ISACA.CISM.v2025-12-26.q389

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	389
Version:	v2025-12-26
# of views:	107
# of Questions views:	4923
https://www.freecram.net/torrent/ISACA.CISM.v2025-12-26.q389.html	

NEW QUESTION: 1
A recent application security assessment identified a number of low- and medium-level vulnerabilities. Which of the following stakeholders is responsible for deciding the appropriate risk treatment option?
A. Security manager
B. Chief information security officer (CISO)
C. System administrator
D. Business owner
Answer: (SHOW ANSWER)
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3, "The appropriate risk treatment option is decided by the chief information security officer (CISO) or the designated risk owner."1 Comprehensive and Detailed Explanation: The CISO is the senior executive who is responsible for overseeing and managing the information security program of an organization. The CISO has the authority and expertise to assess the risks, determine the risk appetite and tolerance levels, and select the most suitable risk treatment options for each risk. The CISO also has the accountability and responsibility for implementing, monitoring, and reporting on the risk treatment activities.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3

NEW QUESTION: 2
Which of the following is the MOST critical input to developing policies, standards, and procedures to secure information assets?
A. Vulnerability assessment
B. Regulatory requirements
C. Industry best practices
D. Enterprise goals
Answer: D (LEAVE A REPLY)

Enterprise goals are the most critical input because security policies must align with and support the organization's objectives and mission. Policies that do not align with enterprise goals are less likely to gain management support and may not effectively protect key assets.
"Information security must support enterprise goals and objectives to ensure alignment with the broader business strategy."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Alignment with Business Goals and Objectives ISACA's CISM questions reiterate that alignment with enterprise goals is essential for policy effectiveness.

NEW QUESTION: 3
Which of the following would BEST demonstrate the status of an organization's information security program to the board of directors?
A. Information security program metrics
B. Results of a recent external audit
C. The information security operations matrix
D. Changes to information security risks
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: 4
Which of the following is the BEST indication of an effective information security awareness training program?
A. An increase in the frequency of phishing tests
B. An increase in positive user feedback
C. An increase in the speed of incident resolution
D. An increase in the identification rate during phishing simulations
Answer: (SHOW ANSWER)
An effective information security awareness training program should aim to improve the knowledge, skills and behavior of the employees regarding information security. One of the ways to measure the effectiveness of such a program is to conduct phishing simulations, which are mock phishing attacks that test the employees' ability to identify and report phishing emails. An increase in the identification rate during phishing simulations indicates that the employees have learned how to recognize and avoid phishing attempts, which is one of the common threats to

information security. Therefore, this is the best indication of an effective information security awareness training program among the given options.
The other options are not as reliable or relevant as indicators of an effective information security awareness training program. An increase in the frequency of phishing tests does not necessarily mean that the employees are learning from them or that the tests are aligned with the learning objectives of the program. An increase in positive user feedback may reflect the satisfaction or engagement of the employees with the program, but it does not measure the actual learning outcomes or behavior changes. An increase in the speed of incident resolution may be influenced by other factors, such as the availability and efficiency of the incident response team, the severity and complexity of the incidents, or the tools and processes used for incident management. Moreover, the speed of incident resolution does not reflect the prevention or reduction of incidents, which is a more desirable goal of an information security awareness training program.
References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1001.

NEW QUESTION: 5
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?
A. To facilitate the continuous improvement of the IT organization
B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan
Answer: (SHOW ANSWER)
The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.
The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3:
Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION: 6
Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?
A. Chief information security officer (CISO)
B. Information security steering committee
C. Data privacy officer (DPO)
D. Enterprise risk committee
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following is MOST important to ensuring that incident management plans are executed effectively?
A. An incident response maturity assessment has been conducted.
B. The incident response team has the appropriate training.
C. Management support and approval has been obtained.
D. A reputable managed security services provider has been engaged.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following is the BEST course of action when an online company discovers a network attack in progress?
A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events
D. Shut off all network access points
Answer: (SHOW ANSWER)
The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

NEW QUESTION: 9
Which of the following is the GREATEST benefit of using AI tools in security operations?
A. Rapid detection and response to threats
B. Prioritized vulnerabilities
C. Reduced time and effort required to patch systems
D. Defined risk tolerance
Answer: (SHOW ANSWER)

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

NEW QUESTION: 10
Which of the following is the MOST important issue in a penetration test?
A. Having an independent group perform the test
B. Obtaining permission from audit
C. Performing the test without the benefit of any insider knowledge
D. Having a defined goal as well as success and failure criteria
Answer: D (LEAVE A REPLY)
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: 11
Which of the following is MOST effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application?

A. A patch management process
B. Version control
C. Change management controls
D. Logical access controls
Answer: (SHOW ANSWER)
= Change management controls are the most effective in preventing the introduction of vulnerabilities that may disrupt the availability of a critical business application. Change management controls are the policies, procedures, and practices that govern the initiation, approval, implementation, testing, and documentation of changes to the information systems and infrastructure. Change management controls help to ensure that changes are authorized, planned, controlled, and monitored, and that they do not introduce any unintended or adverse effects on the security, functionality, performance, or reliability of the system or application. Change management controls also help to identify and mitigate any potential risks or issues that may arise from the changes, and to ensure that the changes are aligned with the business objectives and requirements. By implementing change management controls, the organization can prevent the introduction of vulnerabilities that may disrupt the availability of a critical business application, as well as enhance the quality and efficiency of the change process. References = CISM Review Manual 15th Edition, page 105, page 106.

NEW QUESTION: 12
Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?
A. Perform a risk assessment.
B. Reduce security hardening settings.
C. Inform business management of the risk.
D. Document a security exception.
Answer: (SHOW ANSWER)
Security hardening is the process of applying security configuration settings to systems and software to reduce their attack surface and improve their resistance to threats1. Security hardening settings are based on industry standards and best practices, such as the CIS Benchmarks2, which provide recommended security configurations for various software applications, operating systems, and network devices. However, security hardening settings may not always be compatible with the business requirements and objectives of an organization, and may negatively impact the functionality, performance, or usability of the systems and software3. Therefore, before applying any security hardening settings, an information security manager should perform a risk assessment to evaluate the potential benefits and drawbacks of the settings, and to identify and prioritize the risks associated with them. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses.
A risk assessment helps the information security manager to balance the security and business needs of the organization, and to communicate the risk level and impact to the relevant

stakeholders. A risk assessment should be performed first, before taking any other actions, such as reducing security hardening settings, informing business management of the risk, or documenting a security exception, because it provides the necessary information and justification for making informed and rational decisions. References = 1: Basics of the CIS Hardening Guidelines | RSI Security 2: CIS Baseline Hardening and Security Configuration Guide | CalCom 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 145 : CISM Review Manual 15th Edition, page 146 : CISM Review Manual 15th Edition, page 147

NEW QUESTION: 13
What is the MOST important consideration for an organization operating in a highly regulated market when new regulatory requirements with high impact to the business need to be implemented?
A. Engaging an external audit
B. Conducting a gap analysis
C. Enforcing strong monitoring controls
D. Establishing compensating controls
Answer: (SHOW ANSWER)

NEW QUESTION: 14
In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:
A. evaluate results of the most recent incident response test.
B. review the number of reported security incidents.
C. ensure established security metrics are reported.
D. assess progress of risk mitigation efforts.
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: 15
A new risk has been identified in a high availability system. The BEST course of action is to:
A. Perform a cost-benefit analysis for mitigating controls
B. Recommend risk acceptance to the business owner
C. Develop and implement a plan to mitigate the identified risk
D. Evaluate and prioritize the identified risk
Answer: (SHOW ANSWER)
The best first step is to evaluate and prioritize the risk to determine the appropriate treatment strategy before implementing mitigation.
"Once risks are identified, they should be evaluated and prioritized to determine the best response (mitigation, transfer, acceptance, or avoidance)."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment*
ISACA practice questions confirm the need for evaluation and prioritization before taking further action.

NEW QUESTION: 16
Which of the following BEST supports effective communication during information security incidents7
A. Frequent incident response training sessions
B. Centralized control monitoring capabilities
C. Responsibilities defined within role descriptions
D. Predetermined service level agreements (SLAs)
Answer: (SHOW ANSWER)
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: 17
Which of the following would be the BEST way to reduce the risk of disruption resulting from an emergency system change?
A. Confirm the change implementation is scheduled.
B. Verify the change request has been approved.
C. Confirm rollback plans are in place.
D. Notify users affected by the change.
Answer: (SHOW ANSWER)
The best way to reduce the risk of disruption from an emergency system change is to confirm rollback plans are in place. According to the CISM Review Manual, having an effective rollback (or backout) plan ensures that if the emergency change causes unexpected issues, the organization can quickly revert to a known, stable state. This minimizes downtime and impact to business operations. Approval and communication are important, but only a rollback plan directly addresses risk reduction during unexpected disruptions.
Reference:ISACA CISM Review Manual, 16th Edition, Page 210, "Change Management - Rollback Planning".

NEW QUESTION: 18
The categorization of incidents is MOST important for evaluating which of the following?
A. Appropriate communication channels
B. Allocation of needed resources
C. Risk severity and incident priority
D. Response and containment requirements
Answer: C (LEAVE A REPLY)
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: 19
An employee clicked on a link in a phishing email, triggering a ransomware attack Which of the following should be the information security?
A. Wipe the affected system.
B. Notify internal legal counsel.
C. Notify senior management.
D. Isolate the impacted endpoints.
Answer: (SHOW ANSWER)
Isolating the impacted endpoints is the best course of action for the information security manager after an employee clicked on a link in a phishing email, triggering a ransomware attack because it prevents the ransomware from spreading to other systems or devices on the network, and minimizes the damage or disruption caused by the attack. Wiping the affected system is not a good course of action because it may destroy any evidence or data that could be used for investigation or recovery. Notifying internal legal counsel is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. Notifying senior management is not a good course of action because it does not address the immediate threat or impact of the ransomware attack. References: https://www.isaca.org/resources/isaca-journal/issues
/2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018
/volume-3/incident-response-lessons-learned

NEW QUESTION: 20
When an organization lacks internal expertise to conduct highly technical forensics investigations, what is the BEST way to ensure effective and timely investigations following an information security incident?

A. Purchase forensic standard operating procedures.
B. Provide forensics training to the information security team.
C. Retain a forensics firm prior to experiencing an incident.
D. Ensure the incident response policy allows hiring a forensics firm.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which of the following BEST enables staff acceptance of information security policies?
A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program
D. Adequate security funding
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: 22
An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?
A. Identify the skill set of the provider's incident response team.
B. Evaluate the provider's audit logging and monitoring controls.
C. Review the provider's incident definitions and notification criteria.
D. Update the incident escalation process.
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: 23
Which of the following is the BEST way to assess the risk associated with using a Software as a Service (SaaS) vendor?
A. Verify that information security requirements are included in the contract.

