This will improve the efficiency, effectiveness, and consistency of the incident response process. References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

NEW QUESTION: 342
下列哪一個因素對資訊安全戰略目標的成功實施影響最大？
A. 監理要求
B. 合規驗收
C. 管理支持
D. 預算核准
Answer: (SHOW ANSWER)
Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring

adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance1. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with2. Compliance acceptance is the degree to which the organization adheres to the information security policies and standards3. Budgetary approval is the process of allocating financial resources for the information security activities and initiatives4. References: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

NEW QUESTION: 343
當偵測到伺服器上的多個網路入侵時，資訊安全經理的主要關注點應該是確保：
A. 伺服器已斷電。
B. 該事件已報告給高階管理層。
C. 取證調口軟體已載入到伺服器上。
D. 保留證據的完整性。
Answer: (SHOW ANSWER)

NEW QUESTION: 344
在建立資訊安全治理框架時，資訊安全管理者最重要的是要了解：
A. 威脅環境。
B. 風險管理技術。
C. 資訊安全最佳實務。
D. 企業文化。
Answer: (SHOW ANSWER)

NEW QUESTION: 345
資訊安全風險評估的下列哪一個組成部分對高階管理層最有價口？
A. 威脅概況
B. 剩餘風險
C. 投資報酬率 (ROI)
D. 緩解措施
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after implementing risk mitigation actions. It is the most valuable component for senior management because it helps them to evaluate the effectiveness and efficiency of risk management and make informed decisions about risk acceptance, transfer or avoidance. References = CISM Review Manual, 16th Edition, Chapter 2, Section 2.3.41

NEW QUESTION: 346
在使事件回應計畫與公司策略一致時，應先更新下列哪一項？
A. 災難復原計畫 (DRP)
B. 事件通知計劃
C. 風險因應場景
D. 安全程序
Answer: (SHOW ANSWER)
The answer to the question is C. Risk response scenarios. This is because risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents, such as cyberattacks, natural disasters, or data breaches. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization, and guides the decision- making and resource allocation processes. By aligning the risk response scenarios with the corporate strategy, the organization can ensure that the incident response plan supports the achievement of the desired outcomes and benefits, and minimizes the impact and disruption to the business operations and performance.
Risk response scenarios are the predefined plans and actions that the organization will take to respond to specific types of incidents. Risk response scenarios should be aligned with the corporate strategy, which defines the vision, mission, goals, and objectives of the organization. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2111; CISM domain 4:
Information security incident management [2022 update] | Infosec2; A Guide to Effective Incident Management Communications3

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 347
對於新聘用的負責制定和實施資訊安全策略的資訊安全經理來口，下列哪一項最有用？
A. 資訊安全團隊的能力與專業知識
B. 組織的使命宣言與路線圖
C. 先前成功的資訊安全策略
D. 組織的資訊科技 (IT) 策略
Answer: (SHOW ANSWER)

= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security strategy with them. The information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes.

The capabilities and expertise of the information security team (A) are important factors for the information security manager to consider, but they are not the most useful source of information for developing and implementing an information security strategy. The information security team is responsible for executing and maintaining the information security program and activities, such as risk management, security awareness, incident response, and compliance. The information security manager should assess the capabilities and expertise of the information security team to identify the strengths, weaknesses, opportunities, and threats, and to plan the resource allocation, training, and development of the team. However, the capabilities and expertise of the information security team do not directly inform the information security strategy, which should be driven by the organization's business objectives, risk appetite, and security needs.

A prior successful information security strategy © is a possible source of information for the information security manager to refer to, but it is not the most useful one. A prior successful information security strategy is a strategy that has been implemented and evaluated by another organization or a previous information security manager, and has achieved the desired security outcomes and benefits. The information security manager can learn from the best practices, lessons learned, and challenges of a prior successful information security strategy, and apply them to the current organization or situation. However, a prior successful information security strategy may not be relevant, applicable, or suitable for the organization, as it may not reflect the current or future business objectives, risk appetite, and security needs of the organization, or the changing threat landscape and business environment.

The organization's information technology (IT) strategy (D) is also a possible source of information for the information security manager to consult, but it is not the most useful one. The IT strategy is a strategy that defines the IT vision, goals, and initiatives of the organization, and how IT supports and enables the business processes and activities. The information security manager should review the IT strategy to understand the IT infrastructure, systems, and services of the organization, and how they relate to the information security program and activities. However, the IT strategy is not the primary driver of the information security strategy, which should be aligned with the organization's business objectives, risk appetite, and security needs, and not only with the IT objectives, capabilities, and requirements.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Information Security Strategy Development, page 23-241

NEW QUESTION: 348
在定義事件分類和分類等級時，組織最適合考慮下列哪一項？
A. 事件回應活動的成熟度
B. 威脅環境
C. 受影響資口的數量
D. 事件影響
Answer: (SHOW ANSWER)
Incident impact is the primary factor for classification and categorization. It ensures incidents are addressed based on their potential to disrupt the organization.
"Incident impact should be the primary factor in defining categorization levels to ensure appropriate prioritization and response."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization* ISACA practice database stresses that focusing on impact ensures incidents receive the proper response priority.

NEW QUESTION: 349
下列哪一項是資訊安全治理的預期結果？
A. 滲透測試
B. 改善風險管理
C. 業務敏捷性
D. 成熟度模型
Answer: (SHOW ANSWER)
Business agility is a desired outcome of information security governance, as it enables the organization to respond quickly and effectively to changing business needs and opportunities, while maintaining a high level of security and risk management. Information security governance provides the strategic direction, policies, standards, and oversight for the information security program, ensuring that it aligns with the organization's business objectives and stakeholder expectations. Information security governance also facilitates the integration of security into the business processes and systems, enhancing the organization's ability to adapt to the dynamic and complex environment. By implementing information security governance, the organization can achieve business agility, as well as other benefits such as improved risk management, compliance, reputation, and value creation. References = CISM Review Manual 15th Edition, page 25.

NEW QUESTION: 350
組織的安全策略是禁止存取筆記型電腦和桌上型電腦上的 USB 儲存裝置。下列哪一項是給予政策例外的最有力的理由？
Freecram.net
A. 收益大於潛在風險。
B. 根據使用者角色口用 USB 儲存裝置。

C. 使用者接受不合規的風險。

D. 存取權限僅限於唯讀。

Answer: (SHOW ANSWER)

The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security pol-icy should also be aligned with the organization's business objectives and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2. The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as:

*Enhancing data mobility and accessibility

*Improving data backup and recovery

*Supporting data sharing and collaboration

*Enabling data encryption and authentication

However, USB storage devices also pose significant security risks for users and organi-zations, such as:

*Introducing malware or viruses to laptops and desktops

*Exposing sensitive data to unauthorized access or disclosure

*Losing or stealing data due to device loss or theft

*Violating security policies or regulations

Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of

users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4.
Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5.
References: 1:
Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

NEW QUESTION: 351
在哪一種雲端模式中，雲端服務購買者承擔最多的安全責任？
A. 災難復原即服務 (DRaaS)
B. 基礎設施即服務 (IaaS)
C. 平台即服務 (PaaS)
D. 軟體即服務 (SaaS)
Answer: (SHOW ANSWER)
Infrastructure as a Service (IaaS) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment.
In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page
140-1411

NEW QUESTION: 352
下列哪一項可以最全面地洞察組織面臨的持續威脅？
A. 業務影響分析 (BIA)

B. 風險登記冊
C. 滲透測試
D. 漏洞評估
Answer: (SHOW ANSWER)
A risk register is a document that records and tracks the information security risks facing an organization, such as their sources, impacts, likelihoods, responses, and statuses. A risk register provides the most comprehensive insight into ongoing threats facing an organization, as it covers both internal and external threats, as well as their current and potential effects on the organization's assets, processes, and objectives. A risk register also helps to prioritize and monitor the risk mitigation actions and controls, and to communicate the risk information to relevant stakeholders. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a business impact analysis (BIA) is a process that identifies and evaluates the critical business functions, assets, and dependencies of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA does not provide a comprehensive insight into ongoing threats facing an organization, as it focuses more on the consequences of the threats, rather than their sources, likelihoods, or responses. A BIA is mainly used to support the business continuity and disaster recovery planning, rather than the information security risk management.
Option C is not the best answer because penetration testing is a method of simulating a malicious attack on an organization's IT systems or networks, to evaluate their security posture and identify any vulnerabilities or weaknesses that could be exploited by real attackers. Penetration testing does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers a specific scope, target, and scenario, rather than the whole range of threats, sources, and impacts. Penetration testing is mainly used to validate and improve the technical security controls, rather than the information security risk management.
Option D is not the best answer because vulnerability assessment is a process of scanning and analyzing an organization's IT systems or networks, to detect and report any flaws or gaps that could pose a security risk.
Vulnerability assessment does not provide a comprehensive insight into ongoing threats facing an organization, as it only covers the technical aspects of the threats, rather than their business, legal, or regulatory implications. Vulnerability assessment is mainly used to identify and remediate the security weaknesses, rather than the information security risk management. References = CISM Review Manual 15th Edition1, pages 258-259; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 306.
A risk register provides the MOST comprehensive insight into ongoing threats facing an organization. This is because a risk register is a document that records and tracks the identified risks, their likelihood, impact, mitigation strategies, and status. A risk register helps an organization to monitor and manage the threats that could affect its objectives, assets, and operations. A risk register also helps an organization to prioritize its response efforts and allocate its resources accordingly.

