ISACA.CISM-CN.v2026-02-27.q395

Exam Code:	CISM-CN
Exam Name:	Certified Information Security Manager (CISM中文版)
Certification Provider:	ISACA
Free Question Number:	395
Version:	v2026-02-27
# of views:	108
# of Questions views:	4331
https://www.freecram.net/torrent/ISACA.CISM-CN.v2026-02-27.q395.html	

NEW QUESTION: 1
下列何者最能顯示資訊安全治理和公司治理是一體化的？
A. 資訊安全團隊了解業務目標。
B. 定期向董事會通報資訊安全關鍵績效指標 (KPI)、
C. 資訊安全指導委員會由企業領導人組成。
D. 對所有資訊安全措施進行成本效益分析。
Answer: (SHOW ANSWER)
The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

NEW QUESTION: 2
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: 3
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: 4
一旦確認網路安全攻擊，應先執行下列哪一項操作？
A. 隔離受影響的系統。
B. 通知高階管理層。
C. 關閉系統電源。
D. 聯絡法律機關。
Answer: (SHOW ANSWER)
Isolating the affected system is the first step in the incident response process, as it helps to contain the attack, prevent further damage, and preserve the evidence for analysis. Isolating the system can be done by disconnecting it from the network, blocking the malicious traffic, or applying quarantine rules.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.22; Cybersecurity Incident Response Exercise Guidance3

NEW QUESTION: 5
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: 6
下列哪一項是實施漏洞評估流程的主要好處？
A. 威脅管理得到增強。
B. 合規狀態改善。
C. 安全指標得到增強。
D. 促進主動風險管理。
Answer: (SHOW ANSWER)

A vulnerability assessment process is a systematic and proactive approach to identify, analyze and prioritize the vulnerabilities in an information system. It helps to reduce the exposure of the system to potential threats and improve the security posture of the organization. By implementing a vulnerability assessment process, the organization can facilitate proactive risk management, which is the PRIMARY benefit of this process.
Proactive risk management is the process of identifying, assessing and mitigating risks before they become incidents or cause significant impact to the organization. Proactive risk management enables the organization to align its security strategy with its business objectives, optimize its security resources and investments, and enhance its resilience and compliance.
A: Threat management is enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Threat management is the process of identifying, analyzing and responding to the threats that may exploit the vulnerabilities in an information system. Threat management is enhanced by implementing a vulnerability assessment process, as it helps to reduce the attack surface and prioritize the most critical threats.
However, threat management is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a reactive rather than proactive approach to risk management.
B: Compliance status is improved. This is a secondary benefit of implementing a vulnerability assessment process. Compliance status is the degree to which an organization adheres to the applicable laws, regulations, standards and policies that govern its information security. Compliance status is improved by implementing a vulnerability assessment process, as it helps to demonstrate the organization's commitment to security best practices and meet the expectations of the stakeholders and regulators. However, compliance status is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a result rather than a driver of risk management.
C: Security metrics are enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Security metrics are the quantitative and qualitative measures that indicate the effectiveness and efficiency of the information security processes and controls. Security metrics are enhanced by implementing a vulnerability assessment process, as it helps to provide objective and reliable data for security monitoring and reporting. However, security metrics are not the PRIMARY benefit of implementing a vulnerability assessment process, as they are a means rather than an end of risk management.
References =
* CISM Review Manual 15th Edition, pages 1-301
* CISM Exam Content Outline2
* Risk Assessment for Technical Vulnerabilities3
* A Step-By-Step Guide to Vulnerability Assessment4

NEW QUESTION: 7
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: 8
下列何者最能幫助組織持續保證滿足法律和法規合規性要求？
A. 將合規性要求嵌入營運流程中
B. 聘請外部專家就合規性要求的變化提供指導
C. 定期審核以確保遵守法律和法規要求
D. 分配營運經理滿足合規性要求的責任
Answer: (SHOW ANSWER)
Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.
Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2. Compliance requirements may vary depending on the industry, location, and nature of the organization2. Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

NEW QUESTION: 9
高階管理層表示擔心組織的入侵防禦系統 (IPS) 可能會反覆擾亂業務運營 下列哪一項最能表明資訊安全經理已調整系統以解決此問題？

A. 漏報率增加
B. 減少漏報
C. 減少誤報
D. 誤報增加
Answer: (SHOW ANSWER)
Decreasing false positives is the best indicator that the information security manager has tuned the system to address senior management's concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations. False positives are alerts generated by the IPS when it mistakenly blocks legitimate traffic or activity, causing disruption or downtime. Decreasing false positives means that the IPS has been configured to reduce such errors and minimize unnecessary interruptions. Increasing false negatives is not a good indicator because it means that the IPS has failed to detect or block malicious traffic or activity, increasing the risk of compromise or damage. Decreasing false negatives is not a good indicator because it does not affect business operations, but rather improves security detection or prevention. Increasing false positives is not a good indicator because it means that the IPS has increased its errors and interruptions, worsening senior management's concern. 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: 10
專案團隊成員向資訊安全經理通報尚未包含在風險登記冊中的潛在安全風險。資訊安全經理應該先執行下列哪一項操作？

A. 分析已識別的風險。
B. 實施補償控制。
C. 將風險加入風險登記冊。
D. 制定風險緩解計畫。
Answer: (SHOW ANSWER)

NEW QUESTION: 11
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: (SHOW ANSWER)
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: 12
資訊安全狀態報告管理包含下列何者最重要？
A. 最近的安全事件列表
B. 關鍵風險指示 (KRI)
C. 資訊安全政策審核
D. 資訊安全預算請求
Answer: (SHOW ANSWER)
Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References:
https://www.isaca.org/resources/isaca- journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004

NEW QUESTION: 13
下列哪一項是對面向公眾的 Web 伺服器的分散式阻斷服務 (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. 竄改網站口容
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: 14
某組織計劃利用軟體即服務 (SaaS)，並且正在選擇供應商 資安經理應該先做些什麼來支持這項措施？
A. 口看每個供應商的獨立安全評估報告。
B. 根據行業最佳實踐對每個供應商的服務進行基準測試。
C. 分析風險並提出緩解控制措施。
D. 定義資訊安全要求和流程。
Answer: (SHOW ANSWER)
Defining information security requirements and processes is the FIRST thing that the information security manager should do to support the initiative of utilizing Software as a Service (SaaS) and selecting a vendor.
This is because information security requirements and processes provide the basis for evaluating and comparing the SaaS vendors and solutions, as well as for ensuring the alignment of the SaaS services with the organization's security objectives, policies, and standards. Information security requirements and processes should include aspects such as data protection, access control, encryption, authentication, authorization, audit, compliance, incident response, disaster recovery, and service level agreements12. Reviewing independent security assessment reports for each vendor (A) is a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Independent security assessment reports can provide valuable information about the security posture, practices, and performance of the SaaS vendors and solutions, such as their compliance with industry standards, frameworks, and regulations, their vulnerability and risk management, and their security testing and auditing results. However, reviewing independent security assessment reports should be done after defining the information security requirements and processes, which can help to determine the scope, criteria, and expectations for the security assessment12. Benchmarking each vendor's services with industry best practices (B) is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Benchmarking each vendor's services with

industry best practices can help to measure and compare the quality, performance, and value of the SaaS vendors and solutions, as well as to identify the gaps, strengths, and weaknesses of the SaaS services. However, benchmarking each vendor's services with industry best practices should be done after defining the information security requirements and processes, which can help to select the relevant and appropriate industry best practices for the SaaS services12. Analyzing the risks and proposing mitigating controls is also a useful thing to do to support the initiative of utilizing SaaS and selecting a vendor, but it is not the FIRST thing to do. Analyzing the risks and proposing mitigating controls can help to identify and evaluate the potential threats, vulnerabilities, and impacts that may affect the security, availability, and reliability of the SaaS vendors and solutions, as well as to recommend and implement the necessary measures to reduce or eliminate the risks. However, analyzing the risks and proposing mitigating controls should be done after defining the information security requirements and processes, which can help to establish the risk appetite, tolerance, and criteria for the SaaS services12. References = 1: CISM Review Manual 15th Edition, page 82-831; 2: How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria - Gartner2

NEW QUESTION: 15
下列何者最有利於及時有效地回應事件？
A. 將事件的嚴重程度進行分類
B. 呼叫事件回應計畫時通知利害關係人
C. 評估受損資口的風險
D. 將滲透測試結果納入事件回應計劃
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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: (SHOW ANSWER)
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: 17
某企業決定從第三方供應商購買安全服務來支援其資訊安全計畫。供應商選擇標準包含下列哪一項最重要？
A. 供應商以前客口的回饋
B. 使供應商的業務目標與企業安全目標一致
C. 供應商口部控制環境的成熟度
D. 針對供應商網路的滲透測試
Answer: (SHOW ANSWER)
The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor's business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise's information security program. The alignment of the vendor's business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.
The vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It's a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

NEW QUESTION: 18
一家國口組織的高階主管宣布了將業務擴展到多個國際地點的計畫。資訊安全經理在獲悉這些計畫後，應該採取下列哪一項措施？
A. 根據國際資訊安全標準進行差距分析

B. 相應地更新安全訓練和意識資源
C. 研究影響新地點的法律和監管要求
D. 為每個新地點準備在地化的資訊安全政策
Answer: (SHOW ANSWER)
The first step is to research legal and regulatory requirements for the new locations. Different countries have varying security and privacy laws, and understanding these is critical before adapting policies or procedures.
"Security requirements will vary depending on local legal and regulatory obligations, which must be understood as part of international expansion."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Requirements The ISACA CISM practice database also highlights this step as the initial and critical move in international expansions.

NEW QUESTION: 19
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: 20

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值得關注的？

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: 21

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. 無法跨口品域互通。

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: 22
某組織最近修訂了資訊安全政策，以支持其新的資訊安全戰略。下列哪一項應該是資訊安全經理的下一步？
A. 檢討技術控制。
B. 刷新安全訓練計畫。
C. 更新標準和程序。
D. 評估與商業策略的一致性。
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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: 24
一位資訊安全經理了解到，業務部門領導者正在鼓勵更多地使用社群媒體平台來接觸客口。應先執行下列哪項操作，以協助降低員工在社群媒體上揭露機密資訊的風險？
A. 建立組織範圍口的社群媒體政策。
B. 制定濫用社群媒體網站的製裁措施。
C. 監控員工造訪的社群媒體網站。
D. 限制公司設備上的社群媒體存取。
Answer: A (LEAVE A REPLY)
An organization-wide social media policy is a document that defines the rules and guidelines for using social media platforms within the organization. It covers topics such as who can use social media, what they can post, how they should protect confidential information, and what are the consequences for violating the policy. An organization-wide social media policy helps to mitigate the risk of confidential information being disclosed by employees on social media by providing a clear and consistent framework for managing social media activities12.

References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION: 25
一位資訊安全經理收到通知，兩名高階主管有權提升公司會計系統中的權限，違反了公司政策解決這個問題的第一步是什麼？
A. 立即暫停高階主管的存取權限。
B. 執行系統存取審口。
C. 對過去 90 天口的所有系統交易進行全面審口。
D. 通知 CISO 安全政策違規行為。
Answer: (SHOW ANSWER)

NEW QUESTION: 26
在資訊安全事件後審口期間，應優先考慮下列何者？
A. 足口詳細地記錄所採取的操作
B. 更新關鍵風險指標 (KRI)
C. 評估事件回應團隊成員的表現
D. 評估事件回應有效性
Answer: (SHOW ANSWER)
An information security post-incident review is a process that aims to identify the root causes, impacts, lessons learned, and improvement actions of a security incident. The highest priority during a post-incident review should be evaluating the effectiveness of the incident response, which means assessing how well the incident response plan, procedures, roles, resources, and communication were executed and aligned with the business objectives and requirements. Evaluating the incident response effectiveness can help to identify the gaps, weaknesses, strengths, and opportunities for improvement in the incident response process and capabilities. Documenting actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are also important activities during a post-incident review, but they are not as critical as evaluating the incident response effectiveness, which can provide a holistic and strategic view of the incident response maturity and value.
References =
* ISACA, CISM Review Manual, 16th Edition, 2020, page 2411
* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2192 During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of

incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

NEW QUESTION: 27
下列哪一個是滲透測試中最重要的問題？
A. 讓一個獨立的小組執行測試
B. 取得審核許可
C. 在沒有任何口部知識的情況下執行測試
D. 有明確的目標以及成功與失敗標準
Answer: (SHOW ANSWER)
The most important issue in a penetration test is having a defined goal as well as success and failure criteria.
A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach, as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

NEW QUESTION: 28
在決定是否需要將事件升級為高階人員時，下列哪一項對於資訊安全經理最有用？
A. 事件管理程序
B. 事件管理策略
C. 系統風險評估
D. 組織風險登記冊
Answer: (SHOW ANSWER)
The organizational risk register is the most useful for an information security manager when determining the need to escalate an incident to senior management because it contains a list of

identified risks to the organization, their likelihood and impact, and their predefined risk thresholds or targets, which can help the information security manager assess the severity and urgency of the incident and decide whether it requires senior management's attention or action. Incident management procedures are not very useful for this purpose because they do not provide any specific criteria or guidance on when to escalate an incident to senior management. Incident management policy is not very useful for this purpose because it does not provide any specific criteria or guidance on when to escalate an incident to senior management. System risk assessment is not very useful for this purpose because it does not reflect the current risk exposure or status of the organization as a whole. 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-5/incident-response-lessons-learned

NEW QUESTION: 29
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: 30
下列哪一項是支持組織資訊安全願景和策略的最佳資訊來源？
A. 指標儀表板
B. 企業資訊安全架構

C. 能力成熟度模型
D. 治理政策
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
當資訊安全計劃與以下方面緊密結合時，它最能取得成功：
A. 資訊安全最佳實務。
B. 公認的口業架構。
C. 資訊安全策略。
D. 資訊安全策略。
Answer: (SHOW ANSWER)
An information security program is best positioned for success when it is closely aligned with the information security strategy, which defines the organization's vision, mission, goals, objectives, and risk appetite for information security. The information security strategy provides the direction and guidance for developing and implementing the information security program, ensuring that it supports the organization's business processes and objectives. The information security strategy also helps to establish the scope, boundaries, roles, responsibilities, and resources for the information security program.
References = CISM Manual, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Information Security Strategy1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 32
下列哪一項指標最能證明組織安全意識計畫的有效性？
A. 向服務台報告的安全事件數量
B. 定期參加安全訓練的員工百分比
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: 33

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: A (LEAVE A REPLY)

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: 34

下列哪一項是確定資訊安全計畫與業務策略一致性最有效的方法？

A. 評估業務連續性測試的結果。

B. 口看關鍵績效指標 (KPI)。

C. 評估事件對業務的影響。

D. 吸引業務流程擁有者。

Answer: (SHOW ANSWER)

The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.

Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

NEW QUESTION: 35

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. 資訊技術
C. 資訊安全
D. 人力資源 (HR)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
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: 37
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: 38
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: 39
下列哪一項是在資源有限的組織中競爭資訊安全計畫資金的最佳方式？
A. 展示業務連續性計劃 (BCP) 的有效性。
B. 報告關鍵績效指標 (KPI) 趨勢。
C. 證明程式支援業務活動。
D. 提供同儕組織安全事件增加的證據。

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

The goal of securing funding for an information security program often requires aligning the program with business goals and demonstrating its value to the organization. Here's an analysis of each option:

* A. Demonstrate the effectiveness of business continuity plans (BCPs): While important, this focuses on continuity rather than the overall value of the information security program to business objectives. This is not the strongest method to justify funding.
* B. Report key performance indicator (KPI) trends: KPI trends are useful for tracking performance but may not directly demonstrate how the program supports business activities or adds value.
* C. Demonstrate that the program enables business activities: This is the BEST option because it ties the information security program directly to business operations. When security is seen as an enabler (e.g., reducing risks in critical areas like customer data protection), stakeholders are more likely to allocate resources.
* D. Provide evidence of increased security events at peer organizations: This may indicate a general threat landscape but does not provide concrete evidence of the program's value or relevance to the organization's specific goals.

Reference: CISM Job Practice Area 1 (Information Security Governance) emphasizes aligning information security strategies with organizational objectives to gain stakeholder support.

NEW QUESTION: 40

當服務中斷時，下列哪一項最能讓組織在容量減少的情況下順利運作？

A. 危機管理計劃

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)

A business continuity plan (BCP) is the best option that enables an organization to operate smoothly with reduced capacities when service has been disrupted, as it defines the processes and procedures to maintain or resume critical business functions and minimize the impact of the disruption on the organization's objectives, customers, and stakeholders. A BCP also includes strategies for resource management, communication, recovery, and testing.

References = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans4

NEW QUESTION: 41

下列哪一項是資訊安全計畫成功的最關鍵因素？

A. 資訊安全綜合風險評估計劃

B. 資訊安全經理的業務知識

C. 經過適當訓練和充足資源的保全人員
D. 持續審計與解決未清項目
Answer: (SHOW ANSWER)
The explanation given in the manual is:
The information security manager's knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager's knowledge of the business.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.
An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

NEW QUESTION: 42
使用定量風險分析的一個關鍵考慮因素是：
A. 符合資訊資□風險分析的最佳實務。
B. 為資訊資□的暴露分配數□。
C. 將常用標籤應用於資訊資□。
D. 基於資訊資□的關鍵性分析。
Answer: (SHOW ANSWER)
A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent way, and to support the decision-making process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

NEW QUESTION: 43
下列何者最有助於在組織□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: 44
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: C (LEAVE A REPLY)
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: 45
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: 46
已檢測到並遏制了入侵。下列哪一個步驟代表了確保恢復系統完整性的最佳實務？
A. 從原始來源安裝作業系統、修補程式和應用程式。
B. 從備份中還原作業系統、修補程式和應用程式。
C. 從取證副本還原應用程式和資料。
D. 從作業系統和應用程式中刪除所有入侵跡象。
Answer: (SHOW ANSWER)
After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.
References =
* ISACA, CISM Review Manual, 16th Edition, 2020, page 2401
* ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132 The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

NEW QUESTION: 47
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口員工。
C. 制定可接受的使用政策。
D. 口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: 48
下列何者最有助於確保 IT 服務提供者遵守組織的資訊安全要求？
A. 要求對 IT 服務提供者進行外部安全審核
B. 請 IT 服務提供者定期報告
C. 與口部 IT 一起定義資訊安全要求
D. 與 IT 服務提供者定義業務復原計劃
Answer: (SHOW ANSWER)
Requiring regular reporting from the IT service provider is the best way to ensure compliance with the organization's information security requirements, as it allows the organization to monitor the performance, security incidents, service levels, and compliance status of the IT service provider. Reporting also helps to identify any gaps or issues that need to be addressed or resolved. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 49
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: 50
在製定處理業務部門資訊系統上的信用卡資料的安全流程時，資訊安全經理應首先：
A. 確保與行業加密標準保持一致。
B. 檢視處理安全支付的口業最佳實務。
C. 審口有關信用卡資訊的公司政策。
D. 確保處理信用卡資料的系統是分段的。
Answer: (SHOW ANSWER)

NEW QUESTION: 51
資訊安全經理發現，即將部署的線上應用程式將風險增加到超出可接受的水平，並且尚未包括必要的控制措施。下列哪一項是資訊安全經理的最佳行動方案？
A. 指示 IT 依照緊急業務需求部署控制措施。
B. 提供高階管理層額外控制的商業案例。
C. 針對補償性控制口品招標。
D. 推薦不同的應用程式。

Answer: (SHOW ANSWER)
The information security manager should present a business case for additional controls to senior management, as this is the most effective way to communicate the risk and the need for mitigation. The information security manager should not instruct IT to deploy controls based on urgent business needs, as this may not align with the business objectives and may cause unnecessary costs and delays. The information security manager should not solicit bids for compensating control products, as this may not address the root cause of the risk and may not be the best solution. The information security manager should not recommend a different application, as this may not be feasible or desirable for the business. References = CISM Review Manual 2023, page 711; CISM Review Questions, Answers & Explanations Manual 2023, page 252

NEW QUESTION: 52
下列哪一項是提升組織偵測和應對事件的能力的最佳方法？
A. 執行安全漏洞分析。
B. 進行業務影響分析 (BIA)。
C. 進行定期意識訓練。
D. 執行網路滲透測試。
Answer: (SHOW ANSWER)

NEW QUESTION: 53
某個組織正在考慮使用第三方來託管敏感的存檔資料。在建立關係之前，下列哪一項是最需要驗證的？
A. 供應商的資料中心位於同一地理區域。
B. 不向供應商提供加密金鑰。
C. 供應商的控制符合組織的安全標準。
D. 定期對供應商的營運進行獨立審核。
Answer: (SHOW ANSWER)
The most important thing to verify before entering into a relationship with a third party to host sensitive archived data is the vendor's controls are in line with the organization's security standards. This is because the organization is ultimately responsible for the security and privacy of its data, even if it is stored or processed by a third party. The organization should ensure that the vendor has adequate and effective controls to protect the data from unauthorized access, modification, disclosure, or destruction. The organization should also ensure that the vendor complies with the applicable laws and regulations regarding data protection, such as the General Data Protection Regulation (GDPR) in the European Union. The organization should conduct a thorough risk assessment of the vendor and its services, and establish a clear contract that defines the roles, responsibilities, expectations, and obligations of both parties.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 2, page 2

NEW QUESTION: 54
在選擇指標來監控資訊安全計畫的有效性時，對於資訊安全經理來口最重要的是：
A. 考慮組織的商業策略。
B. 識別程式的風險和補償控制。
C. 考慮該計劃的策略目標。
D. 利用口業基準。
Answer: (SHOW ANSWER)

NEW QUESTION: 55
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: (SHOW ANSWER)
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: 56
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: 57
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. 檢口網路配置
B. 驗證有效載荷簽名
C. 制定事件回應策略
D. 驗證事件
Answer: (SHOW ANSWER)

NEW QUESTION: 58
滲透測試由經認可的第三方進行。下列哪一項應該是資訊安全經理的首要行動方案？
A. 確保發現的漏洞在可接受的時間口得到解決
B. 確保進行風險評估以評估結果
C. 向高階管理層報告調口結果
D. 請求解決主要漏洞所需的資金
Answer: (SHOW ANSWER)

NEW QUESTION: 59
下列哪一項是獲得組織範圍口資訊安全計畫支援的最佳方式？
A. 強制進行定期安全意識訓練。
B. 制定安全性能指標。
C. 將安全性定位為業務推動者。
D. 根據 IT 策略決定安全計畫的優先順序。
Answer: (SHOW ANSWER)
Positioning security as a business enabler is the BEST way to obtain organization-wide support for an information security program, because it helps to demonstrate the value and benefits of security to the organization's strategic objectives, performance, and reputation. By aligning security with the business goals and needs, the information security manager can gain the buy-in and commitment of senior management and other stakeholders, and foster a positive security culture across the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "The information security manager should position information security as a business enabler that supports the achievement of the enterprise's business objectives and adds value to the enterprise." CISM Review Manual, 16th Edition, ISACA, 2020, p. 39: "The information security manager should communicate the value and benefits of information security to senior management and other stakeholders to obtain their support and commitment for the information security program." CISM Review Manual, 16th Edition, ISACA, 2020, p. 40: "The information security manager should promote a positive

security culture within the enterprise by influencing the behavior and attitude of employees and other parties toward information security."