B. Request customer references from the vendor.
C. Require vendors to complete information security questionnaires.
D. Review the results of the vendor's independent control reports.
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: 24
Who has the PRIMARY authority to decide if additional risk treatments are required to mitigate an identified risk?
A. Information security manager
B. IT risk manager
C. Internal auditor
D. Risk owner
Answer: (SHOW ANSWER)
The risk owner is the person who has the authority and accountability to make decisions about the risk, including whether to accept, avoid, transfer, or mitigate it. The risk owner is also responsible for implementing and monitoring the risk treatment plan and reporting on the risk status. The risk owner is usually the business process owner or the information owner of the

asset affected by the risk. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2.

NEW QUESTION: 25
An organization has multiple data repositories across different departments. The information security manager has been tasked with creating an enterprise strategy for protecting data. Which of the following information security initiatives should be the HIGHEST priority for the organization?
A. Data masking
B. Data retention strategy
C. Data encryption standards
D. Data loss prevention (DLP)
Answer: (SHOW ANSWER)
Data encryption standards are the best information security initiative for creating an enterprise strategy for protecting data across multiple data repositories and different departments because they help to ensure the confidentiality, integrity, and availability of data in transit and at rest. Data encryption is a process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt it. Data encryption standards are the rules or specifications that define how data encryption should be performed, such as the type, strength, and mode of encryption, the key management and distribution methods, and the compliance requirements. Data encryption standards help to protect data from unauthorized access, modification, or theft, as well as to meet the regulatory obligations for data privacy and security. Therefore, data encryption standards are the correct answer.
References:
https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data-protection-strategy
https://cloudian.com/guides/data-protection/data-protection-strategy-10-components-of-an-effective-strategy/
https://www.veritas.com/information-center/enterprise-data-protection

NEW QUESTION: 26
The PRIMARY objective of timely declaration of a disaster is to:
A. ensure engagement of business management in the recovery process.
B. assess and correct disaster recovery process deficiencies.
C. protect critical physical assets from further loss.
D. ensure the continuity of the organization's essential services.
Answer: D (LEAVE A REPLY)
The primary objective of timely declaration of a disaster is to ensure the continuity of the organization's essential services, which are the services that are critical for the survival and operation of the organization, and that cannot be interrupted or delayed without causing severe consequences. By declaring a disaster, the organization can activate its disaster recovery plan

(DRP), which is a set of documented procedures and resources to recover the essential services in the event of a disaster. The DRP should include the roles and responsibilities, the communication channels, the recovery strategies, the backup and restoration procedures, and the testing and maintenance activities for the disaster recovery process1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 9: Business Continuity and Disaster Recovery, Section: Disaster Recovery Planning, Subsection: Disaster Declaration, Page 372.

NEW QUESTION: 27
Which of the following is the BEST method to ensure compliance with password standards?
A. Implementing password-synchronization software
B. Using password-cracking software
C. Automated enforcement of password syntax rules
D. A user-awareness program
Answer: (SHOW ANSWER)
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.
Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for
2020 - Auth0 2: Password synchronization - Wikipedia 3:

NEW QUESTION: 28
The effectiveness of an information security governance framework will BEST be enhanced if:
A. consultants review the information security governance framework.
B. a culture of legal and regulatory compliance is promoted by management.
C. risk management is built into operational and strategic activities.
D. IS auditors are empowered to evaluate governance activities
Answer: B (LEAVE A REPLY)
The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk management is

a key component of information security governance, which is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:
Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2:
Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

NEW QUESTION: 29
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?
A. Employee training on ransomware
B. A properly tested offline backup system
C. A continual server replication process
D. A properly configured firewall
Answer: B (LEAVE A REPLY)
The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures.
Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware.
However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time.

However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable.
A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 30

Which of the following has the GREATEST impact on the ability to successfully execute a disaster recovery plan (DRP)?

A. Conducting tabletop exercises of the plan
B. Updating the plan periodically
C. Communicating the plan to all stakeholders
D. Reviewing escalation procedures
Answer: (SHOW ANSWER)
The CISM Review Manual emphasizes that the success of a DRP (Disaster Recovery Plan) depends greatly on clear communication of the plan to all stakeholders. Stakeholders must be aware of their roles and responsibilities during an incident to ensure the plan can be effectively executed. While testing, updating, and reviewing the plan are also important, communication is critical to effective execution.
Reference:ISACA CISM Review Manual, 16th Edition, Page 250-251, "Disaster Recovery Planning - Key Success Factors".

NEW QUESTION: 31
Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?
A. Escalation processes
B. Technological capabilities
C. Recovery time objective (RTO)
D. Security audit reports
Answer: (SHOW ANSWER)
Escalation processes ensure that the provider and the organization can coordinate quickly and effectively during incidents.
"A clearly defined escalation process ensures that incidents are handled swiftly and with the appropriate level of authority, particularly when working with cloud service providers."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Cloud and Outsourced Incident Response* ISACA practice questions reinforce that escalation processes are critical when collaborating with third parties in incident management.

NEW QUESTION: 32
Which of the following is the BEST indicator of an emerging incident?
A. Customer complaints about lack of website availability
B. A recent security incident at an industry competitor
C. Attempted patching of systems resulting in errors
D. A weakness identified within an organization's information systems
Answer: (SHOW ANSWER)

NEW QUESTION: 33
From an information security perspective, legal issues associated with a transborder flow of technology- related items are MOST often
A. website transactions and taxation.
B. software patches and corporate date.
C. encryption tools and personal data.
D. lack of competition and free trade.
Answer: (SHOW ANSWER)
Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. References: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on- transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

NEW QUESTION: 34

Which of the following is MOST important when conducting a forensic investigation?
A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody
Answer: (SHOW ANSWER)
Maintaining a chain of custody is the most important step when conducting a forensic investigation, as this ensures that the evidence is preserved, protected, and documented from the time of collection to the time of presentation in court. A chain of custody provides a record of who handled the evidence, when, where, why, and how, and prevents any tampering, alteration, or loss of the evidence. A chain of custody also establishes the authenticity, reliability, and admissibility of the evidence in legal proceedings. Analyzing system memory, documenting analysis steps, and capturing full system images are also important, but not as important as maintaining a chain of custody, as they do not guarantee the integrity and validity of the evidence.
References = CISM Review Manual 2023, page 1701; CISM Review Questions, Answers & Explanations Manual 2023, page 332; ISACA CISM - iSecPrep, page 183

NEW QUESTION: 35
During which phase of an incident response plan is the root cause determined?
A. Recovery
B. Lessons learned
C. Containment
D. Eradication
Answer: (SHOW ANSWER)
The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 36
After updating password standards, an information security manager is alerted by various application administrators that the applications they support are incapable of enforcing these standards. The information security manager's FIRST course of action should be to:
A. determine the potential impact.
B. reevaluate the standards.
C. implement compensating controls.
D. evaluate the cost of replacing the applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following is a desired outcome of information security governance?

A. Penetration test
B. Improved risk management
C. Business agility
D. A maturity model
Answer: (SHOW ANSWER)
Business agility is a desired outcome of information security governance, as it enables the organization to respond quickly and effectively to changing business needs and opportunities, while maintaining a high level of security and risk management. Information security governance provides the strategic direction, policies, standards, and oversight for the information security program, ensuring that it aligns with the organization's business objectives and stakeholder expectations. Information security governance also facilitates the integration of security into the business processes and systems, enhancing the organization's ability to adapt to the dynamic and complex environment. By implementing information security governance, the organization can achieve business agility, as well as other benefits such as improved risk management, compliance, reputation, and value creation. References = CISM Review Manual 15th Edition, page 25.

NEW QUESTION: 38
Which of the following is the PRIMARY benefit of implementing an information security governance framework?
A. The framework defines managerial responsibilities for risk impacts to business goals.
B. The framework provides direction to meet business goals while balancing risks and controls.
C. The framework provides a roadmap to maximize revenue through the secure use of technology.
D. The framework is able to confirm the validity of business goals and strategies.
Answer: (SHOW ANSWER)
An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified. References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 39
While conducting a test of a business continuity plan (BCP), which of the following is the MOST important consideration?
A. The test is scheduled to reduce operational impact.
B. The test involves IT members in the test process.
C. The test addresses the critical components.

D. The test simulates actual prime-time processing conditions.

Answer: (SHOW ANSWER)

The test addresses the critical components is the most important consideration while conducting a test of a business continuity plan (BCP), as it ensures that the test covers the essential functions, processes, and resources that are required to maintain or resume the organization's operations in the event of a disruption.

The test should also verify that the recovery objectives, such as recovery time objective (RTO) and recovery point objective (RPO), are met. (From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1; CISSP Exam Cram: Business Continuity and Disaster Recovery Planning1, page 5, section Testing the Plan.

NEW QUESTION: 40

Which of the following is the PRIMARY objective of testing security controls within a critical infrastructure?

A. Reducing the number of control assessments to optimize resources

B. Ensuring the continued resilience and security of IT services

C. Decreasing the percentage of security deployments that cause failures in production

D. Identifying and addressing security team performance issues

Answer: B (LEAVE A REPLY)

NEW QUESTION: 41

An information security manager is assessing security risk associated with a cloud service provider. Which of the following is the MOST appropriate reference to consult when performing this assessment?

A. Previous provider service level agreements (SLAs)

B. Security control frameworks

C. Threat intelligence reports

D. Penetration test results from the provider

Answer: (SHOW ANSWER)

Security control frameworks (e.g., ISO/IEC 27001, NIST SP 800-53, CSA Cloud Controls Matrix) provide a structured and standardized approach to assess the security posture of cloud providers. These frameworks ensure completeness and alignment with best practices.

"Standardized security frameworks enable consistent evaluation of third-party providers and alignment with industry-recognized security requirements."

- CISM Review Manual 15th Edition, Chapter 3: Third-Party Risk Management* Penetration test results and SLAs are useful, but only frameworks provide comprehensive coverage.

NEW QUESTION: 42

An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. Internal IT audit

B. The data custodian
C. The information security manager
D. The data owner
Answer: (SHOW ANSWER)
The data owner is the person who has the authority and responsibility to classify, grant access, and monitor the use of the CRM data. The data owner should ensure that the data is protected according to its classification and business requirements. The data custodian is the person who implements the controls and procedures to protect the data as directed by the data owner. The information security manager is the person who advises the data owner on the best practices and standards for data security. The internal IT audit is the function that evaluates the effectiveness and compliance of the data security controls and procedures.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Roles and Responsibilities, Subsection: Data Owner, Page 23.

NEW QUESTION: 43
Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?
A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.
Answer: (SHOW ANSWER)
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
* 1: Information Security Incident Response Escalation Guideline2, page 4
* 2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
* 3: Computer Security Incident Handling Guide4, page 18

NEW QUESTION: 44
The GREATEST challenge when attempting data recovery of a specific file during forensic analysis is when:
A. the partition table on the disk has been deleted.
B. the tile has been overwritten.
C. all files in the directory have been deleted.

D. high-level disk formatting has been performed.

Answer: (SHOW ANSWER)

Data recovery is the process of restoring data that has been lost, corrupted, or deleted. When a file is deleted, it is usually not physically erased from the disk, but only marked as free space by the operating system.

Therefore, it may be possible to recover the file by using specialized tools that scan the disk for the file's data.