NEW QUESTION: 353
在對系統進行安全控制評估時，下列哪一項是最重要的？
A. 安全文檔
B. 控制規範
C. 保證測試計劃
D. 掃描工具
Answer: (SHOW ANSWER)

NEW QUESTION: 354
對於資安經理來口，在製定針對勒索軟體攻擊的業務連續性計畫(BCP) 時，下列哪一項是最重要的考慮因素？
A. 備份離線維護並定期測試。
B. 生口資料在主站點和輔助站點之間持續複製。
C. 受影響的網路可以在網路交換器層級分離。
D. 備份在多個站點維護並定期審口。
Answer: (SHOW ANSWER)

NEW QUESTION: 355
進行日誌分析屬於事件管理生命週期的哪個階段？
A. 事後
B. 收容
C. 檢測
D. 規劃
Answer: (SHOW ANSWER)
Log analysis is a core detection activity (C) within the incident management lifecycle. Logs provide evidence of abnormal activity, policy violations, or indicators of compromise that enable security teams to identify potential incidents. While logs may also be reviewed during post-incident analysis, their primary role in the lifecycle is to detect events and trigger incident response. Containment (B) focuses on limiting damage after an incident is confirmed, and planning (D) involves preparation activities such as procedures and roles. CISM emphasizes strong detection capabilities-including log monitoring, SIEM, and alerting-as essential to reducing mean time to detect (MTTD) and limiting business impact.
References: ISACA CISM Review Manual (Incident management-lifecycle phases, detection and monitoring); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 356
在分析新出現的風險和威脅情勢時，資訊安全經理應該首先：
A. 將威脅對應到業務資口。
B. 回顧口業口的歷史威脅。
C. 確定新出現的威脅的來源。

D. 確定威脅發生時的影響。
Answer: (SHOW ANSWER)

NEW QUESTION: 357
業務系統更新後執行漏洞評估的主要目標是什麼？
A. 確定營運損失。
B. 改善變更控制流程。
C. 更新威脅態勢。
D. 檢口控制措施的有效性
Answer: (SHOW ANSWER)
The primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1.
A business system update is a process of modifying or enhancing an information system to improve its functionality, performance, security, or compatibility. A business system update may introduce new features, fix bugs, patch vulnerabilities, or comply with new standards or regulations2. Performing a vulnerability assessment following a business system update is important because it helps to:
*Review the effectiveness of controls that are implemented to protect the information sys-tem from threats and risks
*Identify any new or residual vulnerabilities that may have been introduced or exposed by the update
*Evaluate the impact and likelihood of potential incidents that may exploit the vulnerabili-ties
*Prioritize and implement appropriate actions to address the vulnerabilities
*Verify and validate the security posture and compliance of the updated information sys-tem
Therefore, the primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls that are designed to ensure the confidentiality, integrity, and availability of the information system and its data. The other options are not the primary objectives of performing a vulnerability as-sessment following a business system update. Determining operational losses is not an objective, but rather a possible consequence of not performing a vulnerability as-sessment or not addressing the identified vulnerabilities. Improving the change control process is not an objective, but rather a possible outcome of performing a vulnerability assessment and incorporating its results and recommendations into the change man-agement cycle. Updating the threat landscape is not an objective, but rather a prereq- uisite for performing a vulnerability assessment that requires using up-to-date sources of threat intelligence and vulnerability information. References: 1: Vulnerability As-sessment - NIST 2: System Update - Techopedia : Vulnerability Assessment vs Penetra-tion Testing - Imperva : Change Control Process - NIST :
Threat Landscape - NIST

NEW QUESTION: 358
確保經常遇到的事件反映在使用者安全意識培訓計劃中的最佳方法是包括：
A. 離職面談的結果。
B. 之前的訓練課程。
C. 幫助台請求的範例。
D. 安全調口問卷的答案。
Answer: (SHOW ANSWER)
The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users' knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:
* Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users' needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.
* Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users' satisfaction, performance, or behavior.
* Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and appreciate the efforts and contributions of the users and the help desk staff in reporting, responding, or resolving the incidents, and to

encourage and motivate them to continue their involvement and participation in information security.
The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information.
Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents that the users may encounter or experience12. References = Information Security Awareness Training: Best Practices - Infosec Resources, How to Create an Effective Security Awareness Training Program - Infosec Resources, Security Awareness Training: How to Build a Successful Program - ISACA, Security Awareness Training: How to Educate Your Employees - ISACA

NEW QUESTION: 359
資訊安全經理了解到 IT 人員沒有遵守資訊安全策略，因為這會導致流程效率低落 資訊安全經理首先該做什麼？
A. 在 IT 職能部門口進行使用者意識培訓。
B. 建議 IT 更新資訊安全政策和程序。
C. 確定與不遵守政策相關的風險。
D. 請口部稽核對政策制定流程進行審口，
Answer: (SHOW ANSWER)
The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

NEW QUESTION: 360
下列哪一項會導致最精確的控制評估？
A. 成熟的變更管理流程
B. 高階管理層支持
C. 明確定義的安全策略

D. 突擊測試

Answer: D (LEAVE A REPLY)

Unannounced testing is the most accurate way to assess the effectiveness of controls, as it simulates a real- world scenario and does not allow the staff to prepare or modify their behavior in advance. Mature change management processes, senior management support, and well-defined security policies are all important factors for establishing and maintaining a strong security posture, but they do not directly measure the performance of controls. References = CISM Review Manual, 16th Edition, page 149. CISM Questions, Answers & Explanations Database, question ID 1003.

NEW QUESTION: 361

口部審計發現，許多資訊資口的分類不當 為了糾正分類，應將補救責任分配給：

A. 企業用口。

B. 資訊擁有者。

C. 系統管理員。

D. 高階管理層。

Answer: (SHOW ANSWER)

The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities.

This will improve the efficiency, effectiveness, and consistency of the incident response process. References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 362

下列哪一項是定期更新業務連續性和災難復原文件的主要原因？

A. 強制執行安全性原則要求

B. 維護企業資口庫存

C. 確保滿足審核和合規性要求

D. 確保業務運作的可用性

Answer: (SHOW ANSWER)

The primary reason to regularly update business continuity and disaster recovery documents is to ensure that the plans and procedures are aligned with the current business needs and objectives, and that they can effectively support the availability of business operations in the event of a disaster. Updating the documents also helps to enforce security policy requirements, maintain business asset inventories, and ensure audit and compliance requirements are met, but these are secondary benefits.

References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Business Continuity Planning, Subsection: Business Continuity Plan Maintenance, Page

378.

NEW QUESTION: 363

當 SIEM 標記潛在事件時，應先執行下列哪項操作？

A. 驗證事件不是誤報。

B. 口動事件回應計畫。

C. 將事件回報給企業主。

D. 實施補償控制。

Answer: (SHOW ANSWER)

The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise.