NEW QUESTION: 60

對於資安經理來說，整合組織的各種保障功能非常重要，主要是為了：

A. 一致的安全性。

B. 全面審核

C. 安全意識文化

D. 遵守政策

Answer: (SHOW ANSWER)

Consistent security is the primary reason for integrating the various assurance functions of an organization for the information security manager because it ensures that the security policies and standards are applied uniformly and effectively across different domains, processes, and systems of the organization.

Comprehensive audits are not the primary reason for integrating the various assurance functions, but rather a possible outcome or benefit of doing so. A security-aware culture is not the primary reason for integrating the various assurance functions, but rather a desirable state or goal of the organization. Compliance with policy is not the primary reason for integrating the various assurance functions, but rather a basic requirement or expectation of the organization.

References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system

NEW QUESTION: 61

雲端服務供應商 A 公司正在收購 B 公司，以便將B 公司的技術融入其雲端服務中，從而獲得新的利益。

下列哪一項應該是 A 公司資安經理關注的主要重點？

A. B公司的組織架構

B. 遵守 A 公司安全政策的成本

C. 公司 A 的安全架構

D. B 公司的安全政策

Answer: (SHOW ANSWER)

According to the CISM Review Manual, the security architecture of an organization defines the security principles, standards, guidelines and procedures that support the information security strategy and align with the business objectives. When acquiring another company, the information security manager of the acquiring company should focus on ensuring that the security architecture of the acquired company is compatible with its own, or that any gaps or conflicts are identified and resolved.

References = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.2, page 751.

NEW QUESTION: 62
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. 恢復受影響的系統以進行正常運作。
D. 隔離受影響的系統以防止進一步損壞
Answer: (SHOW ANSWER)

NEW QUESTION: 63
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: 64
下列哪一項應該是資訊安全策略的主要基礎？
A. 組織的願景與使命
B. 全面差距分析的結果
C. 資訊安全策略
D. 稽核與監理要求
Answer: (SHOW ANSWER)

The organization's vision and mission should be the PRIMARY basis for an information security strategy, as they define the purpose and direction of the organization and its information security needs. A comprehensive gap analysis is a tool to identify the current state and desired state of information security, and the actions needed to close the gap. Information security policies are the high-level statements of management's intent and expectations for information security, and are derived from the information security strategy. Audit and regulatory requirements are external factors that influence the information security strategy, but are not the primary basis for it. References = CISM Review Manual, 16th Edition, pages 17-181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 782 The primary basis for an information security strategy should be the organization's vision and mission. The organization's vision and mission should be the foundation for the security strategy, and should inform and guide the security policies, procedures, and practices that are implemented. The results of a comprehensive gap analysis, information security policies, and audit and regulatory requirements should all be taken into consideration when developing the security strategy, but should not be the primary basis.

NEW QUESTION: 65
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: (SHOW ANSWER)
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: 66
下列哪項活動必須由資訊安全經理針對變更要求執行？
A. 掃描 IT 系統以尋找作業系統漏洞。
B. 對受影響的系統執行滲透測試。
C. 口看資訊安全業務要求的變更。
D. 評估對資訊安全風險的影響。
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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: (SHOW ANSWER)
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

NEW QUESTION: 68
在確定□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？
A. 確定復原點目標 (RPO)
B. 服務中斷的影響
C. 恢復測試結果
D. 高階管理層的指示
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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: 70

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. 企業範圍內的安全事件的平均解決時間 (MTTR)

D. 為高風險資訊資產識別的漏洞數量

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: 71

影響管理階層對資訊安全支援的最重要資訊是：

A. 與業務策略保持一致的證明。

B. 總體威脅態勢的辨識。

C. 成功攻擊競爭對手的報告。

D. 組織風險的辨識。

Answer: (SHOW ANSWER)
The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. 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: 72
下列哪一項對於確保資訊安全計畫與組織策略一致最為重要？
A. 識別特定於業務的風險因素
B. 採用業界認可的框架
C. 與業界同業進行基準比較
D. 高階管理層批准
Answer: (SHOW ANSWER)

NEW QUESTION: 73
在通報安全事件後，下一步應該採取下列哪一項措施？
A. 遏制
B. 恢復
C. 調口
D. 升級
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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: 75
為了提高新軟體應用程式的開發效率，應定義安全需求：
A. 基於程式碼審口。
B. 基於可用的安全評估工具。
C. 功能需求之後。
D. 與其他要求同時進行。
Answer: (SHOW ANSWER)
Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the organization, not on code review, security assessment tools, or functional requirements. References = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

NEW QUESTION: 76
下列哪一項對於確保有效執行事件管理計畫最重要？
A. 事件回應團隊接受過適當的訓練。
B. 已聘請信譽良好的託管安全服務提供者。
C. 已獲得管理層支持和批准。
D. 已進行事件回應成熟度評估。
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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: C (LEAVE A REPLY)

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: 78

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: 79
下列哪一項最有助於確保軟體口建適當的安全控制？
A. 將安全性整合到整個開發過程中
B. 部署前執行安全性測試
C. 提供開發活動期間的實施標準
D. 為軟體開發團隊提供安全培訓
Answer: (SHOW ANSWER)
The best way to ensure appropriate security controls are built into software is to integrate security throughout the development process. This means that security should be considered from the initial stages of planning, design, coding, testing, deployment, and maintenance of the software. Integrating security throughout the development process helps to identify and mitigate security risks early, reduce the cost and complexity of fixing vulnerabilities later, improve the quality and reliability of the software, and enhance the trust and confidence of the users and customers. Integrating security throughout the development process also aligns with the best practices and standards of information security governance, such as the CISM framework123.
References =
* CISM Review Manual 15th Edition, page 1631
* CISM domain 3: Information security program development and management [2022 update]2
* CISSP domain 8 overview: Software development security4

NEW QUESTION: 80
資安經理的任務是開發材料，向董事會、監管機構和媒體通報安全事件的最新情況。資訊安全經理應該先執行下列哪一項操作？

A. 為目標受眾建立溝通管道。
B. 確定每個受眾的需求和要求。
C. 創造全面的單一溝通
D. 呼叫組織的事件回應計畫。
Answer: (SHOW ANSWER)

The information security manager should do FIRST invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a comprehensive singular communication are all important steps for communicating effectively with the board, regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the relevant information to the target audience according to the plan. References = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012
Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

NEW QUESTION: 81
在執行業務影響分析 (BIA) 時，誰應該計算恢復時間和成本估算？
A. 業務流程擁有者
B. 業務連續性協調員
C. 高階管理層
D. 資訊安全經理
Answer: A (LEAVE A REPLY)
The business process owner 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 business process owner has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the business process owner is the best person to calculate the recovery time and cost estimates when performing a business impact analysis (BIA), which is a process of identifying and quantifying the potential losses, damages, or consequences that could result from 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 recovery time and

cost estimates are the measures that indicate the time and money that are needed to resume and restore the normal business operations and functions after the disruption or incident. The recovery time and cost estimates can help to prioritize and protect the critical activities and resources, to allocate the appropriate budget and resources, to implement the necessary controls and measures, and to evaluate the effectiveness and efficiency of the business continuity and disaster recovery plans.
The business continuity coordinator, the senior management, and the information security manager are all important roles in the BIA process, but they are not the best ones to calculate the recovery time and cost estimates. The business continuity coordinator is the person who is responsible for coordinating and facilitating the BIA process, as well as the development, implementation, and maintenance of the business continuity and disaster recovery plans. The business continuity coordinator can help to define and communicate the scope, objectives, and methodology of the BIA, to collect and analyze the data and information from the business process owners and other stakeholders, to report and present the BIA results and recommendations, and to provide feedback and suggestions for improvement and optimization of the BIA and the plans. The senior management is the group of people who have the ultimate authority and accountability for the organization's strategy, direction, and performance. The senior management can help to approve and support the BIA process and the plans, to provide the strategic guidance and vision for the business continuity and disaster recovery, to allocate the necessary budget and resources, to oversee and monitor the BIA and the plans, and to make the final decisions and approvals. The information security manager is the person who is responsible for ensuring the security of the information assets and systems that support the business processes and functions. The information security manager can help to identify and assess the information security risks and issues that could affect the BIA and the plans, to implement and manage the security controls and measures that are needed to protect and recover the information assets and systems, to coordinate and collaborate with the business process owners and other stakeholders on the security aspects of the BIA and the plans, and to provide the security expertise and advice. References = CISM Review Manual 15th Edition, pages 228-2291; CISM Practice Quiz, question 1722

NEW QUESTION: 82
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: A (LEAVE A REPLY)
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: 83
更新管理安全設備的程序時，下列哪一項是最重要的考量？
A. 依照組織的安全框架進行更新
B. 通知管理階層程序變更
C. 根據風險技術和流程的變更進行更新
D. 管理階層對程序的審口與批准
Answer: (SHOW ANSWER)
According to the CISM Manual, updating procedures for managing security devices should be based on changes in risk technology and process, not on the organization's security framework, notification to management of the procedural changes, or review and approval of procedures by management1. These are not the most important considerations when updating procedures for managing security devices, as they do not reflect the actual impact of the changes on the security posture of the organization.
The CISM Manual states that "procedures for managing security devices should be updated whenever there are significant changes in the risk technology or process that affect the security devices" (IR 8287A)1. For example, if a new security device is introduced or an existing one is replaced, its procedures should be updated accordingly. Similarly, if a new risk technology or process is implemented that affects how security devices are configured, monitored, or maintained, its procedures should be updated as well1.
The CISM Manual also provides guidance on how to update procedures for managing security devices in a systematic and consistent manner. It recommends using a change management process that involves identifying, analyzing, approving, implementing, and evaluating changes to security device procedures1. It also suggests using a change control board (CCB) that consists of representatives from different stakeholders who review and approve changes to security device procedures before they are implemented1.
References: 1: IR 8287A - Managing Security Devices | CSRC NIST

NEW QUESTION: 84
一個小型組織與跨國雲端運算供應商簽訂了合約。如果合約中省略下列哪一項，資安經理最關心的是什麼？

A. 訂口對供應商進行現場審核的權利
B. 具有程式碼發佈條件的軟體程式碼託管
C. 訂口者批准存取其資料的權限
D. 同一實體伺服器上訂口者資料的混合
Answer: C (LEAVE A REPLY)
The greatest concern to an information security manager if omitted from the contract with a multinational cloud computing vendor would be the authority of the subscriber to approve access to its data. This is because the subscriber's data may be subject to different legal and regulatory requirements in different jurisdictions, and the subscriber may lose control over who can access, process, or disclose its data. The subscriber should have the right to approve or deny access to its data by the vendor or any third parties, and to ensure that the vendor complies with the applicable data protection laws and standards. The authority of the subscriber to approve access to its data is also one of the key elements of the ISACA Cloud Computing Management Audit /Assurance Program1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 142.

NEW QUESTION: 85
下列何者最能體現資訊安全計畫的附加價口？
A. 安全基線
B. 差距分析
C. SWOT 分析
D. 平衡計分卡
Answer: (SHOW ANSWER)
A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

NEW QUESTION: 86
下列哪一項對安全營運中心的潛在安全漏洞威脅範圍提出了最大的挑戰？
A. IT 系統時鐘與集中式日誌伺服器不同步。
B. 供應商不再支援作業系統。
C. 補丁管理系統未及時部署修補程式。
D. 組織擁有使用雲端服務的分散式資料中心。
Answer: (SHOW ANSWER)
A security operations center (SOC) relies on the centralized logging server to collect, store, analyze and correlate security events from various sources such as firewalls, intrusion detection

systems, antivirus software, etc. The centralized logging server uses the timestamps of the events to perform the analysis and correlation. If the IT system clocks are not synchronized with the centralized logging server, the SOC will face difficulties in identifying the sequence and causality of the events, which will affect its ability to detect and respond to potential security breaches. Therefore, this presents the greatest challenge to the SOC's awareness of potential security breaches.
Operating systems that are no longer supported by the vendor may pose a security risk, but they can be mitigated by applying compensating controls such as isolation, segmentation, monitoring, etc. The patch management system that does not deploy patches in a timely manner may also increase the vulnerability exposure, but it can be remediated by prioritizing and applying the critical patches as soon as possible. An organization that has a decentralized data center that uses cloud services may face some challenges in ensuring the security and compliance of the cloud environment, but it can leverage the cloud service provider' s security capabilities and tools to enhance the SOC's visibility and control. Therefore, these options are not the greatest challenges to the SOC's awareness of potential security breaches. References = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page
2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; RSI Security, Common Challenges of SOC Teams3; Infosec Matter, Security Operations Center: Challenges of SOC Teams4

NEW QUESTION: 87
在應對重大安全事件時，下列何者最重要？
A. 聯絡法醫調口員
B. 遵循升級流程
C. 通知執法部門
D. 辨識妥協指標
Answer: (SHOW ANSWER)
Following the escalation process ensures that the incident is managed in accordance with established protocols, involving the right stakeholders and prioritizing the incident appropriately. "Following the escalation process is critical to ensure that incidents are handled appropriately and that the right personnel are engaged at the right time."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Escalation Procedures* ISACA practice questions highlight that proper escalation is vital to ensure incidents are managed effectively and consistently.

NEW QUESTION: 88
確定下列哪一項最能遏止網路攻擊？
A. 攻擊的目標段
B. 發動攻擊的電腦的IP位址
C. 發動攻擊的威脅參與者

D. 攻擊所利用的漏洞
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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□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: 90
下列哪一項主要由資產分類決定？
A. 資□所需的保險範圍
B. 資□所需的保護等級
C. 資□替換的優先級
D. 資□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: 91
當適當降低風險的預防性控制不可行時，下列何者是資安經理最重要的行動？
A. 管理影響
B. 識別不可接受的風險等級
C. 評估漏洞
D. 評估潛在威脅
Answer: (SHOW ANSWER)
When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. References:
* https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/
* https://www.osha.gov/safety-management/hazard-prevention
* https://www.cdc.gov/niosh/topics/hierarchy/default.html

NEW QUESTION: 92

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

NEW QUESTION: 93
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: B (LEAVE A REPLY)
= 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: 94
安全事件升級程序中包含下列哪一項最重要？
A. 安全計畫的主要目標
B. 復原過程
C. 通知條件
D. 收容措施
Answer: (SHOW ANSWER)
The most important thing to include in security incident escalation procedures is notification criteria. This is because notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. Notification criteria help to ensure that the appropriate stakeholders are aware of the incident and can take the necessary actions to respond, mitigate, and recover from it. Notification criteria also help to comply with legal and regulatory requirements for reporting incidents to external parties, such as customers, authorities, or media.
Notification criteria define who needs to be informed of an incident, when, and how, depending on the severity, impact, and nature of the incident. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.2, page 2121; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 1, page 1

NEW QUESTION: 95
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: 96
資訊安全團隊正在規劃對現有供應商進行安全評估。下列哪一種方法對於正確確定評估範圍最有幫助？
A. 將審□重點放在風險最高的基礎設施上
B. 審核供應商合約中所列的控制措施
C. 確定供應商是否遵循所選的安全框架規則
D. □看供應商的安全策略
Answer: (SHOW ANSWER)
Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization's data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor's security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices.
Therefore, reviewing controls listed in the vendor contract is the correct answer.
References:
https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/
https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf
https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

NEW QUESTION: 97
實施安全計畫時應先執行下列哪一項操作？
A. 執行風險分析
B. 實現資料加密。
C. 建立資訊資□清單。
D. 決定資訊資□的價□。

Answer: (SHOW ANSWER)
Performing a risk analysis is the first step when implementing a security program because it helps to identify and prioritize the potential threats and vulnerabilities that may affect the organization's assets, processes, or objectives, and determine their impact and likelihood. Implementing data encryption is not the first step, but rather a possible subsequent step that involves applying a specific security control or technique to protect data from unauthorized access or modification. Creating an information asset inventory is not the first step, but rather a possible subsequent step that involves identifying and classifying the organization's assets based on their value and sensitivity. Determining the value of information assets is not the first step, but rather a possible subsequent step that involves estimating and quantifying the worth of information assets to the organization. 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: 98
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.