However, if the file has been overwritten by another file or data, then the original file's data is lost and cannot be recovered. The other options are not as challenging as overwriting, because they only affect the logical structure of the disk, not the physical data. For example, the partition table, the directory, and the formatting information can be reconstructed or bypassed by using forensic tools. References = CISM Review Manual,

16th Edition, Chapter 5, Section 5.4.1.2

NEW QUESTION: 45

When investigating an information security incident, details of the incident should be shared:

A. widely to demonstrate positive intent.

B. only with management.

C. only as needed,

D. only with internal audit.

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: 46

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. Process owners

B. End users
C. Security architects.
D. Corporate auditors
Answer: (SHOW ANSWER)
Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them.
Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to.
Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support.
References = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

NEW QUESTION: 47

Which of the following provides the BEST evidence that a recently established infofmation security program is effective?

A. The number of reported incidents has increased

B. Regular IT balanced scorecards are communicated.

C. Senior management has reported fewer junk emails.

D. The number of tickets associated with IT incidents have stayed consistent

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: 48

Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?

A. To reduce risk mitigation costs

B. To resolve vulnerabilities in enterprise architecture (EA)

C. To manage the risk to an acceptable level

D. To eliminate threats impacting the business

Answer: (SHOW ANSWER)

According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

NEW QUESTION: 49

Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?

A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk
Answer: (SHOW ANSWER)
Communicating the residual risk is the best way to facilitate an information security manager's efforts to obtain senior management commitment for an information security program. The residual risk is the level of risk that remains after applying the security controls and mitigation measures. The residual risk reflects the effectiveness and efficiency of the information security program, as well as the potential impact and exposure of the organization. The information security manager should communicate the residual risk to the senior management in a clear, concise, and relevant manner, using quantitative or qualitative methods, such as risk matrices, heat maps, dashboards, or reports. The communication of the residual risk should also include the comparison with the inherent risk, which is the level of risk before applying any security controls, and the risk appetite, which is the level of risk that the organization is willing to accept. The communication of the residual risk should help the senior management to understand the value and performance of the information security program, as well as the need and justification for further investment or improvement. Presenting evidence of inherent risk, reporting the security maturity level, and presenting compliance requirements are all important aspects of the information security program, but they are not the best ways to obtain senior management commitment. These aspects may not directly demonstrate the benefits or outcomes of the information security program, or they may not align with the business objectives or priorities of the organization. For example, presenting evidence of inherent risk may show the potential threats and vulnerabilities that the organization faces, but it may not indicate how the information security program addresses or reduces them. Reporting the security maturity level may show the progress and status of the information security program, but it may not relate to the risk level or the business impact. Presenting compliance requirements may show the legal or regulatory obligations that the organization must fulfill, but it may not reflect the actual security needs or goals of the organization. Therefore, communicating the residual risk is the best way to obtain senior management commitment for an information security program, as it shows the results and value of the information security program for the organization. References = CISM Review Manual 2023, page 41 1; CISM Practice Quiz 2

NEW QUESTION: 50
The PRIMARY goal when conducting post-incident reviews is to identify:
A. Additional cybersecurity budget needs
B. Weaknesses in incident response plans
C. Information to be shared with senior management
D. Individuals that need additional training
Answer: (SHOW ANSWER)

The core objective of a post-incident review (PIR) is to identify gaps and weaknesses in the response process. This includes missteps, delays, communication failures, or policy limitations - all of which provide insight to improve future incident handling.
"Post-incident reviews focus on identifying root causes and areas for improvement to enhance the organization's preparedness for future incidents."
- CISM Review Manual 15th Edition, Chapter 4: Post-Incident Activities* Though training, reporting, and budgeting may follow, they are secondary outcomes of this process.

NEW QUESTION: 51
Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:
A. hand over the controls to the relevant business owners.
B. prepare to adapt the controls for future system upgrades.
C. ensure the controls are regularly tested for ongoing effectiveness.
D. perform testing to compare control performance against industry levels.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
A Seat a-hosting organization's data center houses servers, appli
BEST approach for developing a physical access control policy for the organization?
A. Review customers' security policies.
B. Conduct a risk assessment to determine security risks and mitigating controls.
C. Develop access control requirements for each system and application.
D. Design single sign-on (SSO) or federated access.
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: 53
Which of the following will BEST facilitate timely and effective incident response?
A. Assessing the risk of compromised assets
B. Including penetration test results in incident response planning
C. Notifying stakeholders when invoking the incident response plan
D. Classifying the severity of an incident
Answer: (SHOW ANSWER)

NEW QUESTION: 54
When developing an incident escalation process, the BEST approach is to classify incidents based on:
A. estimated time to recover.
B. information assets affected.
C. recovery point objectives (RPOs).
D. their root causes.
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: 55
What should be the FIRST step when implementing data loss prevention (DLP) technology?
A. Perform a cost benefit analysis
B. Build a business case
C. Perform due diligence with vendor candidates
D. Classify the organization's data
Answer: (SHOW ANSWER)

NEW QUESTION: 56
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?
A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.
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: 57
Which of the following is the MOST appropriate metric to demonstrate the effectiveness of information security controls to senior management?
A. Downtime due to malware infections
B. Number of security vulnerabilities uncovered with network scans
C. Percentage of servers patched
D. Annualized loss resulting from security incidents
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: 58
Which of the following should be the MOST important consideration when reviewing an information security strategy?
A. Recent security incidents
B. New business initiatives

C. Industry security standards
D. Internal audit findings
Answer: (SHOW ANSWER)
New business initiatives are the most important consideration, as security must align with business changes to effectively protect assets and support growth.
"The security strategy must be aligned with new business initiatives to ensure it continues to protect critical assets and support enterprise goals."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Business Alignment* ISACA practice questions stress that aligning with new business initiatives ensures relevance and effectiveness.

NEW QUESTION: 59
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?
A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process
Answer: D (LEAVE A REPLY)
A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right people are involved in the incident response, that the incident is handled in a timely and efficient manner, and that the relevant information is shared with the appropriate parties. Skills required for the incident response team, a list of external resources to assist with incidents, and service level agreements (SLAs) are also important elements of an incident response plan, but they are not as critical as the incident notification process. Skills required for the incident response team describe the competencies and qualifications of the team members, but they do not specify who should be notified or involved in the incident response. A list of external resources to assist with incidents provides a directory of external parties that can provide support or expertise in the incident response, but it does not define the criteria or process for engaging them. Service level agreements (SLAs) define the expectations and obligations of the service providers and the service recipients in the incident response, but they do not detail the steps or procedures for notifying or escalating incidents. References = CISM Review Manual, 16th Edition, pages 191-1921; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 662

NEW QUESTION: 60
When taking a risk-based approach to vulnerability management, which of the following is MOST important to consider when prioritizing a vulnerability?

A. The information available about the vulnerability
B. The sensitivity of the asset and the data it contains
C. IT resource availability and constraints
D. Whether patches have been developed and tested
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Risk-based vulnerability management prioritizes vulnerabilities based on the potential impact on critical assets.
A). The information available about the vulnerability: While important for assessing risk, it does not directly determine the priority.
B). The sensitivity of the asset and the data it contains: This is the BEST answer because prioritizing vulnerabilities based on the criticality of the affected assets ensures that high-impact threats are addressed first.
C). IT resource availability and constraints: These are logistical considerations but should not outweigh risk impact.
D). Whether patches have been developed and tested: Patches are important for remediation but do not determine prioritization.
Reference: CISM Job Practice Area 2 (Risk Management) emphasizes considering asset criticality when prioritizing vulnerabilities.

NEW QUESTION: 61
Which of the following is the BEST way to reduce the risk associated with a bring your own device (BYOD) program?
A. Provide employee training on secure mobile device practices.
B. Require employees to install an effective anti-malware app.
C. Implement a mobile device management (MDM) solution.
D. Implement a mobile device policy and standard.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which of the following should an information security manager do FIRST when noncompliance with security standards is identified?

A. Report the noncompliance to senior management
B. Include the noncompliance in the risk register
C. Validate the noncompliance
D. Implement compensating controls to mitigate the noncompliance
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following is the PRIMARY objective of incident triage?
A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats
Answer: (SHOW ANSWER)
The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization's information security.
Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization's assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident. 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; Critical Incident Stress Management - National Interagency Fire Center3; Critical Incident Stress Management - US Forest Service4

NEW QUESTION: 64
Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?
A. Capability maturity model
B. Vulnerability assessment
C. IT security risk and exposure
D. Business impact analysis (BIA)
Answer: A (LEAVE A REPLY)

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: 65
Recommendations for enterprise investment in security technology should be PRIMARILY based on:
A. adherence to international standards

B. availability of financial resources
C. the organization s risk tolerance
D. alignment with business needs
Answer: C (LEAVE A REPLY)
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1, "Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance."1 Comprehensive and Detailed Explanation: The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security investments should be, as they can help protect the organization's assets and reputation from potential threats.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

NEW QUESTION: 66
A global organization is planning to expand its operations into a new country with stricter data protection regulations than those in the headquarters' home country. Which of the following is the BEST approach for adopting these new requirements?
A. Adjust organization-wide security polices to align with regulations of the new country.
B. Ensure local operations comply with geographical data protection laws of the headquarters.
C. Work with legal to interpret the local regulatory requirements and implement applicable controls.
D. Procure cybersecurity insurance that covers potential breaches and incidents in the new country.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following desired outcomes BEST supports a decision to invest in a new security initiative?
A. Enhanced security monitoring and reporting
B. Reduced control complexity
C. Enhanced threat detection capability
D. Reduction of organizational risk
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: 68
Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?
A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.
Answer: B (LEAVE A REPLY)
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: 69
A financial company executive is concerned about recently increasing cyberattacks and needs to take action to reduce risk. The organization would BEST respond by:
A. increasing budget and staffing levels for the incident response team.
B. implementing an intrusion detection system (IDS).
C. revalidating and mitigating risks to an acceptable level.
D. testing the business continuity plan (BCP).
Answer: (SHOW ANSWER)
The best response for the organization to reduce risk from increasing cyberattacks is to revalidate and mitigate risks to an acceptable level. This means that the organization should review its current risk profile, identify any new or emerging threats, vulnerabilities, or impacts, and evaluate the effectiveness of its existing controls and countermeasures. Based on this analysis, the organization should implement appropriate risk treatment strategies, such as avoiding, transferring, accepting, or reducing the risks, to achieve its desired risk appetite and tolerance. The organization should also monitor and review the risk situation and the implemented controls on a regular basis, and update its risk management plan accordingly. This approach is consistent with the ISACA Risk IT Framework, which provides guidance on how to align IT risk management with business objectives and value12.
The other options are not the best responses because they are either too narrow or too reactive. Increasing budget and staffing levels for the incident response team may improve the organization's ability to respond to and recover from cyberattacks, but it does not address the root causes or the prevention of the attacks.
Implementing an intrusion detection system (IDS) may enhance the organization's detection and analysis capabilities, but it does not guarantee the protection or mitigation of the attacks. Testing the business continuity plan (BCP) may verify the organization's readiness and resilience to continue its critical operations in the event of a cyberattack, but it does not reduce the likelihood or the impact of the attack. References = Risk IT Framework 1 CISM Review Manual, 16th Edition | Print | English 2, Chapter 3: Information Risk Management, pages 97-

98, 103-104, 107-108, 111-112.