A false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 72, page 19

NEW QUESTION: 364

應對新型和高級攻擊的最有效工具是那些基於以下口容檢測攻擊的工具：

A. 簽名分析。

B. 資料包分析。

C. 滲透測試。

D. 行為分析。
Answer: (SHOW ANSWER)

NEW QUESTION: 365
下列何者最能確定資訊資口的分類？
A. 市場中資訊資口的價口
B. 對業務流程的關鍵性
C. 資料所有者的風險評估
D. 生口資訊資口的成本
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

NEW QUESTION: 366
下列哪一項可以最全面了解組織的資訊安全態勢？
A. 安全成熟度評估結果
B. 組織環境的威脅分析
C. 漏洞評估結果
D. 外部滲透測試結果
Answer: (SHOW ANSWER)
A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture.
"Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models* Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

NEW QUESTION: 367
下列何者最適合向高階管理層傳達資訊風險的訊息？
A. 新興安全技術
B. 風險狀況變化
C. 明確的風險偏好
D. 漏洞掃描進度
Answer: (SHOW ANSWER)

Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2:
Information Risk Management (IRM) [2022 update]

NEW QUESTION: 368
在實施自帶設備 (BYOD) 計劃之前，最重要的是：
A. 選擇行動裝置管理 (MDM) 軟體。
B. 針對所要求的申請調□員工。
C. 制定可接受的使用政策。
D. □看目前使用的應用程式。
Answer: (SHOW ANSWER)
Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non- compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.
References = CISM Review Manual, 16th Edition, page 197

NEW QUESTION: 369
當安全人員發生組織變動時，下列何者最能支援資訊安全管理？
A. 正式製定安全策略和計劃
B. 為員工製定意識計劃
C. 確保安全流程的最新記錄
D. 在安全營運團隊□建立流程
Answer: (SHOW ANSWER)
Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational

changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION: 370

組織需要遵守新的安全事件回應要求。資訊安全經理應該先執行下列哪一項操作？

A. 為新的事件回應計畫建立業務案例。

B. 修改現有的事件回應計畫。

C. 進行差距分析。

D. 評估對預算的影響,

Answer: C (LEAVE A REPLY)

Before implementing any changes to the security incident response plan, the information security manager should first conduct a gap analysis to identify the current state of the plan and compare it with the new requirements. A gap analysis is a systematic process of evaluating the differences between the current and desired state of a system, process, or program. A gap analysis can help to identify the strengths and weaknesses of the existing plan, the gaps that need to be addressed, the priorities and dependencies of the actions, and the resources and costs involved. A gap analysis can also help to create a business case for the changes and justify the investment. A gap analysis can be conducted using various methods and tools, such as frameworks, standards, benchmarks, questionnaires, interviews, audits, or tests1234.

References =

* CISM Review Manual 15th Edition, page 1631
* CISM certified information security manager study guide, page 452
* How To Conduct An Information Security Gap Analysis3
* PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS4

NEW QUESTION: 371

依安全等級標註資訊：

A. 提高人們安全處理資訊的可能性。

B. 減少所需對策的數量和類型。

C. 減少為每個分類確定基線控制的需要。

D. 如果資訊處理不安全，會影響後果

Answer: (SHOW ANSWER)

Labeling information according to its security classification enhances the likelihood of people handling information securely. Security classification is a process of categoriz-ing information based on its level of sensitivity and importance, and applying appropri-ate security controls based on the level of risk associated with that infor-mation1. Labeling is a process of marking the information with the appropriate classifi-cation level, such as public, internal, confidential, secret, or top secret2. The purpose of labeling is to inform the users of the information about its value and protection re-quirements, and to guide them on how to handle it securely. Labeling can help users to:

*Identify the information they are dealing with and its classification level

*Understand their roles and responsibilities regarding the information
*Follow the security policies and procedures for the information
*Avoid unauthorized access, disclosure, modification, or destruction of the information
*Report any security incidents or breaches involving the information
Labeling can also help organizations to:
*Track and monitor the information and its usage
*Enforce access controls and encryption for the information
*Audit and review the compliance with security standards and regulations for the infor-mation
*Educate and train employees and stakeholders on information security awareness and best practices Therefore, labeling information according to its security classification enhances the likelihood of people handling information securely, as it increases their awareness and accountability, and supports the implementation of security measures. The other op-tions are not the primary benefits of labeling information according to its security clas-sification. Reducing the number and type of countermeasures required is not a benefit, but rather a consequence of applying security controls based on the classification lev-el. Reducing the need to identify baseline controls for each classification is not a bene-fit, but rather a prerequisite for labeling information according to its security classifica-tion. Affecting the consequences if information is handled insecurely is not a benefit, but rather a risk that needs to be managed by implementing appropriate security con-trols and incident response procedures. References: 1: Information Classification - Ad-visera 2:
Information Classification in Information Security - GeeksforGeeks : Infor-mation Security Policy - NIST :
Information Security Classification Framework - Queensland Government

NEW QUESTION: 372
一家在全球開展業務的組織正計劃利用第三方服務提供者來處理薪資資訊。下列哪一個問題為組織帶來了最大的風險？
A. 第三方沒有可供審口的獨立控制評估。
B. 第三方未提供遵守資料口生地當地法規的證據。
C. 第三方合約不包含違約情況下的賠償條款。
D. 第三方的服務等級協定 (SLA) 不包含正常運作時間的保證。
Answer: (SHOW ANSWER)
The third party's lack of compliance with local regulations poses the greatest risk to the organization, as it may expose the organization to legal, regulatory, or reputational consequences, such as fines, sanctions, lawsuits, or loss of customer trust. Payroll information is considered sensitive personal data that may be subject to different privacy and security laws depending on the jurisdiction where it is generated, processed, or stored. Therefore, the organization should ensure that the third party adheres to the applicable regulations and standards, and obtains the necessary certifications or attestations to demonstrate compliance. References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task

1.22; Ensuring Vendor Compliance and Third-Party Risk Mitigation; How to Manage Access Risk Regarding Third-Party Service Providers

NEW QUESTION: 373
下列哪一項是遏制 Web 應用程式防火牆偵測到的 SQL 注入攻擊的最佳方法？
A. 強制更改 SQL 資料庫的密碼。
B. 重新設定網頁應用程式防火牆以阻止攻擊。
C. 更新 Web 應用程式防火牆上的偵測模式。
D. 阻止攻擊來源的 IP。
Answer: (SHOW ANSWER)
According to the CISM Review Manual, one of the best ways to contain an SQL injection attack that has been detected by a web application firewall is to reconfigure the web application firewall to block the attack.
This means that the web application firewall should be updated with the latest detection patterns and rules that can identify and prevent SQL injection attacks. By doing so, the web application firewall can reduce the impact and damage of the attack, and prevent further exploitation of the vulnerable database1 The other options are not as effective as reconfiguring the web application firewall to block the attack. Force password changes on the SQL database is a reactive measure that does not address the root cause of the problem, and may cause data loss or corruption if not done properly. Updating the detection patterns on the web application firewall is a preventive measure that can help to detect SQL injection attacks, but it does not stop them from happening in the first place. Blocking IPs from where the attack originates is a defensive measure that can limit or stop some SQL injection attacks, but it does not protect all possible sources of malicious traffic, and may also affect legitimate users or applications1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 32-33...

NEW QUESTION: 374
下列哪一項是事件後檢討活動的最重要目標？
A. 證據蒐集
B. 持續改進
C. 事件分類
D. 事件文檔
Answer: (SHOW ANSWER)
The primary goal of post-incident review (PIR) is continuous improvement. After an incident has been contained, eradicated, and systems recovered, a formal review helps identify:
What went wrong or could have been done better
What controls failed or were missing
How the response process can be improved
The goal is not only to learn from the incident but also to enhance incident response capabilities, update plans, and prevent future occurrences.

"Post-incident reviews are a key activity for improving incident response processes. The goal is continuous improvement and prevention of repeat incidents."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-Incident Activities* While incident documentation and evidence collection are components of the process, they are supportive to the broader strategic objective: learning and improving the overall security posture.

NEW QUESTION: 375
下列哪一項是保護儲存在雲端中的客口個人資訊的最佳控制措施？
A. 及時刪除數位記錄
B. 適當的資料匿名化
C. 強加密法
D. 強大的實體存取控制
Answer: (SHOW ANSWER)
Strong encryption methods are the BEST control to protect customer personal information that is stored in the cloud, because they help to prevent unauthorized access, disclosure, modification, or deletion of the data by encrypting it at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data. Encryption can help to protect the confidentiality, integrity, and availability of the data, as well as to comply with legal and regulatory requirements.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Encryption is the process of transforming data into an unreadable format using a secret key or algorithm." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Encryption can help to protect the confidentiality, integrity, and availability of data, as well as to comply with legal and regulatory requirements for data protection." Saas Data Security: Protecting Your Customers' Information In The Cloud - Fresent's Blog: "Encryption and Data Protection: One of the most effective ways to protect sensitive data in the cloud is to encrypt it both at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data."