NEW QUESTION: 99
事件管理團隊負責人發出通知，表明組織已成功從網路攻擊中恢復。接下來應該執行下列哪項操作？
A. 為高階管理層準備一份執行摘要
B. 收集有關業務影響的回饋
C. 召開會議總結經驗教訓。
D. 保護並保存數位證據以便分析。
Answer: (SHOW ANSWER)
Conducting a meeting to capture lessons learned is the next step after an incident management team leader sends out a notification that the organization has successfully recovered from a

cyberattack because it helps to identify the strengths and weaknesses of the current incident response plan, capture the feedback and recommendations from the incident responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Preparing an executive summary for senior management is not the next step, but rather a subsequent step that involves reporting the incident details, impact, and resolution to the senior management. Gathering feedback on business impact is not the next step, but rather a concurrent step that involves assessing the extent and severity of the damage or disruption caused by the incident.
Securing and preserving digital evidence for analysis is not the next step, but rather a previous step that involves collecting and documenting the relevant data or artifacts related to the incident.
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: 100
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: 101
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: 102
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: 103
下列哪項變更管理程序最有可能引起資安經理的注意？
A. 在進行更改之前的週末測試後備流程
B. 使用者不會收到有關計劃的系統變更的通知
C. 使用手動而不是自動程序來比較程式版本。
D. 開發經理將程式移轉到生口中
Answer: (SHOW ANSWER)
The change management procedure that is MOST likely to cause concern to the information security manager is the development manager migrating programs into production, because it involves a high-risk activity that could compromise the confidentiality, integrity, and availability of the information systems and data.
Migrating programs into production without proper testing, validation, and approval could introduce errors, vulnerabilities, or conflicts that could affect the performance, functionality, or security of the systems. Fallback processes are tested the weekend before changes are made, users are not notified of scheduled system changes, and a manual rather than an automated process is used to compare program versions are all acceptable change management procedures that do not pose significant risks to the information security manager. References = CISM Review Manual, 16th Edition, page 3121; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1522

NEW QUESTION: 104
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: 105
為了在災難期間保持運行，組織應呼叫下列哪一項計劃？
A. 災難復原計畫 (DRP)
B. 事件回應計劃
C. 業務連續性計劃 (BCP)
D. 業務應急計劃
Answer: (SHOW ANSWER)
= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources.
Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders

involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:
* Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
* Restore the essential functions and services as quickly and efficiently as possible.
* Protect the health, safety, and welfare of the staff, customers, and partners.
* Meet the legal, regulatory, contractual, and ethical obligations of the organization.
* Learn from the disaster and improve the business continuity capabilities and readiness of the organization.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

NEW QUESTION: 106
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: 107
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: 108
當授予公司口部網路遠端存取權限時，最重要的考慮因素應該是提供存取權限：
A. 視需要了解並受控制。
B. 透過使用遠端存取伺服器。
C. 是否有強大的 IT 基礎架構。
D. 遵守法律和監管要求。
Answer: (SHOW ANSWER)

NEW QUESTION: 109
下列哪一項對於提升事件回應人員的效率最重要？
A. 與管理團隊溝通

B. 將員工與 IT 部門整合
C. 測試反應場景
D. 每年檢討事件回應計劃
Answer: C (LEAVE A REPLY)
= Testing response scenarios is the most important factor in increasing the effectiveness of incident responders, as it allows them to practice their skills, identify gaps and weaknesses, evaluate the adequacy and feasibility of the incident response plan, and improve their coordination and communication. Testing response scenarios can also help to enhance the confidence and readiness of the incident responders, as well as to measure their performance and compliance with the policies and procedures. Testing response scenarios can be done through various methods, such as tabletop exercises, simulations, drills, or full-scale exercises, depending on the scope, objectives, and complexity of the scenarios.
The other options are not as important as testing response scenarios, although they may also contribute to the effectiveness of incident responders. Communicating with the management team is important to ensure that the incident responders have the necessary support, resources, and authority to carry out their tasks, as well as to report the status and outcomes of the incident response. However, communication alone is not sufficient to increase the effectiveness of incident responders, as they also need to have the relevant knowledge, skills, and experience to handle the incidents. Integrating staff with the IT department may help to facilitate the collaboration and information sharing between the incident responders and the IT staff, who may have the technical expertise and access to the systems and data involved in the incidents. However, integration alone is not enough to increase the effectiveness of incident responders, as they also need to have the appropriate roles, responsibilities, and processes to manage the incidents. Reviewing the incident response plan annually is important to ensure that the plan is updated and aligned with the current risks, threats, and business requirements, as well as to incorporate the lessons learned and best practices from previous incidents.
However, reviewing the plan alone is not enough to increase the effectiveness of incident responders, as they also need to test and validate the plan in realistic scenarios and conditions.
References =
* CISM Review Manual, 16th Edition, ISACA, 2022, pp. 223-225, 230-231.
* CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1004.

NEW QUESTION: 110
下列哪一項對於在組織內建立 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: 111
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: 112
維持資訊安全計畫管理支援的最有用的技術是：
A. 向管理階層通報業務營運的安全性。
B. 實施全面的安全意識和訓練計畫。
C. 辨識不遵守標準的風險和後果。
D. 對可比較組織的安全計畫進行基準測試。
Answer: (SHOW ANSWER)
= According to the CISM Review Manual, one of the key success factors for an information security program is to maintain management support and commitment. This can be achieved by providing regular reports to management on the security status of the organization, the effectiveness of the security controls, and the alignment of the security program with the business objectives and strategy. By informing management about the security of business operations, the information security manager can demonstrate the value and benefits of the security program, and ensure that management is aware of the security risks and issues that need to be addressed. This technique can also help to build trust and confidence between the information security manager and the senior management, and foster a culture of security within the organization1
The other options are not as effective as informing management about the security of business operations.
Implementing a comprehensive security awareness and training program is important, but it is mainly targeted at the end users and staff, not the senior management. Identifying the risks and consequences of failure to comply with standards can help to justify the need for security controls, but it can also create a negative impression of the security program as being too restrictive or punitive. Benchmarking the security programs of comparable organizations can provide some insights and best practices, but it may not reflect the specific needs and context of the organization, and it may not be relevant or applicable to the management's expectations and priorities1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 28-29...

NEW QUESTION: 113

下列哪一項最能顯示組織已在規定的復原時間目標 (RTO) 口有效測試了其業務連續性和災難復原計畫？

A. 滿足監理要求。

B. 滿足口部合規性要求。

C. 正在實現風險管理目標。

D. 業務需求正在滿足。

Answer: (SHOW ANSWER)

The primary purpose of business continuity and disaster recovery plans is to ensure that the organization can resume its critical business functions within the stated recovery time objectives (RTOs) after a disruptive event. RTOs are based on the business needs and the impact analysis of each function or process. Therefore, meeting the business needs is the best indicator that the plans are effective. Regulatory requirements, internal compliance requirements, and risk management objectives are important factors that influence the development and testing of the plans, but they are not the ultimate measure of their effectiveness. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3071; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Imperva, Business Continuity & Disaster Recovery Planning (BCP & DRP)3

NEW QUESTION: 114

當資訊安全治理架構與公司治理一致時，下列哪一項是主要實現的利益？

A. 保護商業價口與資口

B. 確定核心業務策略

C、更容易進入新業務和新技術

C. 改善監理合規狀況

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 and support business objectives, are consistent with applicable laws and regulations, and are effectively managed. By aligning information security governance with corporate governance, the organization can ensure that information security is integrated into the business processes and decision making, and that the information security risks and opportunities are properly identified, assessed, and addressed. References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.1

NEW QUESTION: 115

當大型跨國組織的資訊安全經理將資料處理外包給雲端服務供應商時，最關心的問題是什麼？

A. 供應商服務等級協定 (SLA)

B. 對供應商的獨立審口

C. 當地法律法規

D. 資料的備份與恢復

Answer: (SHOW ANSWER)

he greatest concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider is the local laws and regulations that may apply to the data and the cloud service provider. Local laws and regulations may vary significantly across different jurisdictions and may impose different requirements or restrictions on the data protection, privacy, security, sovereignty, retention, disclosure, transfer, or access. These laws and regulations may also create potential conflicts or inconsistencies with the organization's own policies, standards, or contractual obligations.

Therefore, an information security manager should conduct a thorough legal and regulatory analysis before outsourcing data processing to a cloud service provider and ensure that the cloud service provider complies with all the applicable laws and regulations in the relevant jurisdictions.

References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:

Outsourcing2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1 Outsourcing data processing to a cloud service provider may expose the organization to different legal and regulatory requirements depending on the location of the data and the vendor. This could affect the organization's compliance and liability in case of a breach or dispute. Therefore, the information security manager should be most concerned about the local laws and regulations that apply to the outsourcing arrangement.

NEW QUESTION: 116

在向主要利害關係人提交的關於資訊安全計畫有效性的報告中，下列哪一項是最重要的？

A. 安全指標

B. 安全基線

C. 安全事件詳細信息

D. 安全風險暴露

Answer: (SHOW ANSWER)

Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.

An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations.

The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and

business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

NEW QUESTION: 117
下列哪一項對於確定組織目前降低風險的能力最有幫助？
A. 能力成熟度模型
B. 漏洞評估
C. IT 安全風險與暴露
D. 商業影響分析 (BIA)
Answer: (SHOW ANSWER)
A capability maturity model (CMM) is a framework that helps organizations assess and improve their processes and capabilities in various domains, such as software development, project management, information security, and others1. A CMM defines a set of levels or stages that represent the degree of maturity or effectiveness of an organization's processes and capabilities in a specific domain. Each level has a set of criteria or characteristics that an organization must meet to achieve that level of maturity. A CMM also provides guidance and best practices on how to progress from one level to another, and how to measure and monitor the performance and improvement of the processes and capabilities2.
A CMM is most helpful in determining an organization's current capacity to mitigate risks, because it provides a systematic and objective way to evaluate the strengths and weaknesses of the organization's processes and capabilities related to risk management. A CMM can help an organization identify the gaps and opportunities for improvement in its risk management practices, and prioritize the actions and resources needed to address them. A CMM can also help an organization benchmark its risk management maturity against industry standards or best practices, and demonstrate its compliance with regulatory or contractual requirements3.
The other options are not as helpful as a CMM in determining an organization's current capacity to mitigate risks, because they are either more specific, limited, or dependent on a CMM. A vulnerability assessment is a process of identifying and analyzing the vulnerabilities in an organization's systems, networks, or applications, and their potential impact on the organization's assets, operations, or reputation. A vulnerability assessment can help an organization identify the sources and levels of risk, but it does not provide a comprehensive or holistic view of the organization's risk management maturity or effectiveness4. IT security risk and exposure is a measure of the likelihood and impact of a security breach or incident on an organization's IT assets, operations, or reputation. IT security risk and exposure can help an organization quantify and communicate the level of risk, but it does not provide a framework or guidance on how to improve the organization's risk management processes or capabilities5. A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of a disruption or disaster on an organization's critical business functions, processes, or resources. A BIA can help an organization determine the priorities and requirements for business continuity and disaster

recovery, but it does not provide a method or standard for assessing or enhancing the organization's risk management maturity or effectiveness. References = 1: CMMI Institute - What is CMMI? - Capability Maturity Model Integration 2: Capability Maturity Model and Risk Register Integration: The Right ... 3: Performing Risk Assessments of Emerging Technologies - ISACA 4: CISM Review Manual 15th Edition, Chapter 4, Section 4.2 5: CISM Review Manual 15th Edition, Chapter 4, Section 4.3 : CISM Review Manual 15th Edition, Chapter 4, Section 4.4

NEW QUESTION: 118
對於事件偵測能力不成熟的組織來口，下列哪一項應該是主要關注點？
A. 執行滲透測試
B. 提高使用者意識
C. 安裝新的防火牆
D. 更新安全性策略
Answer: B (LEAVE A REPLY)
User awareness is essential for improving detection capabilities in an immature environment. Employees are often the first line of defense and can identify suspicious activities early.
"User awareness and training can significantly improve the detection of incidents by enabling employees to recognize and report suspicious activities."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Detection and Analysis* ISACA practice questions confirm that improving user awareness is the foundational step before deploying new technologies.

NEW QUESTION: 119
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. 評估使用相同技術的同儕組織受到的影響
B. 為最終使用者提供培訓，讓他們熟悉新技術
C. 了解對現有資源的影響
D. 審口供應商合約和服務等級協定 (SLA)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
為了讓資訊安全經理評估目前控制措施的適當性，必須定義下列哪一項？
A. 安全性策略
B. 風險管理框架
C. 風險偏好
D. 安全標準
Answer: (SHOW ANSWER)
= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in

order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION: 121
某個組織已購買了一個具有嚴格維護口明和時間表的新系統。這些資訊應該記錄在哪裡？
A. 標準
B. 政策
C. 指南
D. 程式
Answer: (SHOW ANSWER)
Procedures are the detailed steps or instructions for performing specific tasks or activities. They are usually aligned with standards, policies and guidelines, but they are more specific and prescriptive. System maintenance instructions and schedules are examples of procedures that should be documented and followed to ensure the proper functioning and security of the system. References: The CISM Review Manual 2023 defines procedures as "the lowest level in the hierarchy of documentation. They are detailed steps that a user must follow to accomplish an activity" (p. 80). The CISM Item Development Guide also provides the following explanation for this answer: "Procedures are the correct answer because they provide the specific steps to be followed to maintain the system" (p. 11).

NEW QUESTION: 122
將資訊安全治理納入公司治理框架的最大好處是什麼？
A. 提高資訊安全策略意識
B. 提高遭受攻擊時的流程彈性
C. 向企業推廣安全設計原則
D. 資訊安全的管理責任
Answer: (SHOW ANSWER)

The greatest benefit of incorporating information security governance into the corporate governance framework is D. Management accountability for information security. This is because management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business goals, stakeholder expectations, and regulatory requirements. Management accountability for information security also means that the senior management and the board of directors are accountable for the performance, value, and effectiveness of the information security program, and for the management and mitigation of the information security risks and incidents. Management accountability for information security can help to foster a culture of security awareness and responsibility, and to enhance the trust and confidence of the customers, partners, and regulators in the organization's information security capabilities.
Management accountability for information security means that the senior management and the board of directors are responsible for defining, overseeing, and supporting the information security strategy, policies, and objectives of the organization, and ensuring that they are aligned with the business goals, stakeholder expectations, and regulatory requirements. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.1, page 181; CISM domain 1:
Information security governance [Updated 2022] | Infosec2; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition3

NEW QUESTION: 123
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: 124
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. 執行風險評估。

B. 標識要託管的資料。
C. 執行差距分析。
D. 分析業務需求。
Answer: (SHOW ANSWER)

NEW QUESTION: 125
在製定多年計劃時，資訊安全經理最重要的考慮因素是什麼？
A. 確保針對潛在資訊安全風險制定應急計劃
B. 確保與其他業務部門的計畫保持一致
C. 允許資訊安全計畫擴展其功能
D. 展示預計預算逐年增加
Answer: (SHOW ANSWER)
= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its various units. Alignment also means that the information security plan is consistent and compatible with the plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .
By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :
* Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization's performance, growth, and competitiveness.
The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization's assets, processes, and activities.
* Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.
* Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of

resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.
The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive and enabling aspects. Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization's needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization's financial situation or expectations1 . References = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk Management (IRM) [2022 update], Aligning Information Security with Business Strategy - ISACA, [Aligning Information Security with Business Objectives - ISACA]

NEW QUESTION: 126
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: 127
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. 根據組織策略重新調整資訊安全目標。
C. 將投資與組織的策略計畫連結起來。
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: 128
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: 129
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. 確定威脅發生時的影響。
B. 確定新出現的威脅的來源。
C. 將威脅對應到業務資□。
D. 回顧□業□的歷史威脅。
Answer: (SHOW ANSWER)

NEW QUESTION: 130
下列何者最能幫助組織維持適當的安全控制環境？
A. 與□業安全框架保持一致
B. 安全預算支持
C. 定期員工安全培訓
D. 威脅態勢監控
Answer: (SHOW ANSWER)
Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

NEW QUESTION: 131
發生安全漏洞後立即實施網路隔離技術，以便：
A. 依取證要求保留證據
B. 減少進一步損壞的程度。
C. 為關鍵利害關係人留出時間做決策。
D. 強制執行零信任架構原則。
Answer: (SHOW ANSWER)
Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or

networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. References = CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers & Explanations Database -
12 Month Subscription, Question ID: 1162

NEW QUESTION: 132
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: 133
在進行取證檢口之前，資訊安全經理應該：
A. 在乾淨的系統上口動原始硬碟。
B. 在新媒體上建立原始資料的影像。
C. 從備份媒體複製資料。
D. 關閉並重新定位伺服器。
Answer: (SHOW ANSWER)
= A forensic examination is a process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable. The first step in conducting a forensic examination is to create an image of the original data on new media, such as a hard disk, a CD-ROM, or a USB drive. This is done to ensure that the original data is not altered, damaged, or destroyed during the examination. An image is an exact copy of the data, including the file system, the slack space, and the deleted files. Creating an image also allows the examiner to work on a duplicate of the data, rather than the original, which may be needed as evidence in court. Booting the original hard disk on a clean system is not a good practice, as it may change

the data on the disk, such as the timestamps, the registry entries, and the log files. Duplicating data from the backup media is not sufficient, as the backup media may not contain all the data that is relevant to the investigation, such as the deleted files, the temporary files, and the swap files. Shutting down and relocating the server is not advisable, as it may cause data loss, corruption, or tampering. The server should be kept running and isolated from the network until an image is created. References = CISM Review Manual 15th Edition, page 204-205.
Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

NEW QUESTION: 134
下列何者最能支持資訊安全事件期間的有效溝通7
A. 頻繁的事件回應訓練課程
B. 集中控制監控功能
C. 角色描述中定義的職責
D. 預定的服務等級協定 (SLA)
Answer: D (LEAVE A REPLY)
The best way to support effective communication during information security incidents is to have predetermined service level agreements (SLAs) because they define the expectations and responsibilities of the parties involved in the incident response process, and specify the communication channels, methods, and frequency for reporting and updating on the incident status and resolution. Frequent incident response training sessions are not very effective because they do not address the communication needs or challenges during an actual incident.
Centralized control monitoring capabilities are not very effective because they do not address the communication needs or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or challenges during an actual incident. 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: 135
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: D (LEAVE A REPLY)

= 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 the incident to occur. Identifying the root cause helps to prevent or mitigate future incidents, as well as to improve the incident response process. Re-evaluating the impact of incidents, identifying vulnerabilities, and identifying control improvements are secondary objectives of a post-incident review, which are derived from the root cause analysis. References = CISM Review Manual, 16th Edition, page 3061; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1512 The primary objective of performing a post-incident review is to identify the root cause of the incident. After an incident has occurred, the post-incident review process involves gathering and analyzing evidence to determine the cause of the incident. This analysis will help to identify both the underlying vulnerability that allowed the incident to occur, as well as any control improvements that should be implemented to prevent similar incidents from occurring in the future. Additionally, the post-incident review process can also be used to re-evaluate the impact of the incident, as well as any potential implications for the organization.

NEW QUESTION: 136
下列哪一項是定期檢視網路安全威脅情勢的主要原因？
A. 將新興趨勢與現有組織安全狀況進行比較
B. 向高階管理層傳達最壞情況的情況
C. 訓練資訊安全專業人員以減輕新威脅
D. 確定擴大組織資訊安全的機會
Answer: A (LEAVE A REPLY)
The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks. References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

NEW QUESTION: 137
下列哪一個是用於識別和關聯入侵企圖警報的最佳工具？
A. 威脅分析軟體
B. 主機入侵偵測系統
C. SIEM
D. 網路入侵偵測系統
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Security Information and Event Management (SIEM) systems are designed to collect, analyze, and correlate data from multiple sources, making them the BEST choice for identifying and correlating intrusion attempt alerts.
* A. Threat analytics software: While this can provide insights, it is not specialized for real-time correlation and alerting across various platforms.
* B. Host intrusion detection system (HIDS): HIDS monitors individual hosts and detects intrusions, but it does not correlate alerts from multiple sources.
* C. SIEM: This is the BEST answer because SIEM integrates logs from diverse systems, applies correlation rules, and provides actionable insights into intrusion attempts.
* D. Network intrusion detection system (NIDS): While NIDS detects network-level anomalies, it does not correlate alerts from other systems.
Reference: CISM Job Practice Area 3 (Information Security Program Development and Management) discusses tools and techniques for monitoring and detecting security events.

NEW QUESTION: 138
下列哪一項是資訊安全經理定期檢視現有控制措施的主要原因？
A. 解決最終使用者控制申訴
B. 避免冗餘控制
C. 優先考慮安全措施
D. 為了因應新興風險
Answer: (SHOW ANSWER)

NEW QUESTION: 139
某組織計劃向客口提供一項受法規約束的新服務。在製定支持這項新服務的安全策略時，組織首先應該做什麼？
A. 確定新服務的安全控制。
B. 建立合規計劃,
C. 針對目前狀態執行差距分析
D. 僱用新資源來支援服務。

Answer: (SHOW ANSWER)

A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:

* It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.
* It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
* It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
* It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
* It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.

The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. References = 1: What is a Gap Analysis? | Smartsheet 2: 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 Learn more:
1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.
infosecinstitute.com+2 more

NEW QUESTION: 140

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: 141

識別與社會工程攻擊相關的風險的最佳方法是：

A. 監控入侵偵測系統（IDS），

B. 檢口單一登入 (SSO) 驗證延遲。

C. 測試使用者對資訊安全實務的了解。

D. 對電子郵件過濾系統執行業務風險評估。

Answer: (SHOW ANSWER)

The best way to identify the risk associated with a social engineering attack is to test user knowledge of information security practices. Social engineering is a type of attack that exploits human psychology and behavior to manipulate, deceive, or influence users into divulging sensitive information, granting unauthorized access, or performing malicious actions. Therefore, user knowledge of information security practices is a key factor that affects the likelihood and impact of a social engineering attack. By testing user knowledge of information security practices, such as through quizzes, surveys, or simulated attacks, the information security manager can measure the level of awareness, understanding, and compliance of the users, and identify the gaps, weaknesses, or vulnerabilities that need to be addressed.