NEW QUESTION: 70

Relationships between critical systems are BEST understood by

A. evaluating key performance indicators (KPIs)

B. performing a business impact analysis (BIA)

C. developing a system classification scheme

D. evaluating the recovery time objectives (RTOs)

Answer: (SHOW ANSWER)

The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

NEW QUESTION: 71

Which of the following is MOST helpful in the development of a cost-effective information security strategy that is aligned with business requirements?

A. Categorizing information assets

B. Benchmarking against industry peers

C. Enforcing data retention

D. Developing policy standards

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which of the following should be the PRIMARY outcome of an information security program?

A. Strategic alignment

B. Risk elimination

C. Cost reduction

D. Threat reduction

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: 73
Which of the following is the BEST approach to make strategic information security decisions?
A. Establish regular information security status reporting.
B. Establish an information security steering committee.
C. Establish business unit security working groups.
D. Establish periodic senior management meetings.
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: 74

Which of the following is the BEST source of information to support an organization's information security vision and strategy?
A. Governance policies
B. Metrics dashboard
C. Enterprise information security architecture
D. Capability maturity model
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following is the BEST indication that an organization has a mature information security culture?
A. Information security training is mandatory for all staff.
B. The organization's information security policy is documented and communicated.
C. The chief information security officer (CISO) regularly interacts with the board.
D. Staff consistently consider risk in making decisions.
Answer: (SHOW ANSWER)
The BEST indication that an organization has a mature information security culture is when its staff consistently consider risk in making decisions. When an organization's staff understands the risks associated with their actions and are empowered to make risk-informed decisions, it indicates that the organization has a mature information security culture.
According to the Certified Information Security Manager (CISM) Study Manual, "A mature information security culture exists when the people within the organization understand and appreciate the risks associated with information and technology and when they take steps to manage those risks on a daily basis." While information security training, documented information security policies, and regular interaction between the chief information security officer (CISO) and the board are all important components of a mature information security culture, they are not sufficient on their own. It is only when staff consistently consider risk in making decisions that an organization's information security culture can be considered mature.
Reference:
Certified Information Security Manager (CISM) Study Manual, 15th Edition, Pages 151-152.

NEW QUESTION: 76
Which of the following is the MOST important factor of a successful information security program?
A. The program follows industry best practices.
B. The program is based on a well-developed strategy.
C. The program is cost-efficient and within budget,
D. The program is focused on risk management.
Answer: (SHOW ANSWER)
A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused

on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources, implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus. References = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

NEW QUESTION: 77
For event logs to be acceptable for incident investigation, which of the following is the MOST important consideration to establish chain of evidence?
A. Time clock synchronization
B. Administrator log access
C. Available forensic tools
D. Centralized logging
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following should be an information security manager's PRIMARY concern when an organization is expanding business to a new country?
A. Compliance with local regulations
B. Ability to gather customer data
C. Changes in IT infrastructure
D. Cultural differences in the new country
Answer: (SHOW ANSWER)

NEW QUESTION: 79
The PRIMARY objective of performing a post-incident review is to:
A. re-evaluate the impact of incidents

B. identify vulnerabilities
C. identify control improvements.
D. identify the root cause.
Answer: (SHOW ANSWER)
= The PRIMARY objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled 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: 80
An incident response team has established that an application has been breached. Which of the following should be done NEXT?

A. Maintain the affected systems in a forensically acceptable state
B. Conduct a risk assessment on the affected application
C. Inform senior management of the breach.
D. Isolate the impacted systems from the rest of the network
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: 81

When drafting the corporate privacy statement for a public website, which of the following MUST be included?

A. Limited liability clause

B. Explanation of information usage

C. Information encryption requirements

D. Access control requirements

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: 82

When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

A. Data is encrypted in transit and at rest at the vendor site.

B. Data is subject to regular access log review.

C. The vendor must be able to amend data.

D. The vendor must agree to the organization's information security policy,

Answer: (SHOW ANSWER)

When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization's information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization's information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization's right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.

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

Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

NEW QUESTION: 83

Which of the following is the PRIMARY role of an information security manager in a software development project?

A. To enhance awareness for secure software design

B. To assess and approve the security application architecture

C. To identify noncompliance in the early design stage

D. To identify software security weaknesses

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 84
Which of the following should be done FIRST once a cybersecurity attack has been confirmed?
A. Isolate the affected system.
B. Notify senior management.
C. Power down the system.
D. Contact legal authorities.
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: 85
Which of the following is the GREATEST inherent risk when performing a disaster recovery plan (DRP) test?
A. Poor documentation of results and lessons learned
B. Lack of communication to affected users
C. Disruption to the production environment
D. Lack of coordination among departments
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: 86
Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?
A. Recovery strategy
B. IT strategy
C. Risk mitigation strategy
D. Security 'strategy
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following is MOST important in order to obtain senior leadership support when presenting an information security strategy?
A. The strategy aligns with management's acceptable level of risk.
B. The strategy addresses ineffective information security controls.
C. The strategy aligns with industry benchmarks and standards.
D. The strategy addresses organizational maturity and the threat environment.
Answer: (SHOW ANSWER)
The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat environment is not a very important factor because it does not indicate how the

strategy will advance or adapt the organization's security posture or resilience. References: https://www.isaca.org/resources /isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems https://www.isaca. org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and- objectives

NEW QUESTION: 88
Which of the following is necessary to ensure consistent protection for an organization's information assets?
A. Classification model
B. Control assessment
C. Data ownership
D. Regulatory requirements
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: 89

A global organization has outsourced security processes to a service provider by means of a global agreement.
What is the MOST efficient approach to meet country-specific regulatory requirements?
A. Include binding corporate rules into the global agreement
B. Set up a governance organization for each country
C. Review the agreement for each country separately
D. Set up companion agreements for each country
Answer: (SHOW ANSWER)
Binding Corporate Rules (BCRs) are legally enforceable and approved data protection policies used to facilitate compliance across multiple jurisdictions. Incorporating BCRs into a global agreement enables the organization to efficiently manage regulatory obligations across countries.
"Binding corporate rules offer a scalable and consistent mechanism to address cross-border compliance in global outsourcing agreements."
- CISM Review Manual 15th Edition, Chapter 1: Governance, Section: Cross-Border Data Protection Considerations* Creating separate agreements per country is inefficient and complex compared to centralized BCR-based governance.

NEW QUESTION: 90
An organization is leveraging tablets to replace desktop computers shared by shift-based staff These tablets contain critical business data and are inherently at increased risk of theft Which of the following will BEST help to mitigate this risk"

A. Deploy mobile device management (MDM)
B. Implement remote wipe capability.
C. Create an acceptable use policy.
D. Conduct a mobile device risk assessment
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: 91
Which of the following is MOST important when designing security controls for new cloud-based services?
A. Evaluating different types of deployment models according to the associated risks
B. Understanding the business and IT strategy for moving resources to the cloud

C. Defining an incident response policy to protect data moving between onsite and cloud applications
D. Performing a business impact analysis (BIA) to gather information needed to develop recovery strategies
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: 92
Which of the following is MOST helpful in determining the criticality of an organization's business functions?
A. Disaster recovery plan (DRP)
B. Business impact analysis (BIA)
C. Business continuity plan (BCP)
D. Security assessment report (SAR)
Answer: B (LEAVE A REPLY)
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: 93
When performing a business impact analysis (BIA), who should be responsible for determining the initial recovery time objective (RTO)?
A. External consultant
B. Information owners
C. Information security manager
D. Business continuity coordinator
Answer: (SHOW ANSWER)
Information owners are responsible for determining the initial recovery time objective (RTO) for their information assets and processes, as they are the ones who understand the business requirements and impact of a disruption. An external consultant may assist in conducting the business impact analysis (BIA), but does not have the authority to decide the RTO. An information security manager may provide input on the security aspects of the RTO, but does not have the business perspective to determine the RTO. A business continuity coordinator may facilitate the BIA process and ensure the alignment of the RTO with the business continuity plan, but does not have the ownership of the information assets and processes. References = CISM Review Manual 15th Edition, page 202.
When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the BIA and should be determined in cooperation with the information owners. The RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

NEW QUESTION: 94
Which of the following is the BEST approach for governing noncompliance with security requirements?
A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.
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: 95
Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness program?
A. Number of security incidents reported to the help desk
B. Percentage of employee computers and devices infected with malware
C. Number of phishing emails viewed by end users
D. Percentage of employees who regularly attend security training
Answer: (SHOW ANSWER)

NEW QUESTION: 96
An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?
A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.
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: 97
Following an information security risk assessment of a critical system, several significant issues have been identified. Which of the following is MOST important for the information security manager to confirm?
A. The risks are reported to the business unit's senior management
B. The risks are escalated to the IT department for remediation
C. The risks are communicated to the central risk function
D. The risks are entered in the organization's risk register
Answer: (SHOW ANSWER)
Recording risks in the risk register ensures visibility, accountability, and tracking. This formal documentation is essential for assigning ownership, determining treatment strategies, and ensuring ongoing governance.

A risk that is not entered into the register may go unaddressed. This step supports structured risk tracking and compliance with governance practices.
"The risk register is the primary tool used to track, prioritize, assign, and monitor risks and their treatment. It forms the basis of a structured risk management program."
- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Documentation and Communication*

NEW QUESTION: 98
Which of the following is the BEST indicator of an organization's information security status?
A. Intrusion detection log analysis
B. Controls audit
C. Threat analysis
D. Penetration test
Answer: (SHOW ANSWER)
A controls audit is the best indicator of an organization's information security status, as it provides an independent and objective assessment of the design, implementation, and effectiveness of the information security controls. A controls audit can also identify the strengths and weaknesses of the information security program, as well as the compliance with the policies, standards, and regulations. A controls audit can cover various aspects of information security, such as governance, risk management, incident management, business continuity, and technical security. A controls audit can be conducted by internal or external auditors, depending on the scope, purpose, and frequency of the audit.
The other options are not as good as a controls audit, as they do not provide a comprehensive and holistic view of the information security status. Intrusion detection log analysis is a technique to monitor and analyze the network or system activities for signs of unauthorized or malicious access or attacks. It can help to detect and respond to security incidents, but it does not measure the overall performance or maturity of the information security program. Threat analysis is a process to identify and evaluate the potential sources, methods, and impacts of threats to the information assets. It can help to prioritize and mitigate the risks, but it does not verify the adequacy or functionality of the information security controls. Penetration test is a simulated attack on the network or system to evaluate the vulnerability and exploitability of the information security defenses. It can help to validate and improve the technical security, but it does not assess the non- technical aspects of information security, such as governance, policies, or awareness. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1012.