NEW QUESTION: 376
應防止欺騙，因為它可能用於：
A. 透過偽造寄件者地址非法進入安全系統，
B. 預測出現選項時程式將分支的方式
C. 收集資訊、追蹤流量並識別網路漏洞。
D. 捕獲透過網路傳輸的密碼等訊息
Answer: (SHOW ANSWER)
Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or

something else to deceive or manipulate the recipient or target. Spoofing can be applied to various communication channels, such as emails, websites, phone calls, IP addresses, or DNS servers. One of the common goals of spoofing is to gain unauthorized access to a secure system by faking the sender's address, such as an email address or an IP address. For example, an attacker may spoof an email address of a trusted person or organization and send a phishing email that contains a malicious link or attachment. If the recipient clicks on the link or opens the attachment, they may be redirected to a fake website that asks for their credentials or downloads malware onto their device. Alternatively, an attacker may spoof an IP address of a trusted source and send packets to a secure system that contains malicious code or commands. If the system accepts the packets as legitimate, it may execute the code or commands and compromise its security. Therefore, gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented.
References:
* https://www.kaspersky.com/resource-center/definitions/spoofing
* https://www.cisa.gov/resources-tools/resources/business-case-security
* https://www.avast.com/c-spoofing

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 377
在呈現風險評估結果時，下列何者將為高階管理層提供最大價□？
A. 提供技術風險評估報告
B. 將風險對應到現有控制措施
C. 將風險對應到安全分類方案
D. 在熱圖上□明風險
Answer: (SHOW ANSWER)

NEW QUESTION: 378
某組織最近□動了業務連續性計劃(BCP)。事件發生期間，員工都收到了通知，但部分員工並未完全按照溝通計畫執行。防止此類事件再次發生的最佳方法是什麼？
A. 加強業務連續性計畫中的外部溝通指令
B. 與合適的員工一起進行桌面測試
C. 激勵員工遵守計劃
D. 更新業務影響分析(BIA)

Answer: (SHOW ANSWER)
Tabletop testing with appropriate employees (B) is the best way to prevent recurrence because it reinforces roles, communication paths, and expectations through realistic practice. CISM stresses regular testing and exercises to ensure plans are understood and executable under pressure.
Updating the BIA (D) or incentivizing behavior (C) does not address understanding gaps.
Enhancing instructions (A) alone is insufficient without practice.
References: ISACA CISM Review Manual (Program management-BCP testing and exercises); CISM Exam Content Outline (Domain 3).

NEW QUESTION: 379
在對一個關鍵系統進行資訊安全風險評估後，發現了幾個重大問題 下列哪一項對於資安經理來□最重要？
A. 風險已報告給業務部門的高階管理層
B. 風險已上報至 IT 部門進行補救
C. 風險傳達至中央風險職能
D. 風險已輸入組織的風險登記冊
Answer: D (LEAVE A REPLY)
Recording risks in the risk register ensures visibility, accountability, and tracking. This formal documentation is essential for assigning ownership, determining treatment strategies, and ensuring ongoing governance.
A risk that is not entered into the register may go unaddressed. This step supports structured risk tracking and compliance with governance practices.
"The risk register is the primary tool used to track, prioritize, assign, and monitor risks and their treatment. It forms the basis of a structured risk management program."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Documentation and Communication*

NEW QUESTION: 380
下列何者最有利於制定全面的資訊安全政策？
A. 與已建立的資訊安全框架保持一致
B. 已建立的□部稽核計劃
C. 安全關鍵績效指標 (KPI)
D. 近期資訊安全事件回顧
Answer: (SHOW ANSWER)
Alignment with an established information security framework is the BEST way to facilitate the development of a comprehensive information security policy, because it provides a consistent and structured approach to define, implement, and maintain the policy across the organization. An information security framework is a set of best practices, standards, and guidelines that help to ensure the effectiveness, efficiency, and compliance of the information security policy.
References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "An information security framework is a set of best practices, standards, and guidelines that provide a consistent and structured approach to information security governance." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "The information security policy should be aligned with an established information security framework to ensure its effectiveness, efficiency, and compliance."

NEW QUESTION: 381
一家組織認為修復關鍵應用程式中的安全漏洞成本過高，不可行，但對業務的影響卻十分重大下列哪一項是最適合的風險處理方案？
A. 為應用程式實施補償控制。
B. 購買網路安全保險。
C. 接受繼續使用該應用程式所帶來的風險。
D. 停止使用該應用程式。
Answer: (SHOW ANSWER)

NEW QUESTION: 382
下列哪一項應該是確定資口價口的主要依據？
A. 更換資口的成本
B. 資口不可用時的業務成本
C. 資口的原始成本減去折舊
D. 總擁有成本 (TCO)
Answer: B (LEAVE A REPLY)
The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. References = CISM Review Manual 15th Edition, page 64, page 65.

NEW QUESTION: 383
下列哪一項是高階管理層支援為關鍵應用程式開發監控系統的業務案例的最佳理由？
A. 一位業口同行最近遇到了類似應用程式的漏洞。
B. 可以複製該系統以用於其他用例。
C. 實施系統的成本小於停機的影響。
D. 解決方案在組織的風險承受範圍口。

Answer: (SHOW ANSWER)

A monitoring system for a critical application can help detect and prevent incidents that could affect the availability, integrity, and confidentiality of the application and its data. The impact of downtime could include loss of revenue, reputation, customer satisfaction, and regulatory compliance. Therefore, the cost of implementing the system should be justified by the potential savings from avoiding or minimizing these impacts.

References = CISM Review Manual, 15th Edition, page 173; An Introduction to Metrics, Monitoring, and Alerting; Business-critical applications: What are they and how do you protect them from cyberattack?

NEW QUESTION: 384

某組織的行銷部門想要使用線上協作服務，該服務不符合資訊安全策略，已進行風險評估，並尋求風險接受。風險接受的批准應由以下人員提供：

A. 首席風險長 (CRO)。

B. 企業高階主管。

C. 資訊安全經理。

D. 合規官。

Answer: (SHOW ANSWER)

Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.

The chief risk officer (CRO) (A) is a senior executive who oversees the organization's risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The information security manager © is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

NEW QUESTION: 385
在建立必須遵守適用的資料隱私法規的新資料保護計畫時，應先執行下列哪項操作？
A. 評估資料保護所需的隱私技術。
B. 加密系統和網路上儲存的所有個人資料。
C. 更新紀律流程以解決侵犯隱私的問題。
D. 建立儲存個人資料的系統清單。
Answer: (SHOW ANSWER)
= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:
* Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.
* Assess the risks and impacts associated with the personal data, and the compliance requirements and obligations under the applicable data privacy regulations.
* Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.
* Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.
* Monitor and review the performance and effectiveness of the data protection program, and report and resolve any data breaches or incidents.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Data Protection, pages 202-2051; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 71, page 662.

NEW QUESTION: 386
下列哪一項主要由資口分類決定？
A. 資口所需的保險範圍
B. 資口所需的保護等級
C. 資口替換的優先級
D. 資口重置成本
Answer: (SHOW ANSWER)
Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. References = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

NEW QUESTION: 387
下列哪一項是成功資訊安全文化的最佳標誌？
A. 定期進行滲透測試並修復發現的結果。
B. 最終使用者知道如何辨識和報告事件。
C. 依工作職能為個人指派角色。
D. 分配給資訊安全的預算是充足的。
Answer: (SHOW ANSWER)
The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Culture, page 281.

NEW QUESTION: 388
下列哪一項對執行災難復原計畫 (DRP) 的能力有最大的正面影響？
A. 將計畫儲存在異地位置
B. 向所有利害關係人傳達該計劃
C. 定期更新計劃
D. 對計劃進行演練
Answer: (SHOW ANSWER)
A walk-through of the disaster recovery plan (DRP) is a method of testing the plan by simulating a disaster scenario and having the participants review their roles and responsibilities, as well as the procedures and resources required to execute the plan. A walk-through has the greatest positive impact on the ability to execute the DRP, as it helps to identify and resolve any gaps, errors, or inconsistencies in the plan, as well as to enhance the awareness and readiness of the stakeholders involved in the recovery process. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.3.2.21

NEW QUESTION: 389
□部審計報告了一些不符合監管要求的資訊安全問題。資訊安全經理首先該做什麼？
A. 建立安全例外。
B. 執行差距分析以確定所需資源。
C. 執行漏洞評估。
D. 評估業務營運的風險。
Answer: (SHOW ANSWER)
The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.
References = CISM Review Manual, 16th Edition, page 48

NEW QUESTION: 390
平衡記分卡最有效地實現資訊安全：
A. 風險管理
B. 專案管理
C. 治理
D. 效能
Answer: (SHOW ANSWER)

A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it.
A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2. It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