Monitoring the intrusion detection system (IDS) (A) is a possible way to detect a social engineering attack, but not to identify the risk associated with it. An IDS is a system that monitors network or system activities and alerts or responds to any suspicious or malicious events. However, an IDS may not be able to prevent or recognize all types of social engineering attacks, especially those that rely on human interaction, such as phishing, vishing, or baiting. Moreover, monitoring the IDS is a reactive rather than proactive approach, as it only reveals the occurrence or consequences of a social engineering attack, not the potential or likelihood of it.

Reviewing single sign-on (SSO) authentication lags (B) is not a relevant way to identify the risk associated with a social engineering attack. SSO is a method of authentication that allows users to access multiple applications or systems with one set of credentials. Authentication lags are delays or failures in the authentication process that may affect the user experience or performance. However, authentication lags are not directly related to social engineering attacks, as they do not indicate the user's knowledge of information security practices, nor the attacker's attempts or success in compromising the user's credentials or access.
Performing a business risk assessment of the email filtering system (D) is also not a relevant way to identify the risk associated with a social engineering attack. An email filtering system is a system that scans, filters, and blocks incoming or outgoing emails based on predefined rules or criteria, such as spam, viruses, or phishing. A business risk assessment is a process that evaluates the potential threats, vulnerabilities, and impacts to the organization's business objectives, processes, and assets. However, performing a business risk assessment of the email filtering system does not address the risk associated with a social engineering attack, as it only focuses on the technical aspects and performance of the system, not the human factors and behavior of the users.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Identification, Subsection: Threat Identification, page 87-881

NEW QUESTION: 142
某個組織正在收購一家新公司，下列哪一項是確定如何在整合之前保護新收購的資料資口的最佳方法？
A. 在合約中包含安全要求
B. 評估安全控制。
C. 執行風險評估
D. 口看資料架構。
Answer: (SHOW ANSWER)
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION: 143

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

NEW QUESTION: 144
下列哪一項是確保資訊安全策略被理解的最有效方法？
A. 實施舉報計畫。
B. 提供定期的安全意識訓練。
C. 在職位口明中包含安全職責。
D. 記錄安全程序。
Answer: (SHOW ANSWER)
Security awareness training is the most effective way to ensure information security policies are understood, as it educates employees on the purpose, content and importance of the policies, and how to comply with them. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 183, section 4.3.3.1.

NEW QUESTION: 145
為了確保對組織的資訊資口提供一致的保護，下列哪一項是必要的？
A. 分類模型
B. 控制評估
C. 資料所有權
D. 監理要求
Answer: (SHOW ANSWER)
The answer to the question is A. Classification model. This is because a classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by:
Providing a common language and criteria for defining and communicating the security requirements and expectations for the information assets Enabling the identification and prioritization of the information assets that need the most protection and resources Facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification Supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) A classification model is a system of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. A classification model helps to ensure consistent protection for the organization's information assets by providing a common

language and criteria for defining and communicating the security requirements and expectations for the information assets, enabling the identification and prioritization of the information assets that need the most protection and resources, facilitating the implementation and enforcement of the appropriate level of security controls and measures for the information assets, based on their classification, and supporting the compliance with the legal, regulatory, and contractual obligations regarding the information assets. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISA Domain 5 - Protection of Information Assets2; CISM domain 3: Information security program development and management [2022 update]3; CISM Domain 2: Information Risk Management (IRM) [2022 update]4

NEW QUESTION: 146
一個組織正在考慮實施大數據解決方案來分析客口資料的可行性。為了支持這項舉措，資訊安全經理應該首先：
A. 庫存要由解決方案處理的敏感客口資料。
B. 確定資訊安全資源和預算需求。
C. 評估組織的潛在資訊安全風險。
D. 制定大數據解決方案的資訊安全要求。
Answer: (SHOW ANSWER)
Assessing potential information security risk to the organization is the first step that the information security manager should take when considering the feasibility of implementing a big data solution to analyze customer data, as it helps to identify and evaluate the threats, vulnerabilities, and impacts that may arise from the collection, processing, storage, and sharing of large volumes and varieties of customer data. Assessing risk also helps to determine the risk appetite and tolerance of the organization, and to prioritize the risk treatment options and security controls that are needed to protect the customer data and the big data solution. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Big Data Security and Privacy Issues in Healthcare1, page 1, section 1. Introduction.

NEW QUESTION: 147
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. 了解資訊資口的價口對於風險管理至關重要。
D. 所有員工都有安全責任。
Answer: D (LEAVE A REPLY)
= 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: 148
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. 將此問題提交給口部稽核以尋求建議。
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: 149
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: 150
下列哪一項是業務影響分析 (BIA) 的主要目的？
A. 定義安全角色與職責
B. 確定投資報酬率 (ROI)
C. 建立事件嚴重級別
D. 確定資訊資口的重要性
Answer: (SHOW ANSWER)

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. The primary purpose of a BIA is to determine the criticality of information assets and the impact of their unavailability on the organization's mission, objectives and reputation. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

NEW QUESTION: 151
在應對重大安全漏洞時，下列何者是讓外部取證專家參與證據收集的最重要原因？
A. 為回應團隊提供證據處理的專家培訓
B. 為了防止證據洩漏給任何口部工作人員
C. 驗證事件回應流程
D. 確保證據由合格的資源處理
Answer: (SHOW ANSWER)

NEW QUESTION: 152
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: (SHOW ANSWER)
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: 153
資訊安全經理了解到與組織想要實施的新興技術相關的新標準。資安經理應建議先執行下列哪一項操作？
A. 確定組織是否可以從採用新標準中受益。
B. 取得法律顧問關於標準對法規的適用性的意見,
C. 對新技術進行風險評估。
D. 回顧口業專家對新標準的分析。
Answer: (SHOW ANSWER)
= The first step that the information security manager should recommend when learning of a new standard related to an emerging technology is to determine whether the organization can benefit from adopting the new standard. This involves evaluating the business objectives, needs, and requirements of the organization, as well as the potential advantages, disadvantages, and challenges of implementing the new technology and the new standard. The information security manager should also consider the alignment of the new standard with the organization's existing policies, procedures, and standards, as well as the impact of the new standard on the organization's information security governance, risk management, program, and incident management. By conducting a preliminary analysis of the feasibility, suitability, and desirability of the new standard, the information security manager can provide a sound basis for further decision making and planning.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Standards, page 391; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 43, page 412.

NEW QUESTION: 154
一個組織實施了許多技術和管理控制措施來降低與勒索軟體相關的風險。在報告該計劃的績效時,向高階管理層提出的下列哪一項最重要？
A. 投資總成本
B. 成本和相關風險降低
C. 勒索軟體事件的數量和嚴重程度
D. 受勒索軟體影響的同業基準
Answer: (SHOW ANSWER)
The most important information to present to senior management when reporting on the performance of the initiative to mitigate risk associated with ransomware is the cost and

associated risk reduction, which means showing the value and effectiveness of the technical and administrative controls in terms of reducing the likelihood and impact of ransomware incidents and data extortion, and comparing them with the investment and resources required to implement and maintain them. The cost and associated risk reduction can help senior management to evaluate the return on investment (ROI) and the alignment with the business objectives and risk appetite of the initiative.
References = Ransomware Risk Management - NIST, #StopRansomware Guide | CISA

NEW QUESTION: 155
組織的資訊安全經理在社群媒體上了解到，最近購買的供應商口品已洩露，並且客口資料已發佈在網路上。資訊安全經理首先該做什麼？
A. 執行業務影響分析 (BIA)。
B. 將違規行為通知當地執法機關。
C. 口動事件回應程式。
D. 驗證組織面臨的風險。
Answer: (SHOW ANSWER)
The first thing that the information security manager should do after reading about a vendor product compromise on social media is to validate the risk to the organization. This means verifying the source and credibility of the information, determining if the organization uses the affected product, and assessing the potential impact and likelihood of the compromise on the organization's data and systems. Validating the risk to the organization will help the information security manager to decide on the appropriate course of action, such as activating the incident response program, notifying relevant stakeholders, or performing a BIA.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for identifying and assessing the risks associated with the use of third-party products and services" and that "the information security manager should monitor and review the security performance and incidents of third-party products and services 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: "Validating the risk to the organization is the correct answer because it is the first and most important step to take after reading about a vendor product compromise on social media, as it will help the information security manager to confirm the accuracy and relevance of the information, and to evaluate the potential consequences and probability of the compromise on the organization's data and systems" (p. 63). Additionally, the article Defending Against Software Supply Chain Attacks from the CISA website states that "the first step in responding to a software supply chain attack is to validate the risk to the organization by verifying the source and credibility of the information, determining if the organization uses the affected software, and assessing the potential impact and likelihood of the compromise on the organization's data and systems" (p. 2)

NEW QUESTION: 156
為了維持有效的資訊安全治理框架，必須建立下列哪一項？

A. 安全控制自動化
B. 定義的安全指標
C. 變更管理流程
D. 安全性原則規定
Answer: (SHOW ANSWER)
Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. References:
https://www.iso.org/standard/74046.html
https://www.nistf.gov/cyberframework
https://www.iso.org/standard/27001

NEW QUESTION: 157
事後審□發現用□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: 158
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: D (LEAVE A REPLY)
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: 159
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: 160

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: 161
下列哪一項對改善組織安全狀況的努力影響最大？
A. 定期向高階管理層報告
B. 高層對安全問題的支持態度
C. 安全控制自動化
D. 記錄完備的安全政策與程序
Answer: (SHOW ANSWER)
The supportive tone at the top regarding security is the greatest impact on efforts to improve an organization's security posture. This means that senior management should demonstrate their commitment and leadership to information security by setting clear goals, allocating adequate resources, communicating effectively, and rewarding good practices. A supportive tone at the top can also influence the culture and behavior of the organization, as well as foster trust and collaboration among stakeholders12. References = CISM Review Manual 15th Edition, page 1261; CISM Item Development Guide, page 82

NEW QUESTION: 162
下列何者最能顯示資訊安全投資的回報？
A. 年化損失預期 (ALE) 增加
B. 報告事件數量增加
C. 降低年度損失預期 (ALE)
D. 報告事件數量減少
Answer: (SHOW ANSWER)
A reduction in annualized loss expectancy (ALE) demonstrates that implemented controls have effectively reduced the organization's exposure to risk.
"ALE reduction is a key indicator of the cost-effectiveness of security investments and the improvement of the risk posture."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Cost-Benefit Analysis*

NEW QUESTION: 163
下列哪一項是遷移到雲端環境時使用雲端存取安全代理程式的最重要的好處？
A. 增強的資料治理
B. 增強第三者保證
C.)改善事件管理
D. 降低總擁有成本 (TCO)
Answer: (SHOW ANSWER)

According to the web search results, a cloud access security broker (CASB) is a software solution that stands between the cloud service provider and the cloud service user to enforce security controls. One of the most important benefits of using a CASB when migrating to a cloud environment is enhanced data governance, as it helps to protect sensitive information from unauthorized access, sharing, or loss. A CASB can also provide data classification, encryption, data loss prevention (DLP), and other features that enable organizations to manage and secure their data in the cloud.
References = What Is a Cloud Access Security Broker (CASB)?, A beginner's guide to cloud access security brokers

NEW QUESTION: 164
勒索軟體事件發生後，一個組織的系統得到了恢復。資安經理最應該關注下列哪一項？
A. 未滿足服務等級協定 (SLA)。
B. 未達到復原時間目標 (RTO)。
C. 根本原因尚未確定。
D. 向利害關係人的通知被延遲。
Answer: (SHOW ANSWER)
= After a ransomware incident, the most important concern for the information security manager is to identify the root cause of the incident and prevent it from happening again. The root cause analysis (RCA) is a systematic process of finding and eliminating the underlying factors that led to the incident, such as vulnerabilities, misconfigurations, human errors, or malicious actions. Without performing a RCA, the organization may not be able to address the root cause and may face the same or similar incidents in the future, which could result in more damage, costs, and reputational loss. Therefore, the information security manager should prioritize the RCA over other concerns, such as meeting the SLA, RTO, or notification requirements, which are important but secondary to the RCA.
References = CISM Review Manual 15th Edition, page 254-2551; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 4202

NEW QUESTION: 165
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. 執行隱私影響評估 (PIA)。
B. 執行差距分析。
C. 執行漏洞評估。
D. 執行業務影響分析 (BIA)。
Answer: (SHOW ANSWER)

NEW QUESTION: 166
在發生有限的勒索軟體事件後，下列何者最能實現操作恢復？
A. 根本原因分析

B. 影響評估
C. 可靠的映像備份
D. 記錄的根除程序
Answer: (SHOW ANSWER)

NEW QUESTION: 167
當機密資訊無意間傳播到組織外部時，下列哪一項是最佳行動方案？
A. 口看合規性要求。
B. 傳達曝光。
C. 宣告一個事件。
D. 更改加密金鑰。
Answer: (SHOW ANSWER)
Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task
4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

NEW QUESTION: 168
在收集可接受的證據時，下列哪一項是最重要的要求？
A. 需要知道
B. 保留審核日誌
C. 盡職調口
D. 監理鏈
Answer: (SHOW ANSWER)

Chain of custody is the MOST important requirement when collecting admissible evidence, because it ensures the integrity and authenticity of the evidence by documenting its history, handling, and storage. Chain of custody records who, what, when, where, why, and how the evidence was collected, analyzed, and preserved.
Without a proper chain of custody, the evidence may be challenged or rejected in a court of law. Need to know, preserving audit logs, and due diligence are important aspects of evidence collection, but they are not as critical as chain of custody. References = CISM Review Manual, 16th Edition, page 3031; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492The most important requirement when collecting admissible evidence is the chain of custody. The chain of custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

NEW QUESTION: 169
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: 170
下列哪一項對於確定是否遵守資訊安全政策最有幫助？
A. 偵探控制
B. 修正控制
C. 預防控制
D. 指令控制
Answer: (SHOW ANSWER)

NEW QUESTION: 171
下列哪一項是偵測安全事件最有效的方法？
A. 分析最近的安全風險評估。
B. 分析安全異常。

C. 分析滲透測試結果。
D. 分析漏洞評估。
Answer: (SHOW ANSWER)
Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

NEW QUESTION: 172
下列哪一項需要恢復點目標 (RPO)？
A. 災難復原計畫 (DRP)
B. 資訊安全計劃
C. 事件回應計劃
D. 業務連續性計劃 (BCP)
Answer: (SHOW ANSWER)
A recovery point objective (RPO) is required in a disaster recovery plan (DRP), because it indicates the earliest point in time to which it is acceptable to recover data after a disaster. It effectively quantifies the permissible amount of data loss in case of interruption. It is determined based on the acceptable data loss in case of disruption of operations1. A DRP is a document that defines the procedures, resources, and actions to restore the critical IT systems and data in the event of a disaster that affects the normal operations of the organization2. A DRP should include the RPO for each critical system and data, as well as the backup and restoration methods, frequency, and location to achieve the RPO3.
A RPO is not required in an information security plan, an incident response plan, or a business continuity plan (BCP), because these plans have different purposes and scopes. An information security plan is a document that defines the objectives, policies, standards, and guidelines for information security management in the organization4. An incident response plan is a document that defines the procedures, roles, and responsibilities for identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. A BCP is a document that defines the procedures, resources, and actions to ensure the continuity of the essential business functions and processes in the event of a disruption that affects the normal operations of the organization. These plans may include other metrics, such as recovery time objective (RTO), which is the amount of time after a disaster in which business operation is resumed, or resources are again available for use, but they do not require a RPO.

References = 1: IS Disaster Recovery Objectives - RunModule 2: Information System Contingency Planning Guidance - ISACA 3: CISM Certified Information Security Manager - Question1411 4: CISM Review Manual, 16th Edition, ISACA, 2021, page 23. : CISM Review Manual, 16th Edition, ISACA, 2021, page 223.
CISM Review Manual, 16th Edition, ISACA, 2021, page 199. : RTO vs. RPO - What is the difference? - Advisera

NEW QUESTION: 173
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: 174
下列哪個事件回應階段涉及在維持業務運作的同時幫助保護關鍵系統的行動？
A. 遏制
B. 準備
C. 恢復
D. 識別
Answer: (SHOW ANSWER)

NEW QUESTION: 175
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. 能口在部署之前測試補丁
B. 事件回應計畫的充分性
C. 修補程式的文檔
D. 實施控制的資源可用性

Answer: (SHOW ANSWER)

NEW QUESTION: 176
下列何者最能讓員工接受資訊安全政策？
A. 強大的高階管理層支持
B. 以電腦為基礎的培訓
C. 強大的事件回應程序
D. 充足的安全資金
Answer: (SHOW ANSWER)
= Strong senior management support is the best factor to enable staff acceptance of information security policies, as it demonstrates the commitment and leadership of the organization's top executives in promoting and enforcing a security culture. Senior management support can also help ensure that the information security policies are aligned with the business goals and values, communicated effectively to all levels of the organization, and integrated into the performance evaluation and reward systems. Senior management support can also help overcome any resistance or challenges from other stakeholders, such as business units, customers, or regulators123. References =
* 1: CISM Review Manual 15th Edition, page 26-274
* 2: CISM Practice Quiz, question 1102
* 3: Information Security Governance: Guidance for Boards of Directors and Executive Management,
2nd Edition, page 5-6

NEW QUESTION: 177
在對攻擊進行事件後審口時，以下哪一項對資訊安全經理最有用？
A. 組織的攻擊成本
B. 攻擊者的位置
C. 攻擊者所使用的操作方法
D. 來自入侵偵測系統 (IDS) 日誌的詳細信息
Answer: (SHOW ANSWER)
= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

NEW QUESTION: 178
下列哪一項是幫助確保組織的風險偏好納入風險處理流程的最佳方式？
A. 建立關鍵風險指標 (KRI)。
B. 使用定量風險評估方法。
C. 定期向高階管理層報告風險處理狀況
D. 需要指導委員會批准風險處理計畫。
Answer: (SHOW ANSWER)
= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management.
However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter
2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION: 179
下列哪一項最適合用來確定資訊安全計畫的成熟度？
A. 安全預算分配
B. 組織風險偏好
C. 風險評估結果
D. 安全指標
Answer: (SHOW ANSWER)

Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes.
Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
References:
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security- governance-part-1
https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing- information-security

NEW QUESTION: 180
當資安經理發現某個部門屢次不遵守安全策略時，下一步該採取什麼行動？
A. 引入額外的控制措施以強制遵守政策。
B. 向高階管理層報告違反政策的情況。
C. 請部門使用者重複進行安全意識訓練。
D. 對部門口的系統進行漏洞評估。
Answer: (SHOW ANSWER)

NEW QUESTION: 181
下列哪一項是確定防火牆是否已配置為提供全面外圍防禦的最佳方法9
A. 目前防火牆規則集的驗證
B. 來自口部來源的防火牆連接埠掃描
C. 來自外部來源的 ping 測試
D. 針對防火牆的類比拒口服務 (DoS) 攻擊
Answer: (SHOW ANSWER)
A validation of the current firewall rule set is the best method for determining whether a firewall has been configured to provide a comprehensive perimeter defense because it verifies that the firewall rules are consistent, accurate, and effective in allowing or blocking traffic according to the security policies and standards of the organization. A port scan of the firewall from an internal source is not a good method because it does not test the firewall's behavior from an external perspective, which is more relevant for perimeter defense. A ping test from an external source is not a good method because it only tests the firewall's availability and responsiveness, not its security or functionality. A simulated denial of service (DoS) attack against the firewall is not a good method because it only tests the firewall's resilience and performance under high traffic load, not its security or functionality. 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/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca- journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 182
下列哪一個指標最適合評估事件通知流程？
A. 每個報告事件的平均停機總成本
B. 回應與解決之間經過的時間
C. 每個報告週期的平均事件數
D. 檢測、報告和回應之間經過的時間
Answer: (SHOW ANSWER)
Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.
References:
* https://www.atlassian.com/incident-management/kpis/common-metrics
* https://securityscorecard.com/blog/how-to-use-incident-response-metrics/
* https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

NEW QUESTION: 183
下列哪一項對組織對新□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: C (LEAVE A REPLY)

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: 184
在更新資訊安全政策以適應新法規時，資訊安全經理應首先：
A. 檢討關鍵風險指標 (KRI)
B. 執行差距分析
C. 諮詢流程擁有者
D. 更新關鍵績效指標 (KPI)
Answer: (SHOW ANSWER)
A gap analysis identifies the differences between current practices and the new regulatory requirements, ensuring targeted and effective policy updates.
"Performing a gap analysis is critical to identify the areas where the current policy falls short of new regulatory requirements."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance* ISACA practice questions confirm that a gap analysis is the foundational step before engaging stakeholders or updating policies.