NEW QUESTION: 99
Which of the following is the BEST indicator of the maturity level of a vendor risk management process?
A. Average time required to complete the vendor risk management process

B. Percentage of vendors that have gone through the vendor onboarding process
C. Percentage of vendors that are regularly reviewed against defined criteria
D. Number of vendors rejected because of security review results
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: 100
Which of the following is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model?

A. Host patching
B. Penetration testing
C. Infrastructure hardening
D. Data classification
Answer: (SHOW ANSWER)
Data classification is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model. Data classification is the process of categorizing data based on its sensitivity, value and criticality to the organization. Data classification helps to determine the appropriate level of protection, access control and retention for different types of data. Data classification is an essential part of data governance and risk management, as it enables the organization to comply with legal and regulatory requirements, protect its intellectual property and reputation, and optimize its data storage and usage costs.
In a SaaS model, the client organization has the least control and responsibility over the cloud infrastructure, platform and application, as these are fully managed by the cloud service provider (CSP). The client organization only has control and responsibility over its own data and users. Therefore, the client organization is responsible for defining and implementing data classification policies and procedures, and ensuring that its data is properly labeled and handled according to its classification level. The client organization is also responsible for educating its users about the importance of data classification and the best practices for data security and privacy.
The other options are not the sole responsibility of the client organization in a SaaS model, as they are either shared with or delegated to the CSP. Host patching, penetration testing and infrastructure hardening are all related to the security and maintenance of the cloud infrastructure and platform, which are the responsibility of the CSP in a SaaS model. The CSP is expected to provide regular updates, patches and fixes to the host operating system, network and application components, and to conduct periodic security assessments and audits to identify and remediate

any vulnerabilities or weaknesses in the cloud environment. The client organization may have some responsibility to monitor and verify the CSP's performance and compliance with the service level agreement (SLA) and the cloud security standards and regulations, but it does not have direct control or access to the cloud infrastructure and platform. References = Understanding the Shared Responsibilities Model in Cloud Services - ISACA, Figure 1 CISM Review Manual, Chapter 3, page 121

NEW QUESTION: 101
Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?
A. The security strategy is promoted.
B. Fewer security incidents are reported.
C. Security behavior is improved.
D. More security incidents are detected.
Answer: (SHOW ANSWER)
The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.
The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms. Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208. CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.
The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal, Volume 1,

2019, 1.

NEW QUESTION: 102
Which of the following has the GREATEST influence on the successful integration of information security within the business?
A. Organizational structure and culture
B. Risk tolerance and organizational objectives
C. The desired state of the organization
D. Information security personnel
Answer: (SHOW ANSWER)
The factor that has the greatest influence on the successful integration of information security within the business is organizational structure and culture because they determine how information security is organized, governed, and supported within the organization, and how information security roles and responsibilities are defined, assigned, and communicated across different levels and functions. Risk tolerance and organizational objectives are not very influential because they do not affect how information security is integrated within the business, but rather what information security aims to achieve or protect. The desired state of the organization is not very influential because it does not affect how information security is integrated within the business, but rather what the organization aspires to be or do. Information security personnel are not very influential because they do not affect how information security is integrated within the business, but rather who performs information security tasks or activities. 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: 103
An organization successfully responded to an information security incident. However, the information security manager learned that some of the steps specified in the incident management procedures were not taken by the response team. What should be the information security manager's FIRST step?
A. Review the incident management procedures.
B. Interview the incident response team.
C. Remove the steps from the incident management procedures.
D. Provide additional training to the incident response team.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?
A. Patch management files

B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs
Answer: A (LEAVE A REPLY)
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: 105
How does an organization PRIMARILY benefit from the creation of an information security steering committee?
A. An increased alignment of information security with the business
B. An increased focus on information security resource management
C. An increase in information security risk awareness
D. An increased alignment with industry security trends that impact the business
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which of the following should be of GREATEST concern to an information security manager when evaluating a cloud service provider?
A. Data retention policies are not documented
B. There is no right to audit the security of the provider
C. The provider is new to the market and lacks references
D. Security controls offered by the provider are inadequate
Answer: (SHOW ANSWER)
The lack of audit rights prevents the organization from verifying the security posture and compliance of the provider, representing a major governance and assurance gap.
"Right to audit clauses ensure that organizations retain oversight and can verify the security controls and compliance of their service providers."
- CISM Review Manual 15th Edition, Chapter 3: Outsourced Services, Section: Third-Party Governance* Control inadequacy can be fixed; lack of oversight cannot be tolerated.

NEW QUESTION: 107
Which of the following should be the FIRST step when performing triage of a malware incident?
A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware
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: 108
An incident response plan is being developed for servers hosting sensitive information. In the event of a breach, who should make the decision to shut down the system?
A. Operations manager
B. Service owner
C. Information security manager
D. Incident response team
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which of the following metrics would BEST demonstrate the success of a newly implemented information security framework?
A. An increase in the number of identified security incidents
B. A decrease in the number of security policy exceptions
C. A decrease in the number of security audit findings
D. An increase in the number of compliant business processes
Answer: (SHOW ANSWER)

NEW QUESTION: 110

Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?

A. Current resourcing levels

B. Information security strategy

C. Information security incidents

D. Availability of potential resources

Answer: (SHOW ANSWER)

NEW QUESTION: 111

Which of the following is MOST important to include in security incident escalation procedures?

A. Key objectives of the security program

B. Recovery procedures

C. Notification criteria

D. Containment procedures

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: 112

Who is BEST suited to determine how the information in a database should be classified?

A. Database analyst

B. Database administrator (DBA)

C. Information security analyst

D. Data owner

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: 113
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).
Answer: (SHOW ANSWER)
Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.
Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented. References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

NEW QUESTION: 114
Which of the following is CRITICAL to ensure the appropriate stakeholder makes decisions during a cybersecurity incident?
A. Stakeholder plan
B. Escalation plan
C. Up-to-date risk register
D. Asset classification
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
During a cybersecurity incident, it is vital to ensure that the right people are involved and that decision- making occurs promptly.
A). Stakeholder plan: While identifying stakeholders is important, it does not outline decision-making during an incident.
B). Escalation plan: This is the BEST answer because it specifies how incidents are escalated to the appropriate level of authority, ensuring timely and effective decisions.
C). Up-to-date risk register: Although useful for understanding risks, it does not facilitate decision-making in real-time incidents.
D). Asset classification: This helps identify critical assets but does not address decision-making protocols during an incident.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) highlights the importance of escalation procedures to manage incidents efficiently.

NEW QUESTION: 115
Which of the following should be the GREATEST concern for an information security manager when an annual audit reveals the organization's business continuity plan (BCP) has not been reviewed or updated in more than a year?
A. An outdated BCP may result in less efficient recovery if an actual incident occurs.
B. The organization may suffer reputational damage for not following industry best practices.
C. The audit finding may impact the overall risk rating of the organization.
D. The lack of updates to the BCP may result in noncompliance with internal policies.
Answer: (SHOW ANSWER)
A BCP is a document that outlines the processes and procedures to maintain or resume critical business functions and minimize the impact of a disruption on the organization's objectives, customers, and stakeholders. A BCP should be reviewed and updated regularly to reflect the changes in the organization's environment, risks, resources, and requirements. An outdated BCP may result in less efficient recovery if an actual incident occurs, as it may not account for the current situation, dependencies, priorities, or recovery strategies. This may lead to increased downtime, losses, or damages for the organization.
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 Plans

NEW QUESTION: 116
To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:
A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.
D. right to audit is included in the service level agreement (SLA).
Answer: (SHOW ANSWER)
= To confirm that a third-party provider complies with an organization's information security requirements, it is most important to ensure that the right to audit is included in the service level agreement (SLA), which is a contract that defines the scope, quality, and terms of the services that the third-party provider delivers to the organization. The right to audit is a clause that grants the organization the authority and opportunity to inspect and verify the third-party provider's security policies, procedures, controls, and performance, either by itself or by an independent auditor, at any time during the contract period or after a security incident. The right to audit can help to ensure that the third-party provider adheres to the organization's information security requirements, as well as to the legal and regulatory standards and obligations, and that the organization can monitor and measure the security risks and issues that arise from the outsourcing relationship. The right to audit can also help to identify and address any gaps, weaknesses, or errors that could compromise the security of the information assets and systems that are shared, stored, or processed by the third-party provider, and to provide feedback and recommendations for improvement and optimization of the security posture and performance. Security metrics, contract clauses, and the information security policy of the third-party provider are all important elements of ensuring the compliance of the third-party provider with the organization's information security requirements, but they are not the most important ones. Security metrics are quantitative and qualitative measures that indicate the effectiveness and efficiency of the security controls and processes that the third-party provider implements and reports to the organization, such as the number of security incidents, the time to resolve them, the level of customer satisfaction, or the compliance rate. Security metrics can help to evaluate and compare the security performance and outcomes of the third-party provider, as well as to identify and address any deviations or discrepancies from the expected or agreed levels. Contract clauses are legal and contractual terms and conditions that bind the third-party provider to the organization's information security requirements, such as the confidentiality, integrity, and availability of the information assets and systems, the roles and responsibilities of the parties, the liabilities and penalties for breach or violation, or the dispute resolution mechanisms. Contract clauses can help to enforce and protect the organization's information security interests and rights, as well as to prevent or resolve any conflicts or issues that arise from the outsourcing relationship. The information security policy of the third-party provider is a document that defines and communicates the third-party provider's security vision, mission, objectives, and principles, as well as the security roles, responsibilities, and rules that apply to the third-party provider's staff,

customers, and partners. The information security policy of the third-party provider can help to ensure that the third-party provider has a clear and consistent security direction and guidance, as well as to align and integrate the third- party provider's security practices and culture with the organization's security expectations and requirements. References = CISM Review Manual 15th Edition, pages 57-581; CISM Practice Quiz, question
1662

NEW QUESTION: 117
Which of the following documents should contain the INITIAL prioritization of recovery of services?
A. IT risk analysis
B. Threat assessment
C. Business impact analysis (BIA)
D. Business process map
Answer: (SHOW ANSWER)
A business impact analysis (BIA) is the document that should contain the initial priori-tization of recovery of services. A BIA is a process of identifying and analyzing the po-tential effects of disruptions to critical business functions and processes. A BIA typi-cally includes the following steps1:
*Identifying the critical business functions and processes that support the organization's mission and objectives.
*Estimating the maximum tolerable downtime (MTD) for each function or process, which is the longest time that the organization can afford to be without that function or process before suffering unacceptable consequences.
*Assessing the potential impacts of disruptions to each function or process, such as finan-cial losses, reputational damage, legal liabilities, regulatory penalties, customer dissatis-faction, etc.
*Prioritizing the recovery of functions or processes based on their MTDs and impacts, and assigning recovery time objectives (RTOs) and recovery point objectives (RPOs) for each function or process. RTOs are the target times for restoring functions or processes after a disruption, while RPOs are the acceptable amounts of data loss in case of a disruption.
*Identifying the resources and dependencies required for each function or process, such as staff, equipment, software, data, suppliers, customers, etc.
A BIA provides the basis for developing a business continuity plan (BCP), which is a document that outlines the strategies and procedures for ensuring the continuity or re-covery of critical business functions and processes in the event of a disruption2. The other options are not documents that should contain the initial prioritization of recov-ery of services. An IT risk analysis is a process of identifying and evaluating the threats and vulnerabilities that affect the IT systems and assets of an organization. It helps to determine the likelihood and impact of potential IT incidents, and to select and imple-ment appropriate controls to mitigate the risks3.
A threat assessment is a process of identifying and analyzing the sources and capabilities of adversaries that may pose a threat to an organization's security. It helps to determine the level of

threat posed by different actors, and to develop countermeasures to prevent or respond to attacks. A business process map is a visual representation of the activities, inputs, outputs, roles, and resources involved in a business process. It helps to understand how a process works, how it can be improved, and how it relates to other processes. References: 1:
Business impact analysis (BIA) - Wikipedia 2: Business continuity plan - Wikipedia 3: IT risk management - Wikipedia : Threat assessment - Wikipedia : Business process map-ping - Wikipedia