NEW QUESTION: 391
這違反了禁止在辦公室使用攝影機的政策，向員工發放了配備網路攝影機的智慧型手機和平板電腦。下列哪一項應該是資訊安全經理的首要行動方案？
A. 修改政策。
B. 執行根本原因分析。
C. 進行風險評估，
D. 傳達可接受的使用政策。
Answer: (SHOW ANSWER)
= The information security manager's first course of action in this situation should be to conduct a risk assessment, which is a process of identifying, analyzing, and evaluating the information security risks that arise from the violation of the policy prohibiting the use of cameras at the office. The risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate use of the cameras on the smartphones and tablet computers, such as capturing, transmitting, or disclosing sensitive or confidential information, compromising the privacy or security of the employees, customers, or partners, or violating the legal or regulatory requirements. The risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to disable, restrict, or monitor the camera usage, enforcing the policy compliance and awareness, or revising the policy to reflect the current business needs and environment. The risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the policy and the risk management process.
Revising the policy, performing a root cause analysis, and communicating the acceptable use policy are all possible courses of action that the information security manager can take after conducting the risk assessment, but they are not the first ones. Revising the policy is a process of updating and modifying the policy to align with the business objectives and strategy, to address the changes and challenges in the business and threat environment, and to incorporate the feedback and suggestions from the risk assessment and the stakeholders.
Performing a root cause analysis is a process of investigating and identifying the underlying causes and factors that led to the violation of the policy, such as the lack of awareness, training, or enforcement, the inconsistency or ambiguity of the policy, or the conflict or gap between the policy and the business requirements or expectations. Communicating the acceptable use policy is a process of informing and educating the employees and the other users of the smartphones

and tablet computers about the purpose, scope, and content of the policy, the roles and responsibilities of the users, the benefits and consequences of complying or violating the policy, and the methods and channels of reporting or resolving any policy issues or incidents. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1482

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 392
在恢復需要完全重建的受損系統時，應先考慮下列哪一項？
A. 補丁管理文件
B. 網路系統日誌
C. 設定管理文件
D. 入侵偵測系統 (IDS) 日誌
Answer: (SHOW ANSWER)
Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files are essential to recover a compromised system that needs a complete rebuild, as they can help to restore the functionality, security, and performance of the system. Without patch management files, the system may not be able to run properly or securely, and may expose the organization to further risks or vulnerabilities. Network system logs, configuration management files, and intrusion detection system (IDS) logs are also important for recovering a compromised system, but they should be considered after patch management files. Network system logs can help to identify the source and scope of the attack, configuration management files can help to restore the original settings and policies of the system, and IDS logs can help to detect any malicious activities or anomalies on the system. References = CISM Review Manual, 16th Edition, pages 193-1941; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 672

NEW QUESTION: 393
使用存在已知漏洞的 Web 應用程式時，下列哪一項是最佳行動方案？
A. 安裝反間諜軟體。
B. 監控應用程式層級日誌。
C. 部署基於主機的入侵偵測。
D. 部署應用程式防火牆。

Answer: (SHOW ANSWER)

NEW QUESTION: 394
除了高階主管支援和業務協調之外，下列何者對於資訊安全治理最重要？
A. 安全的所有權
B. 遵守政策
C. 系統的可審核性
D. 培訓資源分配
Answer: (SHOW ANSWER)
Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. In addition to executive sponsorship and business alignment, a critical factor for effective information security governance is ownership of security, which means that the roles and responsibilities for information security are clearly defined and assigned to the appropriate stakeholders, such as business owners, information owners, information custodians, and users. Ownership of security also implies accountability for the protection of information assets and the management of security risks.
References: https://www.isaca.org/credentialing/cism
https://www.nist.gov/publications/information-security- handbook-guide-managers

NEW QUESTION: 395
應先更新下列哪一項，以適應影響目前資訊安全控制的新監管要求？
A. 控制矩陣
B. 風險登記冊
C. 業務影響分析 (BIA)
D. 資訊安全策略
Answer: (SHOW ANSWER)

NEW QUESTION: 396
託管組織的資料中心容納伺服器、應用程式
為組織制定實體存取控制策略的最佳方法？
A. 口看客口的安全策略。
B. 進行風險評估以確定安全風險和緩解控制措施。
C. 為每個系統和應用程式製定存取控制要求。
D. 設計單一登入 (SSO) 或聯合存取。
Answer: (SHOW ANSWER)
= The best approach for developing a physical access control policy for the organization is to conduct a risk assessment to determine the security risks and mitigating controls that are relevant and appropriate for the organization's data center. A risk assessment is a process of identifying, analyzing, and evaluating the information security risks that could affect the availability, integrity,

or confidentiality of the servers, applications, and data that are hosted in the data center. A risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate physical access to the data center, such as theft, damage, sabotage, or espionage, and the potential consequences for the organization and its customers, such as service disruption, data loss, data breach, or legal liability. A risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to prevent, detect, or respond to the physical access incidents, such as locks, alarms, cameras, guards, badges, or logs. A risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the physical access control policy and the risk management process.
Reviewing customers' security policies, developing access control requirements for each system and application, and designing single sign-on (SSO) or federated access are all possible steps that the organization can take after conducting the risk assessment, but they are not the best ones. Reviewing customers' security policies is a process of understanding and complying with the customers' expectations and requirements for the security of their servers, applications, and data that are hosted in the data center, and ensuring that the organization's physical access control policy is consistent and compatible with them. Developing access control requirements for each system and application is a process of defining and implementing the specific rules and criteria for granting or denying the physical access to the servers and applications that are hosted in the data center, based on the roles, responsibilities, and privileges of the users, and the sensitivity and criticality of the systems and applications. Designing single sign-on (SSO) or federated access is a process of enabling and facilitating the authentication and authorization of the users who need to access the servers and applications that are hosted in the data center, by using a single or shared identity and credential across multiple systems and domains. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1542

NEW QUESTION: 397
下列何者最有助於在組織口實現所需的資訊安全文化？
A. 資訊安全意識培訓與活動
B. 有效的資訊安全政策和程序
C. 資訊安全角色與職責的委派
D. 對適當的資訊安全相關行為的激勵
Answer: (SHOW ANSWER)
Information security awareness training and campaigns are the best way to enable the desired information security culture within an organization because they help to educate, motivate and influence the behavior and attitude of the employees towards information security. They also help to raise the awareness of the risks, threats and best practices of information security among the staff and stakeholders.
References = Organizational Culture for Information Security: A Systemic Perspective on the Articulation of Human, Cultural and Social Systems, CISM Exam Content Outline

NEW QUESTION: 398
在網路事件回應的根除階段，下列哪一項活動最適合進行？
A. 緩解被利用的漏洞以阻止未來事件的發生。
B. 估計事件造成的損失金額。
C. 隔離受影響的系統以防止進一步損壞
D. 恢復受影響的系統以進行正常運作。
Answer: (SHOW ANSWER)

NEW QUESTION: 399
在建立事件回應計畫時，下列哪一項最重要？
A. 識別易受攻擊的資料資口
B. 辨識事件的構成
C. 記錄事件通知與升級流程
D. 與風險評估流程保持一致
Answer: (SHOW ANSWER)
= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION: 400
將安全風險管理整合到組織中時，最重要的是確保：
A. 業務部門核准風險管理方法。
B. 定義風險處理流程。
C. 記錄並瞭解資訊安全策略。
D. 風險管理方法遵循既定框架。
Answer: (SHOW ANSWER)
When integrating security risk management into an organization, it is most important to ensure that the risk management methodology follows an established framework, such as ISO 31000, NIST SP 800-30, or COBIT. This is because a framework provides a consistent and structured approach to identify, assess, treat, and monitor risks, and to align the risk management process with the organization's objectives, culture, and governance. A framework also helps to ensure compliance with relevant standards and regulations, and to facilitate communication and reporting of risks to stakeholders.
References: The CISM Review Manual 2023 states that "the risk management methodology should follow an established framework that provides a consistent and structured approach to risk

management" and that "the framework should be aligned with the enterprise's objectives, culture, and governance, and should comply with applicable standards and regulations" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "The risk management methodology follows an established framework is the correct answer because it is the most important factor to ensure the successful integration of security risk management into an organization, as it provides a common language and process for managing risks across the organization" (p. 29). Additionally, the article Integrating Risk Management into Business Processes from the ISACA Journal 2018 states that "a risk management framework provides a systematic and comprehensive approach to risk management that covers the entire risk management cycle, from risk identification to risk monitoring and reporting" and that "a risk management framework should be aligned with the organization's strategy, culture, and governance, and should follow recognized standards and best practices, such as ISO 31000, NIST SP 800-30, or COBIT" (p. 1)

NEW QUESTION: 401
在製定資口分類計畫時，應先完成下列哪一個步驟？
A. 將每個資口分類。
B. 建立庫存。&
C. 為數位版權管理工具建立商業案例。
D. 實施資料遺失防護 (OLP) 系統。
Answer: (SHOW ANSWER)
Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified.
An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12.
Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12.
Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. References = 1:

CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4:
What is Data Loss Prevention (DLP)? - Definition from Techopedia4

NEW QUESTION: 402
在進行全功能連續性測試之前，資安經理需要驗證下列哪一項最重要？
A. 企業接受的風險已記錄在案
B. 已確定負責復原的團隊和個人
C. 復原和事件回應計畫的副本保存在異地
D. 事件回應和復原計畫以簡單的語言記錄
Answer: (SHOW ANSWER)
Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities.
This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

NEW QUESTION: 403
一家醫院的關鍵伺服器已被勒索軟體加密。如果沒有這台伺服器，醫院就無法有效運作，下列哪一項最能有效讓醫院避免支付贖金？
A. 針對勒索軟體的員工培訓
B. 經過適當測試的離線備份系統
C. 持續的伺服器複製過程
D. 正確設定的防火牆
Answer: (SHOW ANSWER)
The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures.
Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware.