NEW QUESTION: 185
下列哪一項最能幫助及時執行事件回應計畫？
A. 決策支援工具的引入
B. 觸發事件的定義
C. 明確定義的資料分類過程
D. 集中服務台
Answer: (SHOW ANSWER)
Definition of trigger events is the best way to enable the timely execution of an incident response plan because it helps to specify the conditions or criteria that initiate the incident response process. Trigger events are predefined scenarios or indicators that signal the occurrence or potential occurrence of a security incident, such as a ransomware attack, a data breach, a denial-of-service attack, or an unauthorized access attempt.
Definition of trigger events helps to ensure that the incident response team is alerted and activated as soon as possible, as well as to determine the appropriate level and scope of response based on the severity and impact of the incident. Therefore, definition of trigger events is the correct answer.
References:
* https://www.atlassian.com/incident-management/kpis/common-metrics

* https://www.varonis.com/blog/incident-response-plan/
* https://holierthantao.com/2023/05/03/minimizing-disruptions-a-comprehensive-guide-to-incident-response-planning-and-execution/

NEW QUESTION: 186
下列哪一項是在高流動率組織中實施事件通知和升級流程的最大障礙？
A. 缺乏流程文檔
B. 缺乏知識豐富的人員
C. 與組織目標缺乏一致性
D. 缺乏溝通過程
Answer: (SHOW ANSWER)

NEW QUESTION: 187
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: 188
下列何者最有利於恢復因網路安全事件而遺失的資料？
A. 可移動儲存媒體
B. 災難復原計畫 (DRP)
C. 異地資料備份
D. 加密資料驅動器
Answer: (SHOW ANSWER)
The best option to facilitate recovery of data lost as a result of a cybersecurity incident is offsite data backups.
This is because offsite data backups provide a secure and reliable way to restore data that may have been corrupted, deleted, or encrypted by malicious actors. Offsite data backups also reduce

the risk of data loss due to physical damage, theft, or natural disasters that may affect the primary data storage location. Offsite data backups should be part of a comprehensive disaster recovery plan (DRP) that defines the roles, responsibilities, procedures, and resources for restoring normal operations after a cyber incident.

NEW QUESTION: 189
以下人員中，誰最適合承擔與特權存取控制失敗相關的風險？
A. 資料擁有者
B. 企業主
C. 資訊安全經理
D. 合規經理
Answer: (SHOW ANSWER)
The business owner is the most appropriate person to own the risk associated with the failure of a privileged access control because they are ultimately responsible for the protection and use of the information in their business unit1. The data owner is responsible for determining the access rights for specific data sets, but not for the access control mechanisms2. The information security manager is responsible for implementing and enforcing the security policies and standards, but not for owning the risk3. The compliance manager is responsible for ensuring that the organization meets the regulatory requirements, but not for owning the risk3.
References: 1 https://www.cyberark.com/resources/blog/how-do-you-prioritize-risk-for-privileged-access- management 3 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for- privileged-access-management 2 https://security.stackexchange.com/questions/218049/what-is-the-difference- between-data-owner-data-custodian-and-system-owner

NEW QUESTION: 190
在建立組織的資訊安全治理委員會時，下列哪一項是最重要的考量因素？
A. 成員了解資訊安全控制。
B. 成員為商業風險負責人。
C. 成員定期輪替。
D. 成員代表整個組織的功能。
Answer: (SHOW ANSWER)
= The most important consideration when establishing an organization's information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization's business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization's mission, vision, and values. Having a diverse and representative committee also helps to foster a culture

of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.
Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization's business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization's business objectives, and to allocate appropriate resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the organization's information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee' s ability to monitor and evaluate the performance and progress of the information security program. References =
* ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37.
* ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID
1014.

NEW QUESTION: 191
下列哪一項是治理不遵守安全要求的最佳方法？
A. 根據殘餘風險進行強制審口和例外批准，
B. 請使用者確認可接受的使用政策。
C. 請指導委員會審口例外請求。
D. 根據固有風險進行強制審口和例外批准。
Answer: (SHOW ANSWER)
= Residual risk is the risk that remains after applying security controls. It reflects the actual exposure of the organization to noncompliance issues. Therefore, basing mandatory review and exception approvals on residual risk is the best approach for governing noncompliance with security requirements. It ensures that the organization is aware of the potential impact and likelihood of noncompliance and can make informed decisions about accepting, mitigating, or transferring the risk. References = CISM Review Manual 15th Edition, page 78.

NEW QUESTION: 192
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: B (LEAVE A REPLY)
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: 193
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. 接受
B. 緩解
C. 轉移
D. 避免
Answer: (SHOW ANSWER)

NEW QUESTION: 194
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: 195
在測試從勒索軟體攻擊中復原的事件回應計畫時，下列哪一項最需要驗證？
A. 數位貨幣立即可用。
B. 網路存取需要雙重認證。
C. 資料備份可從異地位置還原。
D. 備用網路連結立即可用。
Answer: (SHOW ANSWER)
Data backups are recoverable from an offsite location is the most important thing to verify when testing an incident response plan for recovery from a ransomware attack, as it ensures that the organization can restore its data and resume its operations without paying the ransom or losing critical information. Data backups should be performed regularly, stored securely, and tested for integrity and availability. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 196
在回應導致應用程式伺服器上出現惡意軟體的事件時，下列哪種根除方法最適合？
A. 斷開系統與網路的連線。
B. 更改受感染系統上的密碼。
C. 從已知良好的備份還原系統。
D. 執行作業系統強化。
Answer: (SHOW ANSWER)

Restoring the system from a known good backup is the most appropriate eradication method when responding to an incident resulting in malware on an application server, as it ensures that the system is free of any malicious code and that the data and applications are consistent with the expected state. Disconnecting the system from the network may prevent further spread of the malware, but it does not eradicate it from the system. Changing passwords on the compromised system may reduce the risk of unauthorized access, but it does not remove the malware from the system. Performing operation system hardening may improve the security configuration of the system, but it does not guarantee that the malware is eliminated from the system.
References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.4

NEW QUESTION: 197
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: 198
在對資訊資口進行分類時，資訊安全經理注意到多個生口資料庫沒有為其分配所有者。
A. 將職責指派給資料庫管理員 (DBA)。
B. 口看資料庫中的敏感口容。
C. 為高階管理層準備一份資料庫報告。
D. 為這些資料庫指派最高分類等級。
Answer: (SHOW ANSWER)
Information asset classification is the process of identifying, labeling, and categorizing information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to establish appropriate security controls, policies, and procedures for protecting the information assets from unauthorized access, use, disclosure, modification, or destruction. One of the key elements of information asset classification is assigning owners to each information asset. Owners are responsible for managing the information asset throughout its lifecycle, including defining its security requirements, implementing security controls, monitoring its usage and performance, reporting any incidents or breaches, and ensuring compliance with legal and regulatory obligations. Therefore, assigning responsibility to the database administrator (DBA) is the best way to address the situation where several production databases do not have owners assigned to them. References = CISM Review Manual 15th Edition1, page 256; Information Asset and Security Classification Procedure2.

NEW QUESTION: 199
事件回應過程中根除階段的主要目標是：
A. 維持嚴格的監管鏈。
B. 提供有效的事件分類與遏制。
C. 消除威脅並恢復受影響的系統
D. 從受影響的系統取得取證證據。
Answer: (SHOW ANSWER)
The primary goal of the eradication phase in an incident response process is to remove the threat and restore affected systems because it eliminates any traces or remnants of malicious activity or compromise from the systems or network, and returns them to their normal or secure state. Maintaining a strict chain of custody is not a goal of the eradication phase, but rather a requirement for preserving and documenting digital evidence throughout the incident response process. Providing effective triage and containment of the incident is not a goal of the eradication phase, but rather a goal of the containment phase, which isolates and stops the spread of malicious activity or compromise. Obtaining forensic evidence from the affected system is not a goal of the eradication phase, but rather a goal of the identification phase, which collects and

analyzes data or artifacts related to malicious activity or compromise. 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: 200
制定業務連續性計畫 (BCP) 時應先執行下列哪項操作？
A. 定義組織策略。
B. 決定關鍵流程的優先順序。
C. 檢視現有的網路保險範圍。
D. 口看目前的復原策略。
Answer: (SHOW ANSWER)

NEW QUESTION: 201
採用資訊安全框架的主要好處是它提供：
A. 可靠的新興威脅情報。
B. 安全與漏洞報告指南。
C. 常見的可利用性指數。
D. 標準化安全控制。
Answer: (SHOW ANSWER)
A standardized security control is a set of rules, guidelines, or best practices that are designed to protect the confidentiality, integrity, and availability of information assets and systems. An information security framework is a collection of standardized security controls that are aligned with the organization's objectives, strategy, and risk appetite. Adopting an information security framework provides a primary benefit of ensuring consistency, efficiency, and effectiveness in the implementation and management of information security across the organization.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is an Information Security Framework?; Information Security Frameworks: What Are They and Why Do You Need One?

NEW QUESTION: 202
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. 定期進行風險評估
C. 定期進行安全審核
D. 頻繁的安全架構審口
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203

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: 204

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. 備份在多個站點維護並定期審口。

D. 受影響的網路可以在網路交換器層級分離。

Answer: (SHOW ANSWER)

NEW QUESTION: 205

當有關資訊安全投資的管理決策是基於以下因素時，它們將是最有效的：

A. 辨識和分析威脅和漏洞的過程。
B. 根據安全事件歷史確定的年度預期損失 (ALE),
C. 報告一致且定期的風險評估。
D. 管理階層正式接受風險分析,
Answer: (SHOW ANSWER)
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION: 206
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: 207

下列何者是預防資訊安全事件最有效的方法？
A. 實施安全資訊和事件管理 (SIEM) 工具
B. 實施員工安全意識培訓計劃
C. 部署一致的事件回應方法
D. 在網路環境中部署入侵偵測工具
Answer: (SHOW ANSWER)
The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management (SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

NEW QUESTION: 208
下列哪一項是管理使用者存取權限以確保與資料分類保持一致的最佳方法？
A. 將存取權限的管理委託給獨立的第三方。
B. 每年或每當工作職責變更時審□存取權限
C. 對使用者和管理員帳□□用多重身份驗證。
D. 登入嘗試失敗一定次數後鎖定帳號。
Answer: (SHOW ANSWER)

NEW QUESTION: 209
為了使員工行為與組織的資訊安全目標一致，應先考慮下列哪一種控制類型？
A. 技術安全控制
B. 存取安全控制
C. 實體安全控制
D. 管理安全控制
Answer: (SHOW ANSWER)

NEW QUESTION: 210
當漏洞被揭露後，資訊安全經理應該先執行下列哪一項操作？
A. 執行補丁更新。
B. 進行風險評估。
C. 執行滲透測試。
D. 進行影響評估。
Answer: (SHOW ANSWER)

According to the CISM Review Manual, the first step an information security manager should take when a vulnerability has been disclosed is to conduct a risk assessment to determine the likelihood and impact of the vulnerability being exploited, and the appropriate response strategy. Performing a patch update, a penetration test or an impact assessment are possible subsequent steps, but not the first one.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.3.2, page 1331.

NEW QUESTION: 211
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: 212
下列哪一項是風險緩解的例子？
A. 購買保險

B. 停止與風險相關的活動
C. 改善安全控制
D. 執行成本效益分析
Answer: (SHOW ANSWER)
Improving security controls is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. Risk mitigation can be achieved by implementing various strategies, such as purchasing insurance, discontinuing the activity associated with the risk, or improving security controls. Purchasing insurance is a form of risk transfer, which is the process of shifting the responsibility or burden of a risk to another party. Discontinuing the activity associated with the risk is a form of risk avoidance, which is the process of eliminating or avoiding a potential source of harm. Performing a cost-benefit analysis is a form of risk evaluation, which is the process of assessing the costs and benefits of different options to manage a risk. References = CISM Review Manual, 16th Edition, page 1741; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 802

NEW QUESTION: 213
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. 強制保留數據
B. 與業界同業進行基準比較
C. 制定政策標準
D. 資訊資口分類
Answer: (SHOW ANSWER)

NEW QUESTION: 214
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

NEW QUESTION: 215
下列何者最能顯示供應商風險管理流程的有效性？
A. 全球公認安全標準認證的供應商比例增加
B. 完成盡職調口的供應商百分比增加
C. 進行強制性安全訓練的供應商比例增加
D. 報告安全漏洞的供應商百分比增加
Answer: (SHOW ANSWER)
This answer best indicates the effectiveness of the vendor risk management process because it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices.
A globally recognized security standard, such as ISO 27001, NIST CSF, or COBIT, provides a comprehensive and objective framework for assessing and improving the security posture and performance of vendors.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security requirements and expectations for third-party products and services are defined, communicated, and enforced" and that "the information security manager should verify that the third parties have implemented adequate security controls and practices, and that they comply with applicable standards and regulations" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Increase in the percentage of vendors certified to a globally recognized security standard is the correct answer because it best indicates the effectiveness of the vendor risk management process, as it shows that the organization has established and enforced clear and consistent security requirements and expectations for its vendors, and that the vendors have demonstrated their compliance and commitment to security best practices" (p. 63). Additionally, the article Vendor Risk Management Demystified from the ISACA Journal 2015 states that "a globally recognized security standard provides a common language and framework for evaluating and improving the security posture and performance of vendors" and that "a vendor certification to a globally recognized security standard can help to reduce the risk of security breaches, increase the trust and confidence of customers and stakeholders, and enhance the reputation and competitiveness of the vendor" (p. 3

NEW QUESTION: 216
在為組織制定資訊安全策略時，下列何者最有助於理解應重點關注何處？
A. 差距分析
B. 專案計劃
C. 漏洞評估
D. 商業影響分析 (BIA)

Answer: (SHOW ANSWER)
Gap analysis is the MOST helpful tool for understanding where to focus efforts when developing an information security strategy for an organization, because it helps to identify the current state and the desired state of the information security governance, and the gaps between them. Gap analysis also helps to prioritize the actions and resources needed to close the gaps and achieve the information security objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Gap analysis is the process of comparing the current state and the desired state of information security governance and identifying the gaps that need to be addressed." CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Gap analysis should be performed periodically to assess the effectiveness and efficiency of the information security strategy and program and to identify the areas for improvement." CISM domain 1: Information security governance [Updated 2022] - Infosec Resources: "Gap analysis: This is a comparison of the current state of security with the desired state. It helps to identify the gaps in security and prioritize the actions required to close them."

NEW QUESTION: 217
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: 218
進行業務影響分析 (BIA) 的主要目的是確定：
A. 業務恢復所需的資源。
B. 業務連續性計劃的範圍。
C. 復原時間目標 (RTO)。

D. 事件回應計畫的範圍。
Answer: (SHOW ANSWER)

NEW QUESTION: 219
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: 220
哪種類型的復原網站最可靠且可以支援嚴格的復原要求？
A. 冷站點
B. 溫暖站點
C. 熱門站點
D. 行動網站
Answer: C (LEAVE A REPLY)
A hot site is the most reliable type of recovery site and can support stringent recovery requirements because it is a fully operational facility that mirrors the primary production center. A hot site has all the hardware, software, data, network, and personnel ready to resume the critical business functions within minutes of a disruptive event. A hot site also has backup power, security, and communication systems to ensure the continuity of operations.
References: The CISM Review Manual 2023 defines a hot site as "a fully operational facility that mirrors the primary production center" and states that "a hot site can support stringent recovery requirements and provide the shortest recovery time" (p. 190). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A hot site is the correct answer because it is the most reliable type of recovery site and can support stringent recovery requirements, as it is a fully operational facility that mirrors the primary production center and can resume the critical business functions within minutes of a disruptive

event" (p. 96). Additionally, the web search result 1 states that "the recovery site can be hot, warm, cold or mobile. Hot sites are facilities that mirror the primary production center" and that "hot sites are the most reliable and can support stringent recovery requirements" (p. 1).

NEW QUESTION: 221
下列哪一項事件最有可能要求組織重新檢視其資訊安全框架？
A. IT 提供的新服務
B. 風險情勢的變化
C. 最近的網路安全攻擊
D. 實施了一項新技術
Answer: (SHOW ANSWER)
Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

NEW QUESTION: 222
資訊安全策略中包含下列哪一項最重要？
A. 基線
B. 管理目標
C. 最佳實踐
D. 成熟度級別
Answer: (SHOW ANSWER)

NEW QUESTION: 223
建立安全指標的根本目的是：
A. 提高投資報酬率 (ROI)
B. 提供有關控制有效性的回饋
C. 採用安全最佳實踐
D. 建立安全基準
Answer: B (LEAVE A REPLY)
The fundamental purpose of establishing security metrics is to provide feedback on the effectiveness of the information security controls and processes. Security metrics are quantitative

or qualitative measures that indicate how well the organization is achieving its security objectives and goals. Security metrics can help the information security manager to monitor, evaluate, and improve the performance of the information security program, as well as to identify gaps, weaknesses, and areas for improvement. Security metrics can also help the organization to demonstrate compliance with internal and external standards, regulations, and best practices. Increasing return on investment (ROI), adopting security best practices, and establishing security benchmarks are possible outcomes or benefits of using security metrics, but they are not the fundamental purpose of establishing them. References = CISM Review Manual, 16th Edition, pages 46-471; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 642
Learn more:
1. isaca.org2. amazon.com3. gov.uk
Security metrics are used to measure the effectiveness of controls and evaluate the overall security posture of an organization. This feedback provides an understanding of the progress made towards achieving security objectives and allows organizations to make necessary adjustments.

NEW QUESTION: 224
容量規劃將防止：
A. 分散式阻斷服務 (DDoS) 攻擊所造成的檔案系統過載。
B. 因計畫的安全維護而導致的系統停機。
C. 因硬體資源不足而導致應用程式失敗。
D. 因利用緩衝區容量漏洞而導致的軟體故障。
Answer: C (LEAVE A REPLY)
Capacity planning is the process of estimating and allocating the required resources (such as CPU, memory, disk space, bandwidth, etc.) to meet the current and future demands of the information systems and applications. Capacity planning would prevent application failures arising from insufficient hardware resources, as it would ensure that the applications have enough resources to function properly and efficiently, and avoid performance degradation, errors, or crashes.
References = CISM Review Manual 2022, page 3081; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.92; What is Capacity Planning? Definition and Examples

NEW QUESTION: 225
某個組織收到了用口的投訴，表示他們的某些文件已被加密。這些用口收到了解密檔案所需的金錢要求。下列哪一項是最好的行動方案？
A. 進行影響評估。
B. 隔離受影響的系統。
C. 重建受影響的系統。
D. 口動事件回應。
Answer: (SHOW ANSWER)

The best course of action when the organization receives complaints from users that some of their files have been encrypted and they are receiving demands for money to decrypt the files is to initiate incident response.
This is because the organization is facing a ransomware attack, which is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and loss to the organization's operations, assets, and reputation. Therefore, the organization needs to quickly activate its incident response plan and team, which are designed to handle such security incidents in a coordinated, effective, and efficient manner. The incident response process involves the following steps1:
* Preparation: The incident response team prepares the necessary resources, tools, and procedures to respond to the incident. The team also establishes the roles, responsibilities, and communication channels among the team members and other stakeholders.
* Identification: The incident response team identifies the scope, source, and severity of the incident. The team also collects and preserves the relevant evidence and logs for further analysis and investigation.
* Containment: The incident response team isolates the affected systems and networks to prevent the spread of the ransomware and limit the impact of the incident. The team also implements temporary or alternative solutions to restore the essential functions and services.
* Eradication: The incident response team removes the ransomware and any traces of its infection from the affected systems and networks. The team also verifies that the systems and networks are clean and secure before restoring them to normal operations.
* Recovery: The incident response team restores the affected systems and networks to normal operations.
The team also decrypts or restores the encrypted data from backups or other sources, if possible. The team also monitors the systems and networks for any signs of recurrence or residual issues.
* Lessons learned: The incident response team conducts a post-incident review to evaluate the effectiveness and efficiency of the incident response process and team. The team also identifies the root causes, lessons learned, and best practices from the incident. The team also recommends and implements the necessary improvements and corrective actions to prevent or mitigate similar incidents in the future.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Process, pages 229-2331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 45, page 432.