NEW QUESTION: 118
IT projects have gone over budget with too many security controls being added post-production. Which of the following would MOST help to ensure that relevant controls are applied to a project?
A. Involving information security at each stage of project management
B. Identifying responsibilities during the project business case analysis
C. Creating a data classification framework and providing it to stakeholders
D. Providing stakeholders with minimum information security requirements
Answer: (SHOW ANSWER)
The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post-production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

NEW QUESTION: 119
An organization plans to implement a new e-commerce operation in a highly regulated market. Which of the following is MOST important to consider when updating the risk management strategy?
A. Strategy of industry peers
B. Outsourcing needs
C. Business culture
D. Compliance requirements
Answer: (SHOW ANSWER)
When operating in a highly regulated market, compliance requirements become paramount, as failure to comply can lead to severe legal penalties, financial losses, and reputational harm. According to the CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Task 2, understanding and addressing legal, regulatory, and contractual requirements is critical in risk management, especially in regulated environments. This ensures that the risk management strategy is aligned with mandatory regulations and industry standards. Other factors (such as

outsourcing and business culture) are important, but compliance is the primary driver in highly regulated markets.
Reference:ISACA CISM Review Manual, 16th Edition, Page 120-122, "Legal, Regulatory and Contractual Requirements".

NEW QUESTION: 120

Which of the following should be the FIRST consideration when developing a strategy for protecting an organization's data?

A. Access monitoring
B. Access rights
C. Encryption
D. Classification
Answer: (SHOW ANSWER)

NEW QUESTION: 121

An online trading company discovers that a network attack has penetrated the firewall. What should be the information security manager's FIRST response?
A. Notify the regulatory agency of the incident.
B. Implement mitigating controls.
C. Examine firewall logs to identify the attacker.
D. Evaluate the impact to the business.
Answer: (SHOW ANSWER)

NEW QUESTION: 122

When properly implemented, secure transmission protocols protect transactions:
A. from eavesdropping.
B. from denial of service (DoS) attacks.
C. on the client desktop.
D. in the server's database.
Answer: A (LEAVE A REPLY)
Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on

the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information1. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party. Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage2. Therefore, secure transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures3. Some examples of secure transmission protocols are:

* Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.
* Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.
* Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port forwarding, which allows secure tunneling of other network services through SSH connections.

References = 1: 6 Network Security Protocols You Should Know | Cato Networks 2: Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL /TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec - Wikipedia : Secure Shell - Wikipedia

NEW QUESTION: 123

Which of the following will result in the MOST accurate controls assessment?

A. Mature change management processes

B. Senior management support

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

NEW QUESTION: 124
When analyzing the emerging risk and threat landscape, an information security manager should FIRST:
A. determine the sources of emerging threats.
B. review historical threats within the industry.
C. map threats to business assets.
D. determine the impact if threats materialize.
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which of the following is the BEST evidence of alignment between corporate and information security governance?
A. Security key performance indicators (KPIs)
B. Project resource optimization
C. Regular security policy reviews
D. Senior management sponsorship
Answer: (SHOW ANSWER)
Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the commitment and support of the top-level executives and board members for the information security program.
Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

NEW QUESTION: 126
The PRIMARY reason for creating a business case when proposing an information security project is to:
A. articulate inherent risks.
B. provide demonstrated return on investment (ROI).
C. establish the value of the project in relation to business objectives.
D. gain key business stakeholder engagement.
Answer: (SHOW ANSWER)
The primary reason for creating a business case when proposing an information security project is to establish the value of the project in relation to the business objectives and to justify the investment required. A business case should demonstrate how the project aligns with the organization's strategy, goals, and mission, and how it supports the business processes and functions. A business case should also include the expected benefits, costs, risks, and alternatives of the project, and provide a clear rationale for choosing the preferred option. References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 127
Which of the following is the MOST important reason for logging firewall activity?
A. Firewall tuning
B. Intrusion prevention
C. Metrics reporting
D. Incident investigation
Answer: (SHOW ANSWER)

NEW QUESTION: 128
An international organization with remote branches is implementing a corporate security policy for managing personally identifiable information (PII). Which of the following should be the information security manager's MAIN concern?
A. Local regulations
B. Data backup strategy
C. Consistency in awareness programs
D. Organizational reporting structure
Answer: (SHOW ANSWER)
Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the

applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

NEW QUESTION: 129
Which of the following is the MOST important reason for an information security manager to archive and retain the organization's electronic communication and email data?
A. To track personal use of electronic communication by users
B. To provide as evidence in legal proceedings when required
C. To meet the requirements of global security standards
D. To identify and scan attachments for malware
Answer: (SHOW ANSWER)
Retaining communications ensures the organization can produce evidence for litigation or regulatory investigations, which is often a legal obligation.
"Organizations must retain electronic communications to support legal discovery, compliance audits, and investigative needs."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Legal and Regulatory Requirements*

NEW QUESTION: 130
Which of the following should an information security manager do FIRST after a new cybersecunty regulation has been introduced?

A. Conduct a cost-benefit analysis.
B. Consult corporate legal counsel
C. Update the information security policy.
D. Perform a gap analysis.
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: 131

Which is MOST important to identify when developing an effective information security strategy?
A. Security awareness training needs
B. Potential savings resulting from security governance
C. Business assets to be secured
D. Residual risk levels
Answer: C (LEAVE A REPLY)
Business assets are the resources that enable the organization to achieve its objectives and create value.
Identifying the business assets to be secured is the most important step in developing an effective information security strategy, as it helps to align the security goals with the business goals, prioritize the security efforts and resources, and define the scope and boundaries of the security program. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 27, section 1.2.1.

NEW QUESTION: 132
Which of the following is MOST important to include in an information security strategy?
A. Stakeholder requirements
B. Risk register
C. Industry benchmarks
D. Regulatory requirements
Answer: (SHOW ANSWER)
Stakeholder requirements are the most important to include in an information security strategy, as they reflect the business needs, objectives, and expectations of the organization and its key stakeholders. Stakeholder requirements also help to align the information security strategy with the enterprise governance and the organizational culture. Risk register, industry benchmarks, and regulatory requirements are important inputs for the information security strategy, but they are not the most important to include.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Task 1.12

NEW QUESTION: 133
Which of the following is the BEST control to protect customer personal information that is stored in the cloud?
A. Timely deletion of digital records
B. Appropriate data anonymization
C. Strong encryption methods
D. Strong physical access controls
Answer: (SHOW ANSWER)
Strong encryption methods are the BEST control to protect customer personal information that is stored in the cloud, because they help to prevent unauthorized access, disclosure, modification,

or deletion of the data by encrypting it at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data. Encryption can help to protect the confidentiality, integrity, and availability of the data, as well as to comply with legal and regulatory requirements.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Encryption is the process of transforming data into an unreadable format using a secret key or algorithm." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Encryption can help to protect the confidentiality, integrity, and availability of data, as well as to comply with legal and regulatory requirements for data protection." Saas Data Security: Protecting Your Customers' Information In The Cloud - Fresent's Blog: "Encryption and Data Protection: One of the most effective ways to protect sensitive data in the cloud is to encrypt it both at rest and in transit. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can decrypt and access the data."

NEW QUESTION: 134
An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?
A. Conduct an internal audit.
B. Conduct penetration testing.
C. Perform a vulnerability assessment.
D. Prepare compensating controls.
Answer: (SHOW ANSWER)
After implementing controls, performing a vulnerability assessment is the best way to verify that all previously identified weaknesses have been addressed. The CISM Review Manual specifies that vulnerability assessments systematically scan for known vulnerabilities and confirm remediation effectiveness. Penetration testing is valuable but is typically used to exploit vulnerabilities, not comprehensively verify their remediation as efficiently as vulnerability assessments.
Reference:ISACA CISM Review Manual, 16th Edition, Page 164-165, "Vulnerability Management and Assessment".

NEW QUESTION: 135
Which of the following BEST enables an organization to operate smoothly with reduced capacities when service has been disrupted?
A. Crisis management plan
B. Disaster recovery plan (DRP)
C. Incident response plan
D. Business continuity plan (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: 136

Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA

B. To increase awareness of information security among key stakeholders

C. To ensure the stakeholders providing input own the related risk

D. To obtain input from as many relevant stakeholders as possible

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: 137
A security incident has been reported within an organization When should an information security manager contact the information owner?
A. After the incident has been mitigated
B. After the incident has been confirmed.
C. After the potential incident has been togged
D. After the incident has been contained
Answer: (SHOW ANSWER)
= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated. The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

NEW QUESTION: 138
Which of the following presents the GREATEST challenge to a large multinational organization using an automated identity and access management (1AM) system?
A. Large number of applications in the organization
B. Frequent changes to user roles during employment
C. Inaccurate workforce data from human resources (HR)
D. Staff turnover rates that significantly exceed industry averages
Answer: (SHOW ANSWER)

NEW QUESTION: 139
The effectiveness of an incident response team will be GREATEST when:
A. the incident response team members are trained security personnel,
B. incidents are identified using a security information and event monitoring (SIEM) system.
C. the incident response process is updated based on lessons learned,

D. the incident response team meets on a regular basis to review log files

Answer: (SHOW ANSWER)

NEW QUESTION: 140

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

A. Legal

B. Information security

C. Help desk

D. Human resources (HR)

Answer: (SHOW ANSWER)

Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner." SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process." IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access."

Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets.

HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

NEW QUESTION: 141

Which of the following is the PRIMARY impact of organizational culture on the effectiveness of an information security program?