However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable.
A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 404
組織的資訊安全經理正在對發生以下事件的安全事件進行事後審口：
* 不良行為者透過暴力破解管理密碼闖入關鍵業務 FTP 伺服器
* 託管伺服器的第三方服務提供者向服務台發送了自動警報訊息，但被忽略
* 壞人無法存取管理員控制台，但暴露於傳輸到伺服器的加密數據
* 三小時後，不良行為者刪除了FTP 目錄，導致合法客口的傳入FTP 嘗試失敗 透過定期進行事件回應測試可以避免以下哪一項？
A. 忽略警報訊息
B. 伺服器受到威脅
C. 暴力攻擊
D. 被盜數據
Answer: (SHOW ANSWER)
Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. References:
https://www.isaca.org/resources/isaca-journal/issues/2017
/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 405
下列哪一項是確保勒索軟體攻擊後恢復乾淨資料能力的最佳方法？
A. 購買網路保險
B. 加密敏感生口數據

C. 對備份執行完整性檢口
D. 維護多個離線備份
Answer: (SHOW ANSWER)
The best way to ensure the capability to restore clean data after a ransomware attack is to maintain multiple offline backups. Offline backups are backups that are not connected to the network or the internet, and therefore are not accessible by ransomware. Multiple offline backups provide redundancy and allow the organization to choose the most recent and uncorrupted backup to restore the data. Offline backups should be stored in a secure location and tested regularly to ensure their integrity and availability.
Purchasing cyber insurance may help the organization cover some of the costs associated with a ransomware attack, such as ransom payment, data recovery, legal fees, etc., but it does not guarantee the capability to restore clean data. Cyber insurance policies may have exclusions, limitations, or conditions that affect the coverage and reimbursement. Moreover, cyber insurance does not prevent or mitigate the ransomware attack itself, and it may not cover all the losses or damages caused by the attack.
Encrypting sensitive production data may protect the confidentiality of the data from unauthorized access or disclosure, but it does not prevent ransomware from encrypting the data again. Ransomware does not need to decrypt the data to encrypt it, and it may use a different encryption algorithm or key than the one used by the organization. Encrypting production data may also increase the complexity and time required for data recovery, especially if the encryption keys are lost or compromised.
Performing integrity checks on backups may help the organization verify that the backups are not corrupted or tampered with, but it does not ensure the capability to restore clean data after a ransomware attack. Integrity checks are a preventive measure that should be done before the attack, not after. If the backups are already infected or encrypted by ransomware, performing integrity checks will not help to recover the data. Integrity checks should be complemented by other measures, such as isolation, versioning, and offline storage, to protect the backups from ransomware. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3081; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Ransomware recovery: 8 steps to successfully restore from backup3; Ransomware Recovery: 5 Steps to Recover Data4

NEW QUESTION: 406
某商業應用程式中偵測到一個嚴重漏洞，外部攻擊者可以利用該漏洞入侵系統 資訊安全經理的最佳應對措施是什麼？
A. 請業務應用程式擁有者立即套用此修復程式。
B. 實施暫時補救措施
C. 立即關閉應用程式
D. 向業務應用程式擁有者報告風險
Answer: (SHOW ANSWER)

The best course of action is to implement temporary remediation (B) to reduce exposure while a permanent fix is planned and approved. CISM emphasizes balancing risk reduction with business continuity.
Immediate shutdown (C) or unilateral action (A) may disrupt business operations without proper authorization. Reporting the risk (D) is necessary but insufficient on its own. Temporary controls, such as access restrictions or additional monitoring, reduce risk while enabling informed decision-making by the business owner.
References: ISACA CISM Review Manual (Program management-risk response and operational controls); CISM Exam Content Outline (Domain 3).

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 407
在下列情況下，組織最有可能接受不遵守新監管要求的風險：
A. 員工抵制新法規所要求的控制。
B. 監理要求與業務要求相衝突。
C. 不合規的風險超出了組織的風險偏好。
D. 遵守法規的成本超過了潛在的處罰。
Answer: (SHOW ANSWER)
An organization is most likely to accept the risk of noncompliance with a new regulatory requirement when the cost of complying with the regulation exceeds the potential penalties. In such cases, from a cost-benefit perspective, the organization might find it more economical to absorb potential fines or penalties rather than implementing costly controls or processes to comply with the regulation.
"Risk acceptance occurs when the cost of mitigating or transferring the risk exceeds the benefit of the mitigation. This also applies to regulatory noncompliance if the penalties are less than the costs of compliance."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* ISACA's practice questions highlight that risk acceptance is a legitimate treatment when costs outweigh potential penalties or impact.

NEW QUESTION: 408
讓最終用口參與連續性規劃的主要優點是：
A. 更了解特定業務需求。

B. 比資訊安全管理更客觀。
C. 可以看到對業務的整體影響。
D. 可以平衡技術和業務風險。
Answer: (SHOW ANSWER)
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION: 409
資訊安全政策應主要反映與以下方面的一致性：
A. 業界最佳實務。
B. 資料安全標準。
C. 高階管理層意圖。
D. 一個資訊安全框架。
Answer: (SHOW ANSWER)

NEW QUESTION: 410
當得知一項具有重大影響力的新法規即將生效時，全球資訊安全經理首先應該做什麼？
A. 執行差距分析。
B. 執行漏洞評估。
C. 執行業務影響分析 (BIA)。
D. 執行隱私影響評估 (PIA)。
Answer: (SHOW ANSWER)

NEW QUESTION: 411
下列哪一項對資訊資口固有風險的影響最大？
A. 風險承受能力
B. 淨現口 (NPV)
C. 投資報酬率 (ROI)
D. 業務關鍵性
Answer: (SHOW ANSWER)
Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business

criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes. References = CISM Review Manual,
16th Edition, page 971
Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

NEW QUESTION: 412
詳細的業務連續性計劃（BCP）應主要基於：
A. 可用的本地供應商的能力。
B. 經高階管理層驗證的策略。
C. 執行所需的成本和資源。
D. 涵蓋所有應用程式的策略。
Answer: B (LEAVE A REPLY)

NEW QUESTION: 413
漏洞識別的主要目的是：
A. 在漏洞被利用之前修復漏洞
B. 發現控制缺陷
C. 提供用於風險報告的漏洞標識符
D. 優先修復漏洞
Answer: (SHOW ANSWER)
The primary purpose of identifying vulnerabilities is to remediate them before they can be exploited by malicious actors. While risk reporting and prioritization are part of the overall process, the most immediate goal is remediation.
"Vulnerability assessments identify weaknesses that need to be addressed to reduce risk to acceptable levels and prevent potential exploits."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Assessment and Analysis This aligns with ISACA's official practice questions, where vulnerability identification directly aims to prevent exploitation.

NEW QUESTION: 414
維護資訊安全治理框架的組織的主要好處是什麼？
A. 優先考慮資源以最大化投資回報 (ROI)
B. 資訊安全準則在整個企業口傳達_
C. 組織仍符合監理要求。
D. 業務風險已控制在可接受的程度。
Answer: (SHOW ANSWER)

According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.
Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.
According to the Certified Information Security Manager (CISM) Study Manual, "Information security governance provides a framework for managing and controlling information security practices and technologies at an enterprise level. Its primary objective is to manage and reduce risk through a process of identification, assessment, and management of those risks." While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 60-63.