NEW QUESTION: 226
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. 滲透測試結果
B. 資料預存程序
C. 資料保護口品的特點
D. 資料分類策略

Answer: (SHOW ANSWER)

NEW QUESTION: 227
下列哪一項指標可以準確衡量資訊安全計畫的表現？
A. 支持決策的定性和定量趨勢的組合
B. 準確衡量安全異常的定性指標集合
C. 與口業基準進行比較的量化指標集合
D. 從分配給安全計畫的各種措施中得出的單一數字分數
Answer: (SHOW ANSWER)

NEW QUESTION: 228
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. 企業文化。
B. 威脅環境。
C. 資訊安全最佳實務。
D. 風險管理技術。
Answer: (SHOW ANSWER)

NEW QUESTION: 229
衡量下列哪一項是確定資訊安全策略與組織目標一致性的最精確方法？
A. 阻止入侵嘗試的次數
B. 高階管理層審口的業務案例數量
C. 已識別的業務威脅數量趨勢
D. 整合到業務流程中的控制的百分比
Answer: (SHOW ANSWER)
Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number

of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations.
References = CISM Review Manual 2023, page 291; CISM Review Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

NEW QUESTION: 230
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: 231
下列哪一項應該是建立衡量資訊安全計畫有效性的指標的主要基礎？
A. 剩餘風險
B. 監理要求
C. 風險承受能力
D. 控制目標
Answer: (SHOW ANSWER)
The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the

business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance. References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 232
下列哪一項是減少不必要的合規活動重複的最佳方法？
A. 控製程式的文檔
B. 合規性要求的標準化
C. 控制自動化
D. 保障工作的整合
Answer: (SHOW ANSWER)
= Standardization of compliance requirements is the best approach to reduce unnecessary duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business partners. Standardization also facilitates the alignment of compliance activities with the organization's risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. References = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

NEW QUESTION: 233
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: 234
下列哪一項是資訊資口分類的最大好處？
A. 協助確定復原點目標 (RPO)
B. 為實施需要了解的政策提供基礎
C. 支援職責分離

D. 定義資源所有權

Answer: (SHOW ANSWER)

The greatest benefit of information asset classification is providing a basis for imple-menting a need-to-know policy. Information asset classification is a process of catego-rizing information based on its level of sensitivity and importance, and applying appro-priate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by:

*Defining the value and protection requirements of different types of information

*Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret

*Establishing the roles and responsibilities of information owners, custodians, and users

*Enforcing access controls and encryption for the information

*Documenting the security policies and procedures for the information

By providing a basis for implementing a need-to-know policy, information asset classi-fication can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification.

Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud4.

De-fining resource ownership is not a benefit, but rather a component of information asset classification.

Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5. References: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3:

Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST : Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy

- UCI

NEW QUESTION: 235

一家新創公司在生口環境中部署了多個存在漏洞的新應用程序，原因是未進行安全審口。BEST 將如何協助確保未來有效的應用程式風險管理？

A. 在部署之前對應用程式進行自動掃描。

B. 以安全工程師補充現有的開發團隊。
C. 將資訊安全融入現有的變更管理
D. 創建一個新的應用程式安全治理委員會。
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
Integrating information security into existing change management processes ensures that security considerations are included in all application changes and deployments. This addresses the root cause of bypassed security reviews and provides a consistent, repeatable process to manage risk going forward.
"Integrating security into change management ensures that changes to systems and applications undergo appropriate security review and testing prior to implementation, thereby addressing vulnerabilities proactively."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Change Management*

NEW QUESTION: 236
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: 237
下列哪一項是組織向受影響方傳達已發生安全事件的最重要原因？
A. 提高資訊安全意識
B. 揭露事件的根本原因
C. 增加對組織的好感
D. 遵守有關通知的規定
Answer: (SHOW ANSWER)
Complying with regulations regarding notification is the most important reason for an organization to communicate to affected parties that a security incident has occurred, as it helps to avoid legal penalties, fines, or sanctions that may result from failing to notify the relevant authorities, customers, or other stakeholders in a timely and appropriate manner. Additionally, complying with regulations regarding notification may also help to preserve the trust and reputation of the organization, as well as to facilitate the investigation and resolution of the incident.
References = CISM Review Manual 2022, page 3151; CISM Exam Content Outline, Domain 4, Task 4.5

NEW QUESTION: 238
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: 239
當組織網路中的物聯網 (IoT) 設備被確認遭到駭客攻擊時，第一步應該是什麼？

A. 監控網路。
B. 執行取證分析。
C. 斷開設備與網路的連接,
D. 升級至事件回應團隊
Answer: (SHOW ANSWER)
= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures123. References =
* 1: CISM Review Manual 15th Edition, page 2004
* 2: CISM Practice Quiz, question 1072
* 3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

NEW QUESTION: 240
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. 購買網路安全保險。
B. 接受繼續使用該應用程式所帶來的風險。
C. 停止使用該應用程式。
D. 為應用程式實施補償控制。
Answer: (SHOW ANSWER)

NEW QUESTION: 241
進行災難復原測試的最適當時間是在以下時間之後：
A. 主要業務流程已重新設計。
B. 業務連續性計劃 (BCP) 已更新。
C. 安全風險狀況已審核
D. 已記錄不合規事件。
Answer: (SHOW ANSWER)
The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well as identify any gaps, issues, or improvement opportunities123. References =
1: CISM Review Manual 15th Edition, page 2114
2: CISM Practice Quiz, question 1042

3: Business Continuity Planning and Disaster Recovery Testing, section "Testing the Plan"

NEW QUESTION: 242
在為制定事件回應計畫而建立安全事件分類時，下列哪一項提供了最有價口的意見？
A. 業務連續性計劃 (BCP)
B. 業務影響分析 (BIA) 結果
C. 漏洞評估結果
D. 高階管理層的建議
Answer: (SHOW ANSWER)

NEW QUESTION: 243
下列何者最能緩解意外資料遺失事件？
A. 定期進行使用者意識培訓。
B. 獲得高階管理層對資訊安全策略的支持。
C. 進行資料遺失防護 (DLP) 審核。
D. 強制執行資料硬碟加密策略。
Answer: (SHOW ANSWER)
Conducting periodic user awareness training is the best way to mitigate accidental data loss events because it can educate the users on the causes, consequences, and prevention of data loss, and increase their awareness of the security policies and procedures of the organization. User awareness training can also help users to identify and report potential data loss incidents, and to adopt good practices such as backing up data, encrypting data, and using secure channels for data transmission and storage.
References: The article Mistakes Happen-Mitigating Unintentional Data Loss from the ISACA Journal 2018 states that "user awareness training is the most effective way to prevent unintentional data loss" and that "user awareness training should include information on the types and sources of data loss, the impact and cost of data loss, the legal and regulatory requirements for data protection, the organization's data security policies and procedures, the roles and responsibilities of users in data security, the best practices and tools for data security, and the reporting and escalation process for data loss incidents" (p. 2)1. The Data Spill Management Guide from the Cyber.gov.au website also states that "user awareness training is an important preventative measure to reduce the likelihood of data spills" and that "user awareness training

should cover topics such as data classification, data handling, data storage, data transmission, data disposal, and data spill reporting" (p. 2)

NEW QUESTION: 244
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: 245
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: 246
下列哪一個角色負責確保評估新監理架構對業務系統的影響？
A. 資訊安全經理
B. 應用程式擁有者
C. 法定代理人
D. 高階管理層
Answer: (SHOW ANSWER)

NEW QUESTION: 247
組織的災難復原計畫 (DRP) 被記錄並保存在災難復原站點。下列哪一項是確保計劃在緊急情況下執行的最佳方法？
A. 將災難復原文件儲存在公有雲中。
B. 在另一個國家維護一個外包聯絡中心。
C. 要求所有關鍵決策者都儲存災難復原文件。
D. 提供適當的員工年度災難復原訓練。

Answer: (SHOW ANSWER)

= The best way to ensure that the disaster recovery plan (DRP) can be carried out in an emergency is to provide annual disaster recovery training to the appropriate staff, such as the disaster recovery team, the business process owners, and the IT staff. Disaster recovery training is a process of educating and preparing the staff for their roles, responsibilities, and actions in the event of a disaster that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. Disaster recovery training can help to ensure that the staff are aware, capable, and confident to execute the DRP, as well as to minimize the impact and damage to the business continuity, reputation, and value. Disaster recovery training can also help to evaluate the adequacy, accuracy, and applicability of the DRP, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the disaster recovery process. Disaster recovery training can also help to document and report the training details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the DRP and the training process. Storing disaster recovery documentation in a public cloud, maintaining an outsourced contact center in another country, and requiring disaster recovery documentation be stored with all key decision makers are all possible ways to ensure the availability and accessibility of the DRP in an emergency, but they are not the best ones. Storing disaster recovery documentation in a public cloud is a process of using a third-party service provider to store and manage the DRP documents online, which can offer benefits such as scalability, flexibility, and cost-efficiency, but also risks such as data breach, data loss, or service disruption. Maintaining an outsourced contact center in another country is a process of using a third-party service provider to handle the communication and coordination of the disaster recovery process with the internal and external stakeholders, such as the customers, partners, or regulators, which can offer benefits such as redundancy, reliability, and expertise, but also risks such as cultural, legal, or contractual issues. Requiring disaster recovery documentation be stored with all key decision makers is a process of ensuring that the senior management and the business process owners have a copy of the DRP documents, which can offer benefits such as accountability, authority, and visibility, but also risks such as inconsistency, duplication, or unauthorized access. References = CISM Review Manual 15th Edition, pages 233-2341; CISM Practice Quiz, question 1602

NEW QUESTION: 248

在業務連續性計畫 (BCP) 中定義復原策略時，下列哪一項是最重要的考量因素？

A. 法律和監管要求

B. 發生災難的可能性

C. 組織對服務中斷的容忍度

D. 備份站點的地理位置

Answer: (SHOW ANSWER)

= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to

service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. References = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 792 Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 249
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. 災難復原計畫 (DRP)
C. 業務影響分析 (BIA)
D. 事件回應計劃
Answer: (SHOW ANSWER)

NEW QUESTION: 250
下列哪一項是授予安全例外的主要原因？
A. 業務成本證明此風險是合理的。
B. 安全性的好處證明此風險是合理的。
C. 安全成本證明此風險是合理的。
D. 此風險的合理性取決於對企業的利益。
Answer: (SHOW ANSWER)
= A security exception is a formal authorization to deviate from a security policy, standard, or control, due to a valid business reason or requirement. The primary reason for granting a security exception is that the risk associated with the deviation is justified by the benefit to the business, such as increased efficiency, productivity, customer satisfaction, or competitive advantage. The security exception should be approved by the appropriate authority, such as the senior management or the risk committee, based on a risk assessment and a cost-benefit analysis. The security exception should also be documented, communicated, monitored, and reviewed periodically123. References =
* 1: CISM Review Manual 15th Edition, page 364
* 2: CISM Practice Quiz, question 1132
* 3: Security Policy Exception Management, section "Security Policy Exception Management Process"

NEW QUESTION: 251
下列哪一項最有助於確保組織災難復原計畫 (DRP) 的有效執行？
A. 該計劃由高階和 IT 營運管理層審核。

B. 該計劃基於行業最佳實踐。
C. 災難復原團隊記錄了流程步驟。
D. 製程在主要位置和故障轉移位置可用。
Answer: (SHOW ANSWER)
The best way to ensure the effective execution of a disaster recovery plan (DRP) is to make sure that the procedures are available at both the primary and the failover location, so that the staff can access them in case of a disaster. The procedures should be clear, concise, and updated regularly to reflect the current situation and requirements. Having the procedures available at both locations also helps to avoid confusion and delays in the recovery process.
References = CISM Review Manual, 16th Edition eBook1, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Recovery Plan Development, Page 373.

NEW QUESTION: 252
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: (SHOW ANSWER)
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: 253
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（SAR）
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: 254
下列哪一項最能描述緩衝區溢位？
A. 執行函數時使用的資料超出了函數可以處理的資料量
B. 程式包含隱藏的非預期功能，會帶來安全風險
C. 旨在幹擾正常操作的惡意程式碼
D. 一種捕獲資料的隱藏通道
Answer: (SHOW ANSWER)
A buffer overflow is a software coding error or vulnerability that occurs when a function is carried out with more data than the function can handle, resulting in adjacent memory locations being overwritten or corrupted by the excess data1. A program contains a hidden and unintended function that presents a security risk is not a buffer overflow, but rather a backdoor2. Malicious code designed to interfere with normal operations is not a buffer overflow, but rather malware3. A type of covert channel that captures data is not a buffer overflow, but rather a keylogger.
References: 1 https://www.fortinet.com/resources/cyberglossary/buffer- overflow 2 https://www.fortinet.com/resources/cyberglossary/backdoor 3 https://www.fortinet.com/resources/cyberglossary/malware https://www.fortinet.com/resources/cyberglossary/keylogger

NEW QUESTION: 255
反向口找可用於防止成功：
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: 256

組織的品質流程可以透過提供以下□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: 257
在拒□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□
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.

NEW QUESTION: 258
下列哪一項是資訊安全計畫中最重要的要素？
A. 根據全球相關性標準對計畫進行基準測試
B. 根據可用資源決定計劃可交付成果的優先級
C. 讓職能經理參與專案開發
D. 應用企業使用的專案管理實踐
Answer: (SHOW ANSWER)
Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units." CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

NEW QUESTION: 259
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: D (LEAVE A REPLY)
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: 260
為了了解組織的安全態勢，組織的高階領導最重要的是：

A. 評估最近事件回應測試的結果。
B. 口看報告的安全事件的數量。
C. 確保報告已建立的安全指標。
D. 評估風險緩解工作的進展。
Answer: (SHOW ANSWER)
According to the CISM Review Manual, an organization's security posture is the overall condition of its information security, which is determined by the effectiveness of its security program and the alignment of its security objectives with its business goals. To understand the security posture, the senior leadership needs to have a holistic view of the security risks and the actions taken to address them. Therefore, assessing the progress of risk mitigation efforts is the most important activity for the senior leadership, as it provides them with the information on how well the security program is performing and whether it is meeting the expected outcomes. Evaluating the results of the most recent incident response test, reviewing the number of reported security incidents, and ensuring established security metrics are reported are all useful activities for the senior leadership, but they are not sufficient to understand the security posture. They only provide partial or isolated information on the security performance, which may not reflect the overall security condition or the alignment with the business objectives. References = CISM Review Manual, 16th Edition, Chapter 1, Information Security Governance, pages 28-29.

NEW QUESTION: 261
我們正在為託管敏感資訊的伺服器製定事件回應計劃。一旦發生洩露，誰應該做出關閉系統的決定？
A. 營運經理
B. 事件回應團隊
C. 服務擁有者
D. 資訊安全經理
Answer: (SHOW ANSWER)

NEW QUESTION: 262
將資訊安全活動整合到變更管理流程中的主要好處是：
A. 為業務中與安全相關的變更提供更大的責任。
B. 保護組織免受未經授權的變更。
C. 確保所需的控制權包含在變更中。
D. 保護企業免受勾結和合規威脅。
Answer: (SHOW ANSWER)

NEW QUESTION: 263
一個組織即將實施基於雲端的應用程式。已收到的獨立滲透測試結果顯示有高評級漏洞。以下哪一項是最好的繼續方式？
A. 實施應用程式並請求雲端服務提供者修復漏洞。

B. 評估漏洞是否在組織的風險承受範圍口。
C. 委託進一步的滲透測試來驗證初步測試結果,
D. 延遲實施，直到漏洞得到修復。
Answer: (SHOW ANSWER)
The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.
Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.
Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information.
The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project.
Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk-averse approach, as it may hinder the organization's innovation and competitiveness. References =
* ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.
* ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID
1025.

NEW QUESTION: 264
在營運中使用公司自有行動裝置的組織中，下列何者是資安經理的主要職責？
A. 需要裝置的遠端擦除功能。
B. 進行安全意識訓練。
C. 檢視並更新現有安全性策略。
D. 在裝置上強制執行密碼和資料加密。
Answer: (SHOW ANSWER)
The primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations is to review and update existing security policies. Security policies are the foundation of an organi-zation's security program, as they define the goals, objectives, principles, roles, respon-sibilities, and requirements for protecting information and systems. Security policies should be reviewed and updated regularly to reflect changes in the organization's envi-ronment, needs, risks, and technologies1. Implementing the use of company-owned mobile devices in its operations is a significant change that may introduce new threats and vulnerabilities, as well as new opportunities and benefits, for the organiza-tion. Therefore, the information security manager should review and update existing security policies to address the following aspects2:
*The scope, purpose, and ownership of company-owned mobile devices
*The acceptable and unacceptable use of company-owned mobile devices
*The security standards and best practices for company-owned mobile devices
*The roles and responsibilities of users, managers, IT staff, and vendors regarding compa-ny-owned mobile devices
*The procedures for provisioning, managing, monitoring, and decommissioning company-owned mobile devices
*The incident response and reporting process for company-owned mobile devices By reviewing and updating existing security policies, the information security manager can ensure that the organization's security program is aligned with its business objec-tives and risk appetite, as well as compliant with applicable laws and regulations. The other options are not the primary responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations. They are possible actions or controls that may be derived from or support-ed by the updated security policies. Requiring remote wipe capabilities for devices is a technical control that can help prevent data loss or theft in case of device loss or com-promise3. Conducting security awareness training is an administrative control that can help educate users about the security risks and responsibilities associated with using company-owned mobile devices. Enforcing passwords and data encryption on the de-vices is a technical control that can help protect data confidentiality and integrity on company-owned mobile devices. References:
1: Information Security Policy - NIST 2: Mobile Device Security Policy - SANS 3: Remote Wipe: What It Is
& How It Works - Lifewire : Security Awareness Training - NIST : Mobile Device Encryption - NIST

NEW QUESTION: 265
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: 266
下列哪一項是組織選擇關鍵風險指標 (KRI) 時最重要的因素？
A. 投資報酬率 (ROI)
B. 合規性要求
C. 目標受眾
D. 資訊的重要性
Answer: (SHOW ANSWER)
A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us /CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 267
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: 268
在製定事件升級流程時，最好的方法是根據以下因素對事件進行分類：
A. 預計恢復時間。
B. 受影響的資訊資口。
C. 復原點目標 (RPO)。
D. 其根本原因。
Answer: (SHOW ANSWER)
The best approach to developing an incident escalation process is to classify incidents based on the information assets affected, because this will help to determine the impact and severity of the incidents, as well as the appropriate response and recovery actions. The information assets affected by an incident can indicate the potential loss of confidentiality, integrity, or availability of the information, as well as the legal, regulatory, contractual, or reputational implications. By classifying incidents based on the information assets affected, the organization can prioritize the incidents and escalate them to the relevant stakeholders and authorities.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

NEW QUESTION: 269
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: 270
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: 271
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. 它幫助組織滿足合規性要求。
B. 它有助於加快資訊安全預算的批准。
C. 組織中的每個人都對資訊安全負責。
D. 安全事件對整個組織口生不利影響。
Answer: (SHOW ANSWER)

NEW QUESTION: 272
當組織缺乏口部專業知識來進行高技術取證調口時，確保資訊安全事件發生後有效和及時調口的最佳方法是什麼？
A. 提供資訊安全團隊取證訓練。
B. 確保事件回應政策允許僱用取證公司。
C. 購買取證標準作業程序。
D. 在發生事件之前聯絡取證公司。
Answer: (SHOW ANSWER)

NEW QUESTION: 273
在審口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: 274
下列哪一項是針對透過社會工程未經授權存取公司網路的最佳技術防禦？
A. 需要質詢/回應訊息
B. 需要多重身份驗證
C. 強制頻繁更改密碼
D. 強制執行複雜的密碼格式
Answer: (SHOW ANSWER)
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

NEW QUESTION: 275
下列哪一項是降低實施應用程式安全控製成本的最佳選擇？
A. 在開發環境中進行安全測試。
B. 將安全活動整合到開發流程中
C. 專案完成後執行風險分析。
D. 包含標準應用程式安全要求
Answer: (SHOW ANSWER)
Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios. Performing a risk analysis after project completion is not a good option because it may be too late to identify or mitigate security risks that may have been

introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software- development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems

NEW QUESTION: 276
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: 277
下列哪一項是確定資訊安全設定檔是否符合業務需求的最佳方法？
A. 口看關鍵績效指標 (KPI) 儀表板
B. 檢視與安全相關的關鍵風險指標 (KRI)
C. 審核控制自我評估 (CSA) 結果
D. 審口定期安全審核
Answer: (SHOW ANSWER)
Security-related KRIs are metrics that measure the effectiveness of the information security profile in achieving the business objectives and managing the risks. Reviewing security-related KRIs can help to determine if the information security profile is aligned with business requirements, as they reflect the security performance and outcomes that are relevant for the business. Reviewing other options, such as KPIs, CSAs, or audits, may provide some insights into the security status, but they are not the best way to assess the alignment with business requirements, as they may not capture the business context and goals adequately.