A. The culture shapes behaviors toward information security.
B. The culture defines responsibilities necessary for program implementation.
C. The culture helps determine budget for information security controls.
D. The culture has minimal impact as long as information security controls are adhered to.
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: 142
Which of the following BEST helps to ensure the effective execution of an organization's disaster recovery plan (DRP)?
A. The plan is reviewed by senior and IT operational management.
B. The plan is based on industry best practices.
C. Process steps are documented by the disaster recovery team.
D. Procedures are available at the primary and failover location.
Answer: D (LEAVE A REPLY)
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: 143
Which of the following BEST indicates the effectiveness of the vendor risk management process?
A. Increase in the percentage of vendors certified to a globally recognized security standard
B. Increase in the percentage of vendors with a completed due diligence review
C. Increase in the percentage of vendors conducting mandatory security training
D. Increase in the percentage of vendors that have reported security breaches
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: 144
Which of the following is the MOST essential element of an information security program?
A. Benchmarking the program with global standards for relevance
B. Prioritizing program deliverables based on available resources
C. Involving functional managers in program development
D. Applying project management practices used by the business
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: 145
Which of the following is MOST important for building 4 robust information security culture within an organization?
A. Mature information security awareness training across the organization
B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies
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: 146
A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated FIRST?
A. Local regulatory requirements

B. Training requirements of the framework
C. Cross-border data mobility
D. Global framework standards
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which of the following should be the PRIMARY focus for an information security manager when reviewing access controls for data stored in an off-premise cloud environment?
A. Reviewing and updating access controls in response to changes in organizational structure
B. Implementing strong password policies and enforcing regular password changes
C. Ensuring access is granted to only those individuals whose job functions require it
D. Implementing strong encryption protocols to protect sensitive data
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: 148
Which of the following BEST helps to ensure a risk response plan will be developed and executed in a timely manner?
A. Establishing risk metrics
B. Training on risk management procedures
C. Reporting on documented deficiencies
D. Assigning a risk owner
Answer: D (LEAVE A REPLY)
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: 149
Which of the following events is MOST likely to require an organization to revisit its information security framework?
A. New services offered by IT
B. Changes to the risk landscape
C. A recent cybersecurity attack
D. A new technology implemented
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: 150
Data classification is PRIMARILY the responsibility of:
A. the security manager.
B. the data custodian.
C. senior management.
D. the data owner.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Network isolation techniques are immediately implemented after a security breach to:
A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.
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: 152
An information security manager learns that business unit leaders are encouraging increased use of social media platforms to reach customers. Which of the following should be done FIRST to help mitigate the risk of confidential information being disclosed by employees on social media?
A. Establish an organization-wide social media policy.
B. Develop sanctions for misuse of social media sites.
C. Monitor social media sites visited by employees.
D. Restrict social media access on corporate devices.
Answer: (SHOW ANSWER)
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: 153

An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?

A. Include security requirements in the contract

B. Assess security controls.

C. Perform a risk assessment

D. Review data architecture.

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: 154

Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?

A. Defining information stewardship roles

B. Defining security asset categorization

C. Assigning information asset ownership

D. Developing a records retention schedule

Answer: (SHOW ANSWER)

The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section:

Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

NEW QUESTION: 155
Which of the following would be the GREATEST obstacle to implementing incident notification and escalation processes in an organization with high turnover?
A. Lack of communication processes
B. Lack of process documentation
C. Lack of alignment with organizational goals
D. Lack of knowledgeable personnel
Answer: (SHOW ANSWER)

NEW QUESTION: 156
The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:
A. the organization has the required funds to implement the plan.
B. compliance with legal and regulatory requirements.
C. staff participation in information security efforts.
D. the plan aligns with corporate governance.
Answer: (SHOW ANSWER)
The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly1. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization2. The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives3. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation4. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253:
CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA,
2017, page 27.
Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION: 157
What should be an information security manager's MOST important consideration when developing a multi- year plan?
A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year
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: 158
Which of the following is the BEST course of action when using a web application that has known vulnerabilities?
A. Install anti-spyware software.
B. Deploy an application firewall.
C. Monitor application level logs.
D. Deploy host-based intrusion detection.
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?
A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Business contingency plan
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: 160

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

A. Internal security audit
B. External security audit
C. Organizational risk appetite
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

NEW QUESTION: 161
Which of the following should be an information security manager's FIRST course of action when a newly introduced privacy regulation affects the business?
A. Consult with IT staff and assess the risk based on their recommendations
B. Update the security policy based on the regulatory requirements
C. Propose relevant controls to ensure the business complies with the regulation
D. Identify and assess the risk in the context of business objectives

Answer: (SHOW ANSWER)
Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

NEW QUESTION: 162
Which of the following is the BEST way to obtain support for a new organization-wide information security program?
A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.
Answer: D (LEAVE A REPLY)
= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by:
Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.
Establishing roles and responsibilities for the security program and ensuring accountability and ownership.
Securing adequate resources and budget for the security program and allocating them appropriately.
Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.
Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.
Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges.
Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the

support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.
Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization. An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.
Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication, confusion, or conflict. However, a RACI chart does not ensure the support or commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders.
References = CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112
Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition
- ISACA1
Information Security Strategy: The Key to Success - ISACA2
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

NEW QUESTION: 163
Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?
A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes

C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards
Answer: (SHOW ANSWER)
A service provider is a third-party supplier that provides IT services or products to an organization. A service provider should comply with the organization's information security requirements, such as policies, standards, procedures, and controls, to ensure the confidentiality, integrity, and availability of the organization's data and systems. The best way to provide an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements is to have the ability to audit the third-party supplier's IT systems and processes. An audit is a systematic and independent examination of evidence to determine the degree of conformity to predetermined criteria. An audit can verify the effectiveness and efficiency of the service provider's security controls, identify any gaps or weaknesses, and provide recommendations for improvement. An audit can also ensure that the service provider adheres to the contractual obligations and service level agreements (SLAs) with the organization. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a live demonstration of the third-party supplier's security capabilities may not be comprehensive, objective, or reliable. A live demonstration may only show the positive aspects of the service provider's security, but not reveal any hidden or potential issues. A live demonstration may also be subject to manipulation or deception by the service provider.
Option C is not the best answer because third-party security control self-assessment (CSA) results may not be accurate, complete, or consistent. A self-assessment is a process where the service provider evaluates its own security controls against a set of criteria or standards. A self-assessment may be biased, subjective, or incomplete, as the service provider may not disclose or report all the relevant information or issues. A self- assessment may also vary in quality and scope depending on the service provider's expertise, resources, and methodology.
Option D is not the best answer because an independent review report indicating compliance with industry standards may not be sufficient or specific for the organization's information security requirements. An independent review is a process where an external party evaluates the service provider's security controls against a set of industry standards or best practices, such as ISO/IEC 27001, NIST CSF, PCI DSS, etc. An independent review report may provide a general overview of the service provider's security posture, but not address the organization's unique or specific security needs, risks, or expectations. An independent review report may also be outdated, limited, or generic, as the industry standards or best practices may not reflect the current or emerging security threats or trends. References = CISM Review Manual 15th Edition1, pages 257-
258; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 301.
An independent review report indicating compliance with industry standards BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is

an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

NEW QUESTION: 164
Which of the following would be MOST helpful when creating information security policies?
A. The information security framework
B. Business impact analysis (BIA)
C. Information security metrics
D. Risk assessment results
Answer: (SHOW ANSWER)
The information security framework is a set of principles, standards, guidelines, and best practices that define the scope, objectives, and requirements for information security in an organization. The information security framework is most helpful when creating information security policies because it provides a consistent and coherent approach to managing information security risks, aligning with business goals and strategy, and complying with relevant laws and regulations. The information security framework also helps to establish the roles, responsibilities, and accountability of all stakeholders involved in information security governance, management, and operations.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1:
Information Security Framework2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1

NEW QUESTION: 165
The PRIMARY objective of a post-incident review of an information security incident is to:
A. update the risk profile
B. minimize impact
C. prevent recurrence.
D. determine the impact
Answer: (SHOW ANSWER)
post-incident review of an information security incident is a process that aims to identify the root causes, contributing factors, and lessons learned from the incident, and to implement corrective and preventive actions to avoid or mitigate similar incidents in the future. The primary objective of a post-incident review is to prevent recurrence, as it helps to improve the security posture, awareness, and resilience of the organization. Preventing recurrence also helps to reduce the impact and cost of future incidents, as well as to enhance the reputation and trust of the organization. Updating the risk profile, minimizing impact, and determining the impact are not the primary objectives of a post-incident review, although they may be part of its outcomes or outputs.
References = CISM Review Manual, 16th Edition, page 1011

NEW QUESTION: 166
Management has announced the acquisition of a new company. The information security manager of the parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies. To BEST address this concern, the information security manager should:
A. review access rights as the acquisition integration occurs.
B. perform a risk assessment of the access rights.
C. escalate concerns for conflicting access rights to management.
D. implement consistent access control standards.
Answer: (SHOW ANSWER)
Performing a risk assessment of the access rights is the best way to address the concern of conflicting access rights during the integration of two companies. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the access rights of both companies, as well as the potential impact and likelihood of information exposure. A risk assessment will also provide a basis for selecting and evaluating the controls to mitigate the risks. According to NIST, a risk assessment is an essential component of risk management and should be performed before implementing any security controls1. The other options are not the best ways to address the concern of conflicting access rights during the integration of two companies, but rather possible subsequent actions based on the risk assessment. Reviewing access rights as the acquisition integration occurs may be too late or too slow to prevent information exposure. Escalating concerns for conflicting access rights to management may not be effective without evidence or recommendations from a risk assessment. Implementing consistent access control standards may not be feasible or desirable for different systems or business units. References: 1: NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments 2: M&A integration strategy is crucial for deal success but remains difficult: PwC 3: The 10 steps to successful M&A integration | Bain & Company : Cracking the code to successful post-merger integration

NEW QUESTION: 167
Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?
A. Applying global security standards to the IT projects

B. Having the information security manager participate on the project steering committees
C. Training project managers on risk assessment
D. Integrating the risk assessment into the internal audit program
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which type of recovery site is MOST reliable and can support stringent recovery requirements?
A. Cold site
B. Warm site
C. Hot site
D. Mobile site
Answer: (SHOW ANSWER)
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: 169
Of the following, who should be assigned as the owner of a newly identified risk related to an organization's new payroll system?
A. Data privacy officer
B. Head of IT department
C. Head of human resources (HR)
D. Information security manager
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
Which of the following is the PRIMARY preventive method to mitigate risks associated with privileged accounts?

A. Provide privileged account access only to users who need it.

B. Perform periodic certification of access to privileged accounts.
C. Frequently monitor activities on privileged accounts.
D. Eliminate privileged accounts.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 171
An organization has acquired a new system with strict maintenance instructions and schedules. Where should this information be documented?
A. Standards
B. Policies
C. Guidelines
D. Procedures
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: 172
A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?
A. Automated controls
B. Security policies
C. Guidelines
D. Standards
Answer: (SHOW ANSWER)
Standards are the most important thing to review, as they define the specific and mandatory requirements for setting up new user accounts, such as the naming conventions, access rights, password policies, and expiration dates. Standards help to ensure consistency, security, and compliance across the organization's information systems and users. If the standards are not followed, the organization may face increased risks of unauthorized access, data breaches, or audit failures.
References = CISM Review Manual 2022, page 341; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.32; CISM 2020: IT Security Policies; Information Security Policy, Standards, and Guidelines

NEW QUESTION: 173
Which of the following is the BEST starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities?
A. Controls analysis
B. Emerging risk review
C. Penetration testing
D. Traffic monitoring
Answer: (SHOW ANSWER)
The best starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities is C. Penetration testing. This is because penetration testing is a method of simulating real-world attacks on a network to evaluate its security posture and identify any weaknesses or gaps that could be exploited by malicious actors. Penetration testing can help the information security manager to assess the effectiveness of the existing controls, prioritize the remediation efforts, and demonstrate compliance with the relevant standards and regulations. Penetration testing can also provide valuable insights into the network architecture, configuration, and behavior, as well as the potential impact and likelihood of different types of attacks.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 50, page 14

NEW QUESTION: 174
A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?
A. Mitigate
B. Accept
C. Transfer
D. Avoid
Answer: A (LEAVE A REPLY)
Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures.
A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched.
Therefore, mitigate is the correct answer.
References:
https://simplicable.com/risk/risk-treatment
https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk- treatment.