NEW QUESTION: 415
下列哪一項是確定遺留系統中是否有新風險的最佳方法？
A. 頻繁更新風險登記冊
B. 定期進行安全審核
C. 定期進行風險評估
D. 頻繁的安全架構審□
Answer: (SHOW ANSWER)

NEW QUESTION: 416
下列哪一項是軟體開發專案中資訊安全經理的主要角色？
A. 提高安全軟體設計意識
B. 評估並批准安全應用程式架構
C. 在早期設計階段識別不合規情況
D. 辨識軟體安全漏洞
Answer: (SHOW ANSWER)
The primary role of an information security manager in a software development project is to assess and approve the security application architecture. The security application architecture is the design and structure of the software application that defines how the application components

interact with each other and with external systems, and how the application implements the security requirements, principles, and best practices. The information security manager is responsible for ensuring that the security application architecture is aligned with the organization's information security policies, standards, and guidelines, and that it meets the business objectives, functional specifications, and user expectations. The information security manager is also responsible for reviewing and evaluating the security application architecture for its completeness, correctness, consistency, and compliance, and for identifying and resolving any security issues, risks, or gaps. The information security manager is also responsible for approving the security application architecture before the software development project proceeds to the next phase, such as coding, testing, or deployment.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 80, page 742.

NEW QUESTION: 417
一個擁有遠端分支機構的國際組織正在實施一項企業安全策略來管理個人識別資訊 (PII)。下列哪一項應該是資訊安全經理主要關注的問題？
A. 地方法規
B. 資料備份策略
C. 意識計劃的一致性
D. 組織報告結構
Answer: (SHOW ANSWER)
Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

NEW QUESTION: 418
下列哪一項是偵測資訊安全事件最有效的方法？
A. 實施定期安全意識計劃
B. 定期分析安全事件日誌記錄
C. 即時監控網路活動
D. 關鍵風險指標 (KRI) 的閾口設定
Answer: C (LEAVE A REPLY)

NEW QUESTION: 419
在環境快速變化的組織中，業務管理層已經接受了資訊安全風險 對於資安經理來口，最重要的是確保：
A. 記錄變更活動。
B. 定期檢視接受的理由。
C. 接受與業務策略一致。
D. 遵守風險接受架構。
Answer: (SHOW ANSWER)
= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.
References =
CISM Review Manual 15th Edition, page 1131
CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482 CISM Domain 2: Information Risk Management (IRM) [2022 update]3

NEW QUESTION: 420
在審查儲存在異地雲環境中的資料的存取控制時，下列哪一項應該是資訊安全經理的主要關注點？
A. 根據組織結構的變化審口和更新存取控制
B. 實施強密碼原則並強制定期變更密碼
C. 確保僅授予工作職能需要存取權限的個人存取權限
D. 實施強加密協定來保護敏感數據
Answer: (SHOW ANSWER)
The principle of least privilege-ensuring access is granted only to those whose job functions require it-is the primary control for securing data, especially in cloud environments.
"Access to information and systems should be based on the principles of least privilege and need to know, regardless of environment."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Access Control Management ISACA's CISM practice questions consistently highlight this principle as central to effective cloud security.

NEW QUESTION: 421
在與外包第三方簽訂的合約期間口，資訊安全經理需要定期執行下列哪項活動最為關鍵？
A. 參與式災難復原測試
B. 綜合風險評估
C. 服務等級協定 (SLA) 更新

D. 財務協調審口

Answer: (SHOW ANSWER)

Performing comprehensive risk assessments (B) throughout the life of a third-party contract is the most critical activity because risk posture changes over time due to evolving threats, business changes, or control degradation. CISM emphasizes that third-party risk is not static and must be continuously assessed to ensure ongoing alignment with risk appetite. Disaster recovery testing (A) and SLA updates (C) are important but limited in scope. Financial reviews (D) focus on cost rather than security risk. Periodic risk assessments enable timely identification of new risks and ensure appropriate mitigation or escalation.

References: ISACA CISM Review Manual (Governance-third-party risk lifecycle management); CISM Exam Content Outline (Domain 2).

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 422

在起草公共網站的企業隱私權聲明時，必須包括下列哪一項？

A. 有限責任條款

B. 資訊使用口明

C. 資訊加密要求

D. 存取控制要求

Answer: (SHOW ANSWER)

A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

NEW QUESTION: 423

下列哪一項是資訊安全戰略與 &

A. 在定義的服務等級協定 (SLA) 口解決的資訊安全事件的百分比

B. 分配給資訊安全計畫的企業預算百分比

C. 參加過資訊安全意識會議的企業主管人數

D. 資訊安全計畫直接支援的業務目標數量

Answer: (SHOW ANSWER)

The number of business objectives directly supported by information security initiatives is the best indication of information security strategy alignment with the organizational goals and objectives.

This metric shows how well the information security strategy is aligned with the business strategy, and how effectively the information security program is delivering value to the organization. The more business objectives that are supported by information security initiatives, the more aligned the information security strategy is with the organizational goals and objectives.
The other options are not the best indicators of information security strategy alignment, as they do not directly measure the impact or contribution of information security initiatives to the business objectives. The percentage of information security incidents resolved within defined SLAs is a measure of the efficiency and effectiveness of the incident management process, but it does not reflect how well the information security strategy is aligned with the business strategy. The percentage of corporate budget allocated to information security initiatives is a measure of the investment and commitment of the organization to information security, but it does not indicate how well the information security initiatives are aligned with the business objectives or how they are prioritized. The number of business executives who have attended information security awareness sessions is a measure of the awareness and involvement of the senior management in information security, but it does not show how well the information security strategy is aligned with the business strategy or how it supports the business objectives. References = CISM Exam Content Outline | CISM Certification | ISACA, Domain 1, Task 1.1 CISM MASTER CHEAT SHEET - SkillCertPro, Chapter 1, page 2 Certified Information Security Manager (CISM), page 1 Certified Information Security Manager Exam Prep Guide: Aligned with ..., page 1 CISM: Certified Information Security SKILLS COVERED Manager, page 1

NEW QUESTION: 424
下列哪一個業務部門應該擁有身分管理系統的資料？
A. 酷
B. 資訊安全
C. 資訊技術
D. 人力資源 (HR)
Answer: (SHOW ANSWER)

NEW QUESTION: 425
採用軟體即服務 (SaaS) 模式時，下列何者是客口組織的唯一責任？
A. 主機修補
B. 滲透測試
C. 基礎設施強化
D. 資料分類
Answer: (SHOW ANSWER)
Data classification is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model. Data classification is the process of categorizing data based on its sensitivity, value and criticality to the organization. Data classification helps to determine the appropriate level of protection, access control and retention for different types of data. Data classification is an essential part of data governance and risk management, as it enables the

organization to comply with legal and regulatory requirements, protect its intellectual property and reputation, and optimize its data storage and usage costs.
In a SaaS model, the client organization has the least control and responsibility over the cloud infrastructure, platform and application, as these are fully managed by the cloud service provider (CSP). The client organization only has control and responsibility over its own data and users. Therefore, the client organization is responsible for defining and implementing data classification policies and procedures, and ensuring that its data is properly labeled and handled according to its classification level. The client organization is also responsible for educating its users about the importance of data classification and the best practices for data security and privacy.
The other options are not the sole responsibility of the client organization in a SaaS model, as they are either shared with or delegated to the CSP. Host patching, penetration testing and infrastructure hardening are all related to the security and maintenance of the cloud infrastructure and platform, which are the responsibility of the CSP in a SaaS model. The CSP is expected to provide regular updates, patches and fixes to the host operating system, network and application components, and to conduct periodic security assessments and audits to identify and remediate any vulnerabilities or weaknesses in the cloud environment. The client organization may have some responsibility to monitor and verify the CSP's performance and compliance with the service level agreement (SLA) and the cloud security standards and regulations, but it does not have direct control or access to the cloud infrastructure and platform. References = Understanding the Shared Responsibilities Model in Cloud Services - ISACA, Figure 1 CISM Review Manual, Chapter 3, page 121

NEW QUESTION: 426
下列哪一項是評估組織中出現的風險的最大挑戰？
A. 缺乏風險框架
B. 安全控制無效
C. 存在已知漏洞
D. 威脅識別不完整
Answer: (SHOW ANSWER)
The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed. Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment.
References:
* https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.html
* https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging-risk- analysis
* https://projectriskcoach.com/emerging-risks/

NEW QUESTION: 427
下列哪一項是新出現事件的最佳指標？
A. 嘗試修補系統導致錯誤
B. 組織資訊系統中發現的弱點
C. 客口對網站可用性不足的投訴
D. 業界競爭對手最近發生的安全事件
Answer: (SHOW ANSWER)