References:
* https://www.nist.gov/cyberframework/examples-framework-profiles
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/accountability-for-information- security-roles-and-responsibilities-part-1
* https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea- top-down-approach

NEW QUESTION: 278
在雲端技術環境中，下列哪一項會為安全事件調口帶來最大的挑戰？
A. 存取硬體
B. 資料加密
C. 非標準事件日誌
D. 壓縮的客口數據
Answer: (SHOW ANSWER)

NEW QUESTION: 279
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: (SHOW ANSWER)
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: 280
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. 保留證據的完整性。

B. 該事件已報告給高階管理層。
C. 伺服器已斷電。
D. 取證調口軟體已載入到伺服器上。
Answer: (SHOW ANSWER)

NEW QUESTION: 281
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: 282
在決定資口估口時，下列哪一項是最重要的考量因素？
A. 資口回收成本
B. 資口分類級別
C. 保險費成本
D. 潛在的業務損失
Answer: (SHOW ANSWER)
Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important as potential business loss, as they do not capture the full value of the asset to the organization. References = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

NEW QUESTION: 283
下列哪一項是幫助員工了解其資訊安全責任最有效的方法？
A. 傳達針對違反政策的紀律流程。
B. 要求員工參加資訊安全意識培訓。
C. 請員工簽署保密協議。
D. 在職位口明中包含資訊安全職責。
Answer: (SHOW ANSWER)
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION: 284
資訊安全經理發現第三方提供者不遵守工作口明書 (SOW)。下列哪一項是最佳行動方案？
A. 將此問題通知高階管理層。
B. 向法務人員回報問題。
C. 口動合約重新協商。
D. 評估問題的嚴重程度。
Answer: D (LEAVE A REPLY)
The first course of action when the information security manager becomes aware that a third-party provider is not in compliance with the SOW is to assess the extent of the issue, which means determining the nature, scope, and impact of the non-compliance on the security of the enterprise's data and systems. The assessment should also identify the root cause of the non-compliance and the possible remediation actions. The assessment will help the information security manager to decide the next steps, such as notifying senior management, reporting the issue to legal personnel, initiating contract renegotiation, or terminating the contract.
References = Ensuring Vendor Compliance and Third-Party Risk Mitigation, A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

NEW QUESTION: 285
下列哪一項是資訊安全經理提高組織資訊安全計畫有效性的最佳方法？
A. 著重在解決安全與效能之間的衝突。
B. 與業務和 IT 職能部門合作確定控制措施。
C. 在變更控制流程中包含資訊安全要求。
D. 獲得 IT 部門的協助以實施自動化安全通道。
Answer: (SHOW ANSWER)
The best way for an information security manager to improve the effectiveness of an organization's information security program is to collaborate with business and IT functions in determining controls.
Collaboration is a key factor for ensuring that the information security program is aligned with the organization's business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program.
Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions.
Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance, and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.
Including information security requirements in the change control process is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.

Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Strategy Development, Subsection: Collaboration, page 24-251

NEW QUESTION: 286
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口的主要原因是：
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: 287

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: 288

下列哪一項指標最能證明新實施的資訊安全框架的成功？

A. 已識別的安全事件數量增加

B. 安全策略異常數量減少

C. 安全審核結果數量減少

D. 合規業務流程數量增加

Answer: (SHOW ANSWER)

NEW QUESTION: 289

下列哪一項提供了確定 IT 系統所需保護等級的最佳輸入？

A. 資口分類

B. 漏洞評估

C. 威脅分析

D. 口部稽核結果

Answer: (SHOW ANSWER)

NEW QUESTION: 290

當出現以下情況時，滲透測試是最合適的：

A. 新系統即將上線。

B. 新系統正在設計中。

C. 正在製定安全性策略。

D. 發生安全事件，

Answer: (SHOW ANSWER)

= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process. Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

NEW QUESTION: 291

下列哪項最佳措施能使資訊安全經理向高階管理層展示資訊安全和風險計畫的有效性？

A. 更新的風險評估

B. 審計報告

C. 每月指標

D. 資訊安全事件數量

Answer: (SHOW ANSWER)

NEW QUESTION: 292

下列何者最能決定組織的資料保留策略和後續政策？

A. 業務需求
B. 業務影響分析 (BIA)
C. 供應商要求
D. 風險偏好
Answer: (SHOW ANSWER)

NEW QUESTION: 293
下列哪一項是組織中分配風險負責人的主要原因？
A. 修復殘餘風險
B. 定義職責
C. 確保問責制
D. 辨識新出現的風險
Answer: (SHOW ANSWER)
The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.
References: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

NEW QUESTION: 294
在組織的軟體即服務 (SaaS) 供應商發生違規行為後，資訊安全經理向高階管理層提出的最佳建議是下列哪一項？
A. 聘請法律顧問。
B. 重新協商供應商合約。
C. 終止與供應商的關係。
D. 更新供應商風險評估。
Answer: (SHOW ANSWER)

NEW QUESTION: 295
下列哪一項應該是資訊安全治理框架的主要目標？
A. 提供最佳化組織安全性設定檔的基準。
B. 顯示高階管理層的承諾。
C. 向外部利害關係人展示遵守□業最佳實務。
D. 確保使用者遵守組織的資訊安全策略。
Answer: (SHOW ANSWER)
According to the Certified Information Security Manager (CISM) Study Manual, "The primary objective of information security governance is to provide a framework for managing and controlling information security practices and technologies at an enterprise level. Its goal is to manage and reduce risk through a process of identification, assessment, and management of those risks." While demonstrating senior management commitment, compliance with industry best practices, and ensuring user compliance with policies are all important aspects of information security governance, they are not the primary objective. The primary objective is to manage and reduce risk by establishing a framework for managing and controlling information security practices and technologies at an enterprise level.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 60.

NEW QUESTION: 296
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. 繼續調□。
C. □動升級流程。
D. 聯絡危機管理團隊。
Answer: (SHOW ANSWER)

NEW QUESTION: 297
基於異常的入侵偵測系統 (IDS) 透過收集以下資料來運作：
A. 正常網路行為並將其用作測量異常活動的基線
B. 異常網路行為並向防火牆發出指令以丟棄惡意連接
C. 異常網路行為並將其用作測量正常活動的基線
D. 來自歷史資料的攻擊模式簽名
Answer: (SHOW ANSWER)
An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern

signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

NEW QUESTION: 298
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: 299
下列哪一項是測試關鍵基礎設施□的安全控制的主要目標？
A. 辨識並解決安全團隊績效問題
B. 降低導致生□失敗的安全部署百分比
C. 減少控制評估次數以最佳化資源
D. 確保 IT 服務的持續彈性與安全性
Answer: (SHOW ANSWER)

NEW QUESTION: 300
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.

NEW QUESTION: 301
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: 302
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: 303
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: 304
下列何者最有助於確保及時制定和執行風險應對計畫？
A. 建立風險指標
B. 風險管理程序培訓
C. 報告已記錄的缺陷
D. 分配風險負責人
Answer: (SHOW ANSWER)
Assigning a risk owner is the best way to ensure a risk response plan will be developed and executed in a timely manner, because a risk owner is responsible for monitoring, controlling, and reporting on the risk, as well as implementing the appropriate risk response actions. A risk owner should have the authority, accountability, and resources to manage the risk effectively. Establishing risk metrics, training on risk management procedures, and reporting on documented deficiencies are all important aspects of risk management, but they do not guarantee that a risk response plan will be executed promptly and properly. Risk metrics help to measure and communicate the risk level and performance, but they do not assign any responsibility or action. Training on risk management procedures helps to increase the awareness and competence of the staff involved in risk management, but it does not ensure that they will follow the procedures or have the authority to do so. Reporting on documented deficiencies helps to identify and communicate the gaps and weaknesses in the risk management process, but it does not provide any solutions or corrective actions. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 125-126, 136-
137.

NEW QUESTION: 305
制定災難復原計畫 (DRP) 後應執行下列哪些任務？
A. 制定測試計劃。
B. 分析業務影響。
C. 定義回應團隊角色。
D. 確定復原時間目標 (RTO)。

Answer: (SHOW ANSWER)
= Developing the test plan is the task that should be performed once a disaster recovery plan (DRP) has been developed. The test plan is a document that describes the objectives, scope, methods, and procedures for testing the DRP. The test plan should also define the roles and responsibilities of the test team, the test scenarios and criteria, the test schedule and resources, and the test reporting and evaluation. The purpose of testing the DRP is to verify its effectiveness, identify any gaps or weaknesses, and improve its reliability and usability. Testing the DRP also helps to increase the awareness and readiness of the staff and stakeholders involved in the disaster recovery process. Analyzing the business impact, defining response team roles, and identifying recovery time objectives (RTOs) are all tasks that should be performed before developing the DRP, not after. These tasks are part of the business continuity planning (BCP) process, which aims to identify the critical business functions and assets, assess the potential threats and impacts, and determine the recovery strategies and requirements. The DRP is a subset of the BCP that focuses on restoring the IT systems and services after a disaster. Therefore, the DRP should be based on the results of the BCP process, and tested after it has been developed. References = CISM Review Manual 2023, page 218 1; CISM Practice Quiz 2

NEW QUESTION: 306
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."

NEW QUESTION: 307
由於事件分類中缺乏嚴重性標準，下列哪一項是最令人擔憂的問題？

A. 統計報告將不正確。
B. 服務台的人員配置不正確。
C. 升級程式將無效。
D. 無法及時偵測到攻擊。
Answer: C (LEAVE A REPLY)
The greatest concern resulting from the lack of severity criteria in incident classification is that escalation procedures will be ineffective because they rely on severity criteria to determine when and how to escalate an incident to higher levels of authority or responsibility, and what actions or resources are required for resolving an incident. Statistical reports will be incorrect is not a great concern because they do not affect the incident response process directly, but rather provide information or analysis for improvement or evaluation purposes.
The service desk will be staffed incorrectly is not a great concern because it does not affect the incident response process directly, but rather affects the availability or efficiency of one of its components. Timely detection of attacks will be impossible is not a great concern because it does not depend on severity criteria, but rather on monitoring and alerting mechanisms. 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: 308
下列何者最能支持資訊安全計畫的投資？
A. 商業案例
B. 風險評估結果
C. 業務影響分析 (BIA)
D. 差距分析結果
Answer: (SHOW ANSWER)

NEW QUESTION: 309
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: 310
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

NEW QUESTION: 311
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: 312
下列哪一項是資訊安全經理應限制在多用口環境中使用通用管理員帳口的主要原因？
A. 確保系統審核追蹤不會繞過
B. 防止問責問題
C. 確保維持職責分離
D. 防止未經授權的使用者存取
Answer: (SHOW ANSWER)

NEW QUESTION: 313
資訊安全經理應先執行下列哪項操作來解決與不滿足組織安全要求的新第三方雲端應用程式相關的風險？

A. 在合約中包含安全要求。
B. 更新風險登記冊。
C. 與企業主協商。
D. 暫時限制應用程式網路存取。
Answer: (SHOW ANSWER)
Consulting with the business owner is the FIRST course of action that the information security manager should take to address the risk associated with a new third-party cloud application that will not meet organizational security requirements, because it helps to understand the business needs and expectations for using the application, and to communicate the security risks and implications. The information security manager and the business owner should work together to evaluate the trade-offs between the benefits and the risks of the application, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 41: "The information security manager should consult with the business owners to understand their needs and expectations for using third-party services, and to communicate the security risks and implications." CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "The information security manager and the business owners should collaborate to evaluate the trade-offs between the benefits and the risks of using third- party services, and to determine the best course of action, such as modifying the requirements, finding an alternative solution, or accepting the risk." Best Practices to Manage Risks in the Cloud - ISACA: "The information security manager should work with the business owner to define the security requirements for the cloud service, such as data protection, access control, incident response, and compliance."

NEW QUESTION: 314
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: 315
下列哪一項是在事件回應計畫的準備階段建立的？
A. 平均反應時間（MTTR）
B. 復原時間目標（RTO）
C. 利害關係人溝通計劃
D. 監管鏈程序
Answer: (SHOW ANSWER)

NEW QUESTION: 316
一位資安經理了解到，使用網路釣魚電子郵件冒充組織執行長來實施電匯詐欺的攻擊趨勢呈上升趨勢。下列哪一項是降低與此類攻擊相關的風險的最佳方法？
A. 為負責電匯的員工提供意識訓練。
B. 為執行長提供針對此類網路釣魚攻擊的意識培訓。
C. 停用負責電匯的員工的電子郵件。
D. 暫時暫停組織的電匯。
Answer: (SHOW ANSWER)

NEW QUESTION: 317
發生重大資安事件後，下列何者最能幫助資安經理確定糾正措施？

A. 計算事件成本
B. 進行事後評估
C. 執行影響分析
D. 保留證據
Answer: (SHOW ANSWER)
The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future. References = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

NEW QUESTION: 318
下列哪一項是在與第三方進行合約談判期間解決組織安全問題的最有效方法？
A. 與第三方供應商溝通安全策略。
B. 審口與組織法律部門的第三方合約。
C. 對第三方供應商進行資訊安全審核。
D. 確保採購過程涉及安全。
Answer: (SHOW ANSWER)

NEW QUESTION: 319
資訊安全漏洞發生後，下列何者最難衡量？
A. 聲譽損害
B. 人力資源成本
C. 監理制裁
D. 替換工作
Answer: (SHOW ANSWER)
Reputational damage is often intangible, subjective, and hard to quantify, making it the most challenging aspect to measure.
"Reputation impact is difficult to quantify and may have long-term effects that are not immediately apparent."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis* ISACA practice questions highlight that reputational damage is uniquely challenging to measure accurately.

NEW QUESTION: 320
當業務案例提供以下證據時，資訊安全經理最有可能獲得新安全專案的批准：
A. 組織協調

B. IT 策略調整
C. 對組織的威脅
D. 現有控製成本
Answer: (SHOW ANSWER)
A new security project is more likely to be approved if it aligns with the organization's goals, objectives, and strategies. This shows that the project supports the business needs and adds value to the organization. Organizational alignment is one of the key elements of a business case for information security, as stated in the CISM Review Manual, 16th Edition1, page 41. IT strategy alignment, threats to the organization, and existing control costs are also important factors to consider, but they are not as persuasive as organizational alignment in obtaining approval for a new security project. References = 1: CISM Review Manual, 16th Edition by Isaca (Author) Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 321
下列何者最能將資訊安全治理納入公司治理？
A. 完善的資訊安全政策與標準
B. 具有業務代表的資訊安全指導委員會
C. 整個組織中明確的權力界限
D. 高階管理層批准資訊安全策略
Answer: (SHOW ANSWER)
= The best way to enable the integration of information security governance into corporate governance is to establish an information security steering committee with business representation. An information security steering committee is a group of senior executives and managers from different business units and functions who are responsible for overseeing, directing, and supporting the information security program and strategy of the organization. An information security steering committee with business representation can enable the integration of information security governance into corporate governance by providing the following benefits12:
Align the information security objectives and priorities with the business objectives and priorities, and ensure that the information security program and strategy support and enable the achievement of the organizational goals and performance.
Communicate and promote the value and importance of information security to the board of directors, senior management, and other stakeholders, and ensure that information security is considered and incorporated in the decision making and planning processes of the organization.
Provide guidance and direction to the information security manager and the information security team, and ensure that they have the necessary authority, resources, and support to implement and maintain the information security program and strategy effectively and efficiently.
Monitor and evaluate the performance and outcomes of the information security program and strategy, and ensure that they are aligned with the expectations and requirements of the organization and its stakeholders, as well as the relevant laws, regulations, standards, and best practices.

Identify and address the issues, challenges, and opportunities related to information security, and ensure that the information security program and strategy are continuously improved and updated to reflect the changes and developments in the internal and external environment.
The other options are not the best way to enable the integration of information security governance into corporate governance, as they are less comprehensive, effective, or influential than establishing an information security steering committee with business representation. Well-documented information security policies and standards are important components of the information security program and strategy, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not reflect or align with the business needs, priorities, or expectations, and they may not be communicated, implemented, or enforced properly or consistently across the organization. Clear lines of authority across the organization are important factors for the information security governance structure, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not ensure the involvement, participation, or support of the senior executives, managers, and other stakeholders who are responsible for or affected by information security. Senior management approval of the information security strategy is an important outcome of the information security governance process, but it is not sufficient to enable the integration of information security governance into corporate governance, as it may not ensure the alignment, communication, or monitoring of the information security strategy with the business strategy, and it may not ensure the accountability, responsibility, or authority of the information security manager and the information security team12. References = CISM Domain 1: Information Security Governance (ISG) [2022 update], Information Security Governance for CISM | Pluralsight, Aligning Information Security with Business Strategy - ISACA, Aligning Information Security with Business Objectives - ISACA

NEW QUESTION: 322
在為組織制定資訊安全策略時，下列哪一項應該是最重要的考量因素？
A. 職位描述包括口讀安全策略的要求。
B. 政策每年更新一次。
C. 高階管理層支持這些政策。
D. 這些政策與行業最佳實踐保持一致。
Answer: (SHOW ANSWER)
The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization's leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization's goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.

Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing information security policies. The policies should be relevant and applicable to the employees' roles and functions, and should be reinforced by regular training and awareness programs.
The policies should be updated periodically to reflect the changes in the organization's environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.
The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization's specific context, needs, and expectations, and should be consistent with the organization's vision, mission, and values.
References =
* ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.
* ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID
1009.

NEW QUESTION: 323
下列何者最能確保資訊安全治理與公司治理一致？
A. 包括 IT 代表在口的安全指導委員會
B. 一致的風險管理方法
C. 資訊安全風險登記冊
D. 將安全報告整合到公司報告中
Answer: (SHOW ANSWER)
The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with corporate governance by themselves. References = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

NEW QUESTION: 324
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□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□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: 325
事件回應團隊已確定應用程式已被破壞。接下來應該執行下列哪項操作？
A. 將受影響的系統維持在取證可接受的狀態

B. 對受影響的應用程式進行風險評估
C. 將違規情況通知高階管理層。
D. 將受影響的系統與網路的其餘部分隔離
Answer: (SHOW ANSWER)
The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems. References:
https://www.crowdstrike.com/cybersecurity-101/incident-response/
https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks
https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security/

NEW QUESTION: 326
下列哪一項可以為解決潛在系統漏洞的技術解決方案的商業案例提供最佳輸入？
A. 風險評估
B. 業務影響分析 (BIA)
C. 滲透測試結果
D. 漏洞掃描結果
Answer: (SHOW ANSWER)
Risk assessment is the BEST input to a business case for a technical solution to address potential system vulnerabilities, because it helps to identify and prioritize the most critical risks that the solution should mitigate or reduce. Risk assessment also helps to evaluate the costs and benefits of the solution in terms of reducing the likelihood and impact of potential threats and incidents.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 47: "Risk assessment is the process of identifying and analyzing information security risks and determining their potential impact on the enterprise's business objectives." CISM Review Manual, 16th Edition, ISACA, 2020, p. 48: "Risk assessment provides input to the business case for information security investments by identifying and prioritizing the most critical risks that need to be addressed and evaluating the costs and benefits of the proposed solutions."

NEW QUESTION: 327
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: (SHOW ANSWER)
Comprehensive and Detailed Explanation: 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: 328
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: 329
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: 330
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: 331
下列哪一個角色最能影響組織口的安全文化？
A. 首席資訊安全長 (CISO)
B. 資訊長 (CIO)
C. 執行長（CEO）
D. 營運長 (COO)
Answer: (SHOW ANSWER)
The CEO is the best able to influence the security culture within an organization because the CEO sets the tone and direction for the organization and has the authority and responsibility to ensure that the organization' s objectives are aligned with its strategy. The CEO can also communicate the importance and value of information security to all stakeholders and foster a culture of security awareness and accountability. The CISO, CIO and COO are important roles in information security management, but they do not have the same level of influence and authority as the CEO. References = CISM Review Manual, 16th Edition, page 221; CISM Exam Content Outline, Domain 1, Task 12 The Chief Information Security Officer (CISO) is responsible for

leading and coordinating an organization's information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to information security, the CISO can help to create a security- aware culture within the organization.

NEW QUESTION: 332
資料分類主要由以下人員負責：
A. 安全管理員。
B. 資料擁有者。
C. 資料保管人。
D. 高階管理層。
Answer: (SHOW ANSWER)

NEW QUESTION: 333
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: 334
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: 335
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: 336
下列哪一項是在商業影響分析 (BIA) 流程中進行訪談的最重要原因？
A. 促進 BIA 後的定性風險評估
B. 提高主要利害關係人對資訊安全的意識
C. 確保提供意見的利害關係人承擔相關風險
D. 取得盡可能多的相關利害關係人的意見
Answer: (SHOW ANSWER)
The most important reason to conduct interviews as part of the business impact analysis (BIA) process is to obtain input from as many relevant stakeholders as possible. A BIA is a process of identifying and analyzing the potential effects of disruptive events on the organization's critical

business functions, processes, and resources. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's continuity planning. Interviews are one of the methods to collect data and information for the BIA, and they involve direct and interactive communication with the stakeholders who are involved in or affected by the business functions, processes, and resources. By conducting interviews, the information security manager can obtain input from as many relevant stakeholders as possible, such as business owners, managers, users, customers, suppliers, regulators, and partners. This can help to ensure that the BIA covers the full scope and complexity of the organization's business activities, and that the BIA reflects the accurate, current, and comprehensive views and expectations of the stakeholders. Interviews can also help to validate, clarify, and supplement the data and information obtained from other sources, such as surveys, questionnaires, documents, or systems. Interviews can also help to build rapport, trust, and collaboration among the stakeholders, and to increase their awareness, involvement, and commitment to the information security and continuity planning.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Impact Analysis (BIA), pages 178-1801; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 65, page 602.

NEW QUESTION: 337
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: 338
下列哪一項應包含設備和軟體供應商代表的聯絡資訊？
A. 資訊安全計畫章程
B. 業務影響分析 (BIA)
C. 服務等級協定 (SLA)
D. 業務連續性計劃 (BCP)
Answer: D (LEAVE A REPLY)
The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery.
Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. References:
https://www.isaca.org
/resources/isaca-journal/issues/2017/volume-2/business-continuity-management-lifecycle
https://www.isaca.
org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

NEW QUESTION: 339
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: 340
在網路監控中引入單點管理的主要好處是：
A. 減少對系統的未經授權的存取。
B. 提高環境控制效率。
C. 防止分散式環境中資訊不一致。
D. 允許管理人員做出管理決策。
Answer: (SHOW ANSWER)
A single point of administration in network monitoring is a centralized system that allows network administrators to manage and monitor the entire network from one location. A single point of administration can provide several benefits, such as:
* Promoting efficiency in control of the environment: A single point of administration can simplify and streamline the network management tasks, such as configuration, troubleshooting, performance optimization, security updates, backup and recovery, etc. It can also reduce the time and cost of network maintenance and administration, as well as improve the consistency and quality of network services.
* Reducing unauthorized access to systems: A single point of administration can enhance the network security by implementing centralized authentication, authorization and auditing mechanisms. It can also enforce consistent security policies and standards across the network, and detect and respond to any unauthorized or malicious activities.
* Preventing inconsistencies in information in the distributed environment: A single point of administration can ensure the data integrity and availability by synchronizing and replicating the data across the network nodes. It can also provide a unified view of the network status and performance, and facilitate the analysis and reporting of network data.
* Allowing administrative staff to make management decisions: A single point of administration can support the decision-making process by providing relevant and timely information and feedback to the network administrators. It can also enable the administrators to implement changes and improvements to the network based on the business needs and objectives.
Therefore, the primary benefit of introducing a single point of administration in network monitoring is that it promotes efficiency in control of the environment, as it simplifies and streamlines the network management tasks and improves the network performance and quality. References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section
4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 205.

NEW QUESTION: 341
下列哪一項是供應商風險管理流程成熟度的最佳指標？
A. 完成供應商風險管理流程所需的平均時間
B. 已完成供應商入職流程的供應商百分比
C. 依既定標準定期進行審核的供應商百分比
D. 因安全審核結果而被拒口的供應商數量
Answer: (SHOW ANSWER)
The percentage of vendors that are regularly reviewed against defined criteria is the best indicator of the maturity level of a vendor risk management process, as it reflects the extent to which the organization has established and implemented a consistent, repeatable, and effective process to monitor and evaluate the security performance and compliance of its vendors. A high percentage indicates a mature process that covers all vendors and applies clear and relevant criteria based on the organization's risk appetite and objectives. A low percentage indicates a less mature process that may be ad hoc, incomplete, or outdated. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 342
下列哪一項最能幫助組織辨識和遏止安全事件？
A. 風險評估
B. 威脅建模
C. 持續監控
D. 桌上練習
Answer: (SHOW ANSWER)
= Continuous monitoring is the process of collecting, analyzing, and reporting on the security status of an organization's information systems and networks. Continuous monitoring enables an organization to identify and contain security incidents by providing timely and accurate information on the security events, alerts, incidents, and threats that may affect the organization. Continuous monitoring also helps to measure the effectiveness and compliance of the security controls, policies, and procedures that are implemented to protect the organization's information assets. Continuous monitoring can be performed using various tools and methods, such as security information and event management (SIEM) tools, intrusion detection and prevention systems (IDS/IPS), vulnerability scanners, log analyzers, and audit trails.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.2: Continuous Monitoring2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 3

NEW QUESTION: 343
組織越來越多地使用軟體即服務 (SaaS) 來取代 IT 應用程式的口部託管和支援。下列哪一項是幫助確保採購決策考慮資訊安全問題的最有效方法？
A. 將資訊安全風險評估納入採購流程。

B. 為採購團隊提供定期資訊安全訓練。
C. 邀請 IT 成員參加定期採購團隊會議以影響最佳實務。
D. 在與 SaaS 供應商的採購合約中強制執行審核權。
Answer: (SHOW ANSWER)
The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization.
Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.
Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.
Inviting IT members into regular procurement team meetings to influence best practice is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.
Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts.
References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection:
Procurement and Vendor Management, Page 141-1421

NEW QUESTION: 344
下列何者最能決定安全事件回應期間的資源分配？
A. 高階管理層承諾
B. 業務連續性計劃 (BCP)
C. 已建立的升級流程
D. 定義的嚴重級別
Answer: (SHOW ANSWER)

= The allocation of resources during a security incident response depends on the defined levels of severity, which indicate the potential impact and urgency of the incident. The levels of severity help prioritize the response activities and assign the appropriate roles and responsibilities. Senior management commitment, a business continuity plan (BCP), and an established escalation process are important factors for an effective incident response, but they do not directly determine the allocation of resources. References = CISM Review Manual, 16th Edition, page 3011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1462 Learn more:
1. isaca.org2. amazon.com3. gov.uk
Defined levels of severity is the best determinant of the allocation of resources during a security incident response. Having defined levels of severity allows organizations to plan for and allocate resources for each level of incident, depending on the severity of the incident. This ensures that the right resources are allocated in a timely manner and that incidents are addressed appropriately.

NEW QUESTION: 345
在發現和根除惡意軟體攻擊後，確定下列哪一項最重要？
A. 偵測惡意軟體的方法
B. 惡意軟體進入路徑
C. 涉及的惡意軟體類型
D. 惡意軟體的創建者
Answer: (SHOW ANSWER)

NEW QUESTION: 346
下列哪一項應該是獲得外包批准以解決安全漏洞的第一步？
A. 收集其他指標。
B. 執行成本效益分析。
C. 向高階管理層提交資金請求。
D. 開始對外包公司進行盡職調口。
Answer: (SHOW ANSWER)
The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:
* Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements
* Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities

* Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics
* Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process
* Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

NEW QUESTION: 347
下列何者是使用分階段事件復原方法的主要原因？
A. 確保關鍵系統先恢復
B. 決定補救步驟的優先級
C. 給回應團隊時間來分析事件
D. 獲得管理階層的支持
Answer: (SHOW ANSWER)

NEW QUESTION: 348
為了幫助確保資訊安全培訓計劃最有效，其口容應該是
A. 專注於資訊安全政策。
B. 與業務流程保持一致
C. 基於員工角色
D. 基於最近發生的事件
Answer: (SHOW ANSWER)

"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

NEW QUESTION: 349
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. 高階管理層
B. 資訊安全經理
C. 資訊擁有者
D. 業務經理
Answer: (SHOW ANSWER)

NEW QUESTION: 350
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: 351
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. 在供應商合約中包含不合規的罰款條款
B. 監控關鍵風險指標 (KRI)
C. 停用供應商存取並僅在需要存取時重新□用
D. 實現系統與資料之間的職責分離
Answer: B (LEAVE A REPLY)

NEW QUESTION: 352
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

NEW QUESTION: 353
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: 354
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: 355
下列哪一項對於獲得高階管理層對網路基礎設施安全投資的批准最有效？
A. 針對網路執行滲透測試以展示業務漏洞
B. 突顯競爭對手在網路最佳安全實務上的表現
C. 證明有針對性的安全控制與業務目標相關
D. 提供多個供應商的可比較安全實施評估
Answer: (SHOW ANSWER)
The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives. Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.

According to the Certified Information Security Manager (CISM) Study Manual, "To gain senior management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization." While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 305.

NEW QUESTION: 356
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. 完全中斷測試
C. 結構化演練
D. 平行測試
Answer: (SHOW ANSWER)

NEW QUESTION: 357
組織希望將資訊安全整合到其人力資源管理流程中。下列哪一項應該是第一步？
A. 使用最佳實踐對流程進行基準測試，以找出差距
B. 計算投資報酬率 (ROI)。
C. 提供 HR 安全意識訓練。
D. 評估流程的業務目標。
Answer: (SHOW ANSWER)
The first step when integrating information security into HR management processes is to assess the business objectives of the processes, which means understanding the purpose, scope, and expected outcomes of the HR functions and activities, and how they relate to the organization's strategy and goals. The assessment will help to identify the information security requirements, risks, and controls that are relevant and applicable to the HR processes, and to align the information security objectives with the business objectives.
References = CISM Review Manual 15th Edition, CISM: Overview of domains [updated 2022]

NEW QUESTION: 358
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: 359

為了確保新應用程式符合資訊安全策略，最好的方法是：

A. 在實施之前檢口應用程式的安全性。

B. 在開發階段整合功能。

C. 執行漏洞分析。

D. 定期審核應用程式的安全性。

Answer: (SHOW ANSWER)

Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure- software-development-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4 /integrating-assurance-functions

NEW QUESTION: 360

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. 應用程式伺服器

B. 郵件中繼伺服器

C. 資料庫伺服器

D. 代理伺服器

Answer: (SHOW ANSWER)

NEW QUESTION: 361
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: 362
下列哪一項最能實現有效的資訊資口分類流程？
A. 在分類過程中包含安全要求
B. 分析稽核結果
C. 檢口資口的復原時間目標 (RTO) 要求
D. 分配所有權
Answer: (SHOW ANSWER)
Assigning ownership is the best way to enable an effective information asset classification process, as it establishes the authority and responsibility for the information asset and its protection. The owner of the information asset should be involved in the classification process, as they have the best knowledge of the value, sensitivity, and criticality of the asset, as well as the impact of its loss or compromise. The owner should also ensure that the asset is properly labeled, handled, and secured according to its classification level.
(From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Information Asset and Security Classification Procedure1, section 3.1.

NEW QUESTION: 363
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: 364
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: 365
資訊安全經理已確定特權員工對生口伺服器的存取請求已獲得批准；但不會記錄使用者操作。對於這種情況，下列哪一項應該是最令人擔憂的？
A. 缺乏可用性
B. 缺乏問責制
C. 授權不當
D. 身份驗證不充分
Answer: (SHOW ANSWER)
The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. References:
* https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam
* https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices
* https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

NEW QUESTION: 366
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: 367
將 IT 營運轉移到國外託管的基礎設施即服務 (IaaS) 模型時，下列哪一項是最關鍵的考量因素？
A. 資料標籤可能有助於確保將資料指派給正確的雲端類型。
B. 資料可能儲存在未知位置且可能不易擷取。
C. 如果發生安全漏洞，可能會承擔責任並受到處罰。
D. 原籍國的法律法規可能不適用。
Answer: (SHOW ANSWER)

NEW QUESTION: 368

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: 369
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: (SHOW ANSWER)
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: 370
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: 371
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. 進行威脅分析。
B. 實施資訊安全意識培訓計畫。
C. 建立審計委員會。
D. 創建資訊安全指導委員會。
Answer: (SHOW ANSWER)

NEW QUESTION: 372
下列哪一個流程最能支持事件回應有效性的評估？
A. 根本原因分析
B. 事件後審□
C. 監理鏈
D. 事件記錄
Answer: (SHOW ANSWER)
A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement1. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity2.
A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders3.
A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.

The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization ensure that the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the effectiveness of the response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation. However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices. References = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: Post-Incident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

NEW QUESTION: 373
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. 溝通計劃
B. 業務連續性計劃 (BCP)
C. 事件回應計劃
D. 災難復原計畫 (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 374
下列哪一項是製定業務連續性計劃 (BCP) 的第一步？
A. 確定可用資源。
B. 確定具有最短復原時間目標（RTO）的應用程式
C. 辨識關鍵業務流程。
D. 確定業務恢復策略
Answer: C (LEAVE A REPLY)

NEW QUESTION: 375
資訊安全團隊計劃加強面向客口的網站的身份驗證要求，但有人擔心這會對用口體驗口生負面影響。下列哪一項是資安經理的最佳行動方案？
A. 根據安全風險評估業務影響。
B. 為客口提供安全意識培訓。
C. 量化業務的安全風險。
D. 參考口業最佳實務。
Answer: (SHOW ANSWER)

NEW QUESTION: 376
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: 377
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

NEW QUESTION: 378
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: 379
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: 380
新的網路安全法規出台後，資安經理應先執行下列哪一項操作？
A. 進行成本效益分析。
B. 顧問公司法律顧問
C. 更新資訊安全性策略。
D. 執行差距分析。
Answer: (SHOW ANSWER)
When a new cybersecurity regulation has been introduced, an information security manager should first consult corporate legal counsel to understand the scope, applicability, and implications of the regulation for the organization. Legal counsel can also advise on the compliance obligations and deadlines, as well as the potential penalties or sanctions for non-compliance. Based on this information, the information security manager can then perform a gap analysis to assess the current state of compliance and identify any areas that need improvement. The information security policy can then be updated accordingly to reflect the new regulatory 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: 381
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: 382
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. 檢視企業架構 (EA) 中是否有威脅所利用的漏洞。
B. 更新日誌監控的關聯規則以偵測可能出現的威脅。
C. 立即向高階管理層報告威脅，以便做出明智的決定。
D. 評估新威脅一旦成為現實對組織的影響。
Answer: (SHOW ANSWER)

NEW QUESTION: 383
下列哪一項對於確保事件管理準備最重要？
A. 此計劃符合業界標準。
B. 該計劃定期接受測試。
C. 該計劃每年更新一次。
D. 本計劃簡潔且包含清單。
Answer: (SHOW ANSWER)
Regular testing ensures that the incident management plan is practical and effective in real-world scenarios.
"Regular testing of the incident response plan is essential to verify that it can be executed effectively and that staff understand their roles."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Testing and Evaluation*

NEW QUESTION: 384

下列哪一項對於保護企業免受進階持續性威脅 (APT) 最有幫助？

A. 更新的安全性策略

B. 定義的安全標準

C. 威脅情報

D. 定期防毒更新

Answer: B (LEAVE A REPLY)

Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.

The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. 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 1021.
* Advanced Persistent Threats and Nation-State Actors 1
* Book Review: Advanced Persistent Threats 2
* Advanced Persistent Threat (APT) Protection 3
* Establishing Advanced Persistent Security to Combat Long-Term Threats 4
* What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION: 385
新應用程式已進入生口環境，但技術安全控制有缺陷。下列哪一項最有可能是根本原因？
A. 事件回應控制不足
B. 缺乏法律審口
C. 變更控制不足
D. 缺乏品質控制
Answer: (SHOW ANSWER)
Change control is the process of ensuring that changes to an information system are authorized, tested, documented and implemented in a controlled manner. Inadequate change control can result in deficient technical security controls, such as missing patches, misconfigurations, vulnerabilities or errors in the new application.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291

NEW QUESTION: 386
對於遷移到基於雲端的解決方案的組織來口，下列哪一項是最佳的事件回應方法？
A. 採用雲端提供者的事件回應程式。
B. 將事件回應的責任轉移給雲端提供者。
C. 繼續使用現有的事件回應程式。
D. 修改事件回應程式以涵蓋雲端環境。
Answer: D (LEAVE A REPLY)
The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles and responsibilities, service level agreements, notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.
The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment.
References =

* CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-192, 195-196, 199-200.
* Cloud Incident Response Framework - A Quick Guide 2, pages 3-4, 6-7, 9-10.
* CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

NEW QUESTION: 387
某組織的員工報告丟失了包含敏感資訊的智慧型手機解決這種情況的最佳步驟是：
A. 禁止使用者存取公司資源。
B. 終止設備連線。
C. 遠端擦除設備
D. 升級至使用者管理
Answer: (SHOW ANSWER)
The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user' s management, may not be effective or timely enough to secure the sensitive information on the device.
References:
* https://www.security.org/resources/protect-data-lost-device/
* https://support.google.com/android/answer/6160491?hl=en
* https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

NEW QUESTION: 388
下列哪一項是資訊資口分類的主要目標？
A. 減少漏洞
B. 合規管理
C. 風險管理
D. 威脅最小化
Answer: (SHOW ANSWER)
The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security.

Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

NEW QUESTION: 389
下列哪一項對於改善業務連續性計劃 (BCP) 最重要？
A. 結合經驗教訓
B. 記錄關鍵業務流程
C. 實施管理評審
D. 實施 IT 彈性解決方案
Answer: A (LEAVE A REPLY)

NEW QUESTION: 390
在執行災難復原計畫 (DRP) 測試時，下列何者是最大的固有風險？
A. 結果和經驗教訓的記錄不完善
B. 缺乏與受影響使用者的溝通
C. 生口環境中斷
D. 部門之間缺乏協調
Answer: (SHOW ANSWER)
A disaster recovery plan (DRP) test is a simulation of a disaster scenario to evaluate the effectiveness and readiness of the DRP. The greatest inherent risk when performing a DRP test is the disruption to the production environment, which could cause operational issues, data loss, or system damage. Therefore, it is essential to plan and execute the DRP test carefully, with proper backup, isolation, and rollback procedures.
Poor documentation, lack of communication, and lack of coordination are also potential risks, but they are not as severe as disrupting the production environment. References = CISM Review Manual 15th Edition, page
253; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 224.
The greatest inherent risk when performing a disaster recovery plan (DRP) test is disruption to the production environment. A DRP test involves simulating a disaster scenario to ensure that the organization's plans are effective and that it is able to recover from an incident. However, this involves running tests on the production environment, which has the potential to disrupt the normal operations of the organization. This inherent risk can be mitigated by running tests on a non-production environment or by running tests at times when disruption will be minimized.

NEW QUESTION: 391
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: 392
在建立新的資安計畫時，下列哪一項應該是主要目標？
A. 執行安全性策略
B. 最小化組織風險
C. 最佳化資源
D. 促進操作安全
Answer: (SHOW ANSWER)
According to the CISM Review Manual, the primary objective when establishing a new information security program is to execute the security strategy that has been defined and approved by the senior management. The security strategy provides the direction, scope, and goals for the information security program, and aligns with the business objectives and requirements. Minimizing organizational risk, optimizing resources, and facilitating operational security are possible outcomes or benefits of the information security program, but they are not the primary objective.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.1.1, page 1151.

NEW QUESTION: 393
當組織採用新興技術時，下列何者是資訊安全職能部門的主要職責？

A. 開發新技術的安全培訓
B. 設計新的安全控制
C. 為技術制定可接受的使用政策
D. 評估潛在的安全風險
Answer: (SHOW ANSWER)
The primary responsibility of the information security function when an organization adopts emerging technologies is to assess the potential security risk, which means identifying and evaluating the threats, vulnerabilities, and impacts that the new technologies may pose to the organization's data, systems, and objectives. Assessing the potential security risk helps the information security function to determine the appropriate security requirements, controls, and measures to mitigate the risk and ensure the safe and secure adoption of the emerging technologies.
References = Performing Risk Assessments of Emerging Technologies, CISM Review Manual 15th Edition Learn more:
1. isaca.org2. isaca.org3. niccs.cisa.gov4. venturebeat.com
10of30
An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk? A.
Requirement for regular information security awareness B. Right-to-audit clause C. Service level agreement (SLA) D. Requirement to comply with corporate security policy answer: (Refer to the Information Security Manager (CISM) documents and learning resources by ISACA available at https://store.isaca.org/s/store#
/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles to verify the answer of the following questions very carefully.) Use the following format please: **Verified Answer** = (From CISM Manual or related resources) **Very Short Explanation** = (From CISM Manual or related resources) **References** = (From CISM Manual or related resources) ==========

NEW QUESTION: 394
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: 395
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: (SHOW ANSWER)
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.