NEW QUESTION: 428
下列何者最能讓事件回應團隊在初步調口期間確定適當的行動？
A. 團隊的技術能力
B. 事件分類程序
C. 受影響部門的回饋
D. 過去事件的歷史數據
Answer: (SHOW ANSWER)

NEW QUESTION: 429
下列哪一項是公司治理與資訊安全治理之間一致性的最佳證據？
A. 安全關鍵績效指標 (KPI)
B. 專案資源最佳化
C. 定期安全政策審口
D. 高階管理層贊助
Answer: (SHOW ANSWER)
Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the commitment and support of the top-level executives and board members for the information security program.
Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22
Certified Information Security Manager (CISM), page 33

NEW QUESTION: 430
下列哪一項可以最好地確保安全策略在整個業務運作中的應用？
A. 組織標準包含在意識訓練中。

B. 組織標準透過技術控制來執行。
C. 組織標準需要被正式接受。
D. 組織標準記錄在操作程序中。
Answer: (SHOW ANSWER)
= The best assurance that security policies are applied across business operations is that organizational standards are documented in operational procedures. Operational procedures are the specific steps and actions that need to be taken to implement and comply with the security policies and standards. They provide clear and consistent guidance for the staff members who are responsible for performing the security tasks and functions. They also help to ensure that the security policies and standards are aligned with the business objectives and processes, and that they are measurable and auditable. Documenting the organizational standards in operational procedures can help to improve the security awareness, accountability, and performance of the staff members, and to reduce the risks of errors, deviations, and violations. The other options are not the best assurance because they are either too general or too specific. Organizational standards are included in awareness training (A) is a good practice to educate the staff members about the security policies and standards, but it does not guarantee that they will follow them or understand how to apply them in their daily operations. Organizational standards are enforced by technical controls (B) is a way to automate and monitor the compliance with the security policies and standards, but it does not cover all the aspects of security that may require human intervention or judgment. Organizational standards are required to be formally accepted © is a way to obtain the commitment and support from the staff members for the security policies and standards, but it does not ensure that they will adhere to them or know how to execute them in their work activities. References = CISM Review Manual 2022, pages 24-25, 28-29; CISM Item Development Guide 2022, page 9; Policies, Procedures, Standards, Baselines, and Guidelines | CISSP Security- Management Practices | Pearson IT Certification

NEW QUESTION: 431
下列哪一項措施最能幫助服務台辨識資訊安全事件？
A. 訓練服務台人員審口通話記錄。
B. 請服務台參與事後檢討。
C. 向服務台提供安全事件的標準。
D. 將服務台成員納入安全事件回應團隊。
Answer: (SHOW ANSWER)
Providing the help desk with clear criteria for what constitutes a security incident (C) is the most effective way to enable early recognition. In CISM incident management, frontline functions such as the help desk are critical for early detection and escalation, but only if they understand what events require security attention.
Reviewing call logs (A) or participating in post-incident reviews (B) improves awareness after the fact, not recognition in real time. Including help desk staff on the response team (D) is

unnecessary and impractical for incident identification. Clearly defined criteria and escalation thresholds empower the help desk to act quickly and consistently.
References: ISACA CISM Review Manual (Incident management-incident identification and escalation); CISM Exam Content Outline (Domain 4).

NEW QUESTION: 432
下列哪一項最能確保將安全風險評估納入重大 IT 專案的生命週期？
A. 將風險評估納入口部稽核計劃
B. 對專案經理進行風險評估培訓
C. 將全球安全標準應用於 IT 項目
D. 讓資訊安全經理參與專案指導委員會
Answer: (SHOW ANSWER)

NEW QUESTION: 433
一個組織在最近的災難中遭受了收入損失。下列何者最能幫助組織做好恢復準備？
A. 業務連續性計劃 (BCP)
B. 事件回應計劃
C. 業務影響分析 (BIA)
D. 災難復原計畫 (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 434
一旦為組織的業務部門成功實施了一套安全控制措施，資訊安全經理最重要的是：
A. 準備調整控制項以適應未來的系統升級。
B. 執行測試以將控制性能與行業水平進行比較。
C. 將控制權交給相關企業主。
D. 確保定期測試控制措施的持續效度。
Answer: (SHOW ANSWER)

NEW QUESTION: 435
一位資訊安全經理收到多起跨不同業務部門的安全事件警報，這些事件涉及未經授權存取敏感數據，並可能導致關鍵系統資料外洩 下列哪一項是對這些事件進行合理分類和優先排序的最佳行動方案？
A. 組成事件回應團隊來評估事件
B. 口動危機溝通計劃，通知利害關係人事件
C. 聘請外部事件回應顧問進行獨立調口
D. 根據資料分類標準對事件進行優先排序
Answer: (SHOW ANSWER)
Prioritizing incidents based on data classification standards ensures that the most sensitive and critical data exposures are addressed first, reducing the potential impact on the business.

"The impact of incidents should be evaluated based on the classification and sensitivity of the data involved."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Classification and Prioritization* ISACA practice questions emphasize the importance of using data classification to properly prioritize incident response efforts.

NEW QUESTION: 436
下列哪一項是組織使用災難復原即服務 (DRaaS) 的最佳理由？
A. 它消除了企業執行測試的需要。
B. 它降低了企業的年度成本。
C. 無需維護場外設施。
D. 它將與復原相關的風險轉移給第三方。
Answer: (SHOW ANSWER)

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 437
下列哪一項是成功的資安計畫最重要的因素？
A. 該計劃遵循行業最佳實踐。
B. 該計劃是基於完善的策略。
C. 本計劃具有成本效益且在預算範圍口，
D. 該計劃的重點是風險管理。
Answer: (SHOW ANSWER)
A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources, implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-

developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus. References = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

NEW QUESTION: 438
下列哪一項是向董事會提交有關資訊安全計畫狀況的季度報告的最有效方法？
A. 能力與成熟度評估
B. 安全計畫 KPI 詳細分析
C. 資訊安全儀表板
D. 資訊安全風險登記冊
Answer: (SHOW ANSWER)
An information security dashboard is the most effective way to present quarterly reports to the board on the status of the information security program, because it provides a concise, visual, and high-level overview of the key performance indicators (KPIs), metrics, and trends of the information security program. An information security dashboard can help the board to quickly and easily understand the current state, progress, and performance of the information security program, and to identify any gaps, issues, or areas of improvement. An information security dashboard can also help the board to align the information security program with the organization's business goals and strategies, and to support the decision-making and oversight functions of the board.
A capability and maturity assessment is a way of measuring the effectiveness and efficiency of the information security program, and of identifying the strengths and weaknesses of the program. However, a capability and maturity assessment is not the most effective way to present quarterly reports to the board, because it may not provide a clear and timely picture of the status of the information security program, and it may not reflect the changes and dynamics of the information security environment. A capability and maturity assessment is more suitable for periodic or annual reviews, rather than quarterly reports.
A detailed analysis of security program KPIs is a way of evaluating the performance and progress of the information security program, and of determining the extent to which the program meets the predefined objectives and targets. However, a detailed analysis of security program KPIs is not the most effective way to present quarterly reports to the board, because it may be too technical, complex, or lengthy for the board to comprehend and appreciate. A detailed analysis of security program KPIs is more suitable for operational or tactical level reporting, rather than strategic level reporting.
An information security risk register is a tool for recording and tracking the information security risks that affect the organization, and for documenting the risk assessment, treatment, and monitoring activities.
However, an information security risk register is not the most effective way to present quarterly reports to the board, because it may not provide a comprehensive and balanced view of the information security program, and it may not highlight the achievements and benefits of the program. An information security risk register is more suitable for risk management or audit

purposes, rather than performance reporting. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 47-48, 59-60, 63-64, 67-68.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1019.
An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

NEW QUESTION: 439
下列哪一項是網路事件回應遏制階段最適當的行動？
A. 確定事件的最終根本原因。
B. 從網路中刪除該事件的所有實例。
C. 緩解被利用的漏洞以防止將來發生事故。
D. 隔離受影響的系統以防止損害蔓延。
Answer: (SHOW ANSWER)
Isolating affected systems limits the damage and prevents the incident from impacting other parts of the organization.
"During containment, the primary objective is to isolate affected systems to prevent further damage."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Process*

Valid CISM-CN Dumps shared by EduDump.com for Helping Passing CISM-CN Exam! EduDump.com now offer the **newest CISM-CN exam dumps**, the EduDump.com CISM-CN exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CISM-CN dumps with Test Engine here: https://www.edudump.com/exams/ISACA/CISM-CN/premium/ (**1041** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)