NEW QUESTION: 175
Which type of backup BEST enables an organization to recover data after a ransomware attack?
A. Online backup
B. Incremental backup
C. Differential backup
D. Offline backup
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Recovering from ransomware requires backups that are unaffected by the ransomware attack. Here's why offline backups are most effective:
A). Online backup: These are connected to the network and may also be compromised during an attack.
B). Incremental backup: While efficient, incremental backups rely on previous backups and are typically stored online, making them vulnerable to ransomware.
C). Differential backup: Similar to incremental backups, these are not immune if stored online or on compromised systems.
D). Offline backup: This is the BEST choice as offline backups are stored in a location that is not connected to the network, preventing ransomware from encrypting them.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) includes guidance on establishing robust backup strategies for recovery.

NEW QUESTION: 176
Which of the following is the BEST course of action after management has reviewed an identified risk and determines the risk is below the defined risk appetite?
A. Accept
B. Avoid
C. Transfer
D. Mitigate
Answer: (SHOW ANSWER)
When a risk is determined to be below the organization's risk appetite, the most appropriate course of action is to formally accept the risk. Risk acceptance is a valid and cost-effective strategy when the impact and likelihood are within acceptable limits, and the cost of mitigation outweighs the potential loss.
"Risk acceptance is an appropriate response when the level of residual risk is within the organization's defined risk tolerance and appetite."
- CISM Review Manual 15th Edition, Chapter 2: Risk Response and Mitigation* Avoidance, transfer, or mitigation may be overreactions that waste resources in this context.

NEW QUESTION: 177
In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?
A. Access to the hardware
B. Non-standard event logs
C. Compressed customer data
D. Data encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 178
Which of the following is the PRIMARY objective of a cyber resilience strategy?
A. Business continuity
B. Regulatory compliance
C. Employee awareness
D. Executive support
Answer: (SHOW ANSWER)
Business continuity is the primary objective of a cyber resilience strategy, as it aims to ensure that the organization can continue to deliver its essential products and services in the face of cyber disruptions, and recover to normal operations as quickly and effectively as possible. A cyber resilience strategy should align with the business continuity plan and support the organization's mission, vision, and values. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

NEW QUESTION: 179
Which of the following is MOST important to consider when choosing a shared alternate location for computing facilities?
A. The organization's risk tolerance
B. The organization's mission
C. Resource availability
D. Incident response team training
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: 180

Which of the following is the BEST way to achieve compliance with new global regulations related to the protection of personal information?

A. Execute a risk treatment plan.

B. Review contracts and statements of work (SOWs) with vendors.

C. Implement data regionalization controls.

D. Determine current and desired state of controls.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 181

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

A. Security maturity assessment results

B. Threat analysis of the organization's environment

C. Results of vulnerability assessments

D. External penetration test findings

Answer: (SHOW ANSWER)

A security maturity assessment evaluates not only current vulnerabilities but also governance structures, risk management practices, incident response, and ongoing improvement processes. It provides a holistic and strategic view of the security posture.

"Maturity assessments provide a comprehensive evaluation of an organization's security controls and their alignment with business objectives."

- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Maturity Models* Other methods like penetration tests or vulnerability assessments offer snapshots of technical weaknesses, but they lack strategic depth.

NEW QUESTION: 182
Which of the following is MOST important to determine following the discovery and eradication of a malware attack?
A. The method of detecting the malware
B. The malware entry path
C. The type of malware involved
D. The creator of the malware
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following BEST helps to enable the desired information security culture within an organization?
A. Information security awareness training and campaigns
B. Effective information security policies and procedures
C. Delegation of information security roles and responsibilities
D. Incentives for appropriate information security-related behavior
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: 184
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. Perform a risk assessment
B. Perform a gap analysis
C. Review information security policies

D. Review the state of security awareness

Answer: (SHOW ANSWER)

During due diligence, performing a risk assessment is critical to understanding the potential impact of integrating the new organization into the acquiring company. This includes evaluating inherited risks, compliance gaps, and technical vulnerabilities.

"As part of due diligence during mergers and acquisitions, it is crucial to assess risks associated with the target organization to ensure proper integration and continuity."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Due Diligence

ISACA's CISM practice database reinforces that identifying and quantifying risks early helps ensure appropriate controls are in place before the integration, making risk assessment the most critical activity.

NEW QUESTION: 185

Which of the following is ESSENTIAL to ensuring effective incident response?

A. Business continuity plan (BCP)

B. Cost-benefit analysis

C. Classification scheme

D. Senior management support

Answer: (SHOW ANSWER)

Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.

The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality.

References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

NEW QUESTION: 186

Which of the following would BEST justify continued investment in an information security program?

A. Reduction in residual risk

B. Security framework alignment

C. Speed of implementation
D. Industry peer benchmarking
Answer: (SHOW ANSWER)
Residual risk is the risk that remains after implementing controls to mitigate the inherent risk. A reduction in residual risk indicates that the information security program is effective in managing the risks to an acceptable level. This would best justify the continued investment in the program, as it demonstrates the value and benefits of the security activities. Security framework alignment, speed of implementation, and industry peer benchmarking are not direct measures of the effectiveness or value of the information security program. They may be useful for comparison or compliance purposes, but they do not necessarily reflect the impact of the program on the risk profile of the organization. References = CISM Review Manual, 16th Edition, page 431; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 622 Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

NEW QUESTION: 187
A technical vulnerability assessment on a personnel information management server should be performed when:
A. the data owner leaves the organization unexpectedly.
B. changes are made to the system configuration.
C. the number of unauthorized access attempts increases.
D. an unexpected server outage has occurred.
Answer: (SHOW ANSWER)
A technical vulnerability assessment is a process of identifying and evaluating the weaknesses and risks associated with a specific system, component, or network. A technical vulnerability assessment can help to determine the potential impact and likelihood of a security breach, as well as the appropriate measures to prevent or mitigate it. A technical vulnerability assessment should be performed on a personnel information management server whenever there is an increase in the number of unauthorized access attempts to the server, as this indicates that the server may have been compromised or targeted by an attacker12. Therefore, option C is the correct answer. References = CISM Review Manual (Digital Version), Chapter 5: Information Security Program Management CISM Review Manual (Print Version), Chapter 5: Information Security Program Management

NEW QUESTION: 188
Which of the following is the BEST indication of a mature information security program?
A. Security incidents are managed properly.
B. Security spending is below budget.
C. Security resources are optimized.

D. Security audit findings are reduced.

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: 189

Which of the following risk responses is an example of risk transfer?

A. Utilizing third-party applications

B. Purchasing cybersecurity insurance

C. Moving risk ownership to another department

D. Conducting off-site backups

Answer: (SHOW ANSWER)

Risk transfer involves shifting the impact or financial consequences of a risk to a third party. Purchasing cybersecurity insurance is the most common example, where the organization pays a premium to a provider who assumes certain financial responsibilities in the event of a security incident.

Other options listed do not transfer risk:

A). Using third-party applications may introduce new risks, not transfer existing ones.

C). Moving ownership within the organization is reassignment, not transfer.

D). Off-site backups are a form of risk mitigation, not transfer.

"Risk transfer shifts the financial consequences of a risk to another entity, typically through insurance or contractual arrangements."

- CISM Review Manual 15th Edition, Chapter 2: Risk Management, Section: Risk Treatment Options* Example: "An organization may transfer the financial impact of a potential data breach through the purchase of cyber insurance."

NEW QUESTION: 190

An employee of an organization has reported losing a smartphone that contains sensitive information The BEST step to address this situation is to:

A. disable the user's access to corporate resources.

B. terminate the device connectivity.

C. remotely wipe the device

D. escalate to the user's management

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: 191
Which type of plan is PRIMARILY intended to reduce the potential impact of security events that may occur?
A. Incident response plan
B. Security awareness plan
C. Business continuity plan (BCP)
D. Disaster recovery plan (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 192
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?
A. Inform the public relations officer.
B. Monitor the third party's response.
C. Invoke the incident response plan.
D. Inform customers of the breach.
Answer: (SHOW ANSWER)
The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.
References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

NEW QUESTION: 193

An organization is considering using a third party to host sensitive archived data. Which of the following is MOST important to verify before entering into the relationship?
A. The vendor's data centers are in the same geographic region.
B. The encryption keys are not provisled to the vendor.
C. The vendor's controls are in line with the organization's security standards.
D. Independent audits of the vendor's operations are regularly conducted.
Answer: C (LEAVE A REPLY)
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: 194
Which of the following should be the PRIMARY objective of an information security governance framework?
A. Provide a baseline for optimizing the security profile of the organization.
B. Demonstrate senior management commitment.
C. Demonstrate compliance with industry best practices to external stakeholders.
D. Ensure that users comply with the organization's information security policies.
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: 195

Which of the following is the MOST effective way to prevent information security incidents?
A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment
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: 196
Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?
A. Include security requirements in the contract.
B. Update the risk register.
C. Consult with the business owner.
D. Restrict application network access temporarily.
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: 197
Which of the following roles is MOST appropriate to determine access rights for specific users of an application?
A. Data owner
B. Data custodian
C. System administrator
D. Senior management
Answer: A (LEAVE A REPLY)
The data owner is the most appropriate role to determine access rights for specific users of an application because they have legal rights and complete control over data elements4. They are also responsible for approving data glossaries and definitions, ensuring the accuracy of information, and supervising operations related to data quality5. The data custodian is responsible for the safe custody, transport, and storage of the data and implementation of business rules, but not for determining access rights4. The system administrator is responsible for managing the security and storage infrastructure of data sets according to the organization's data governance policies, but not for determining access rights5. Senior management is responsible for setting the strategic direction and priorities for data governance, but not for determining access rights5.
References: 5 https://www.cpomagazine.com/cyber-security/data-owners-vs-data-stewards-vs-data- custodians-the-3-types-of-data-masters-and-why-you-should-employ-them/ 4 https://cloudgal42.com/data- privacy-difference-between-data-owner-controller-and-data-custodian-processor/

NEW QUESTION: 198
An organization is performing due diligence when selecting a third party. Which of the following is MOST helpful to reduce the risk of unauthorized sharing of information during this process?
A. Using secure communication channels
B. Establishing mutual non-disclosure agreements (NDAs)

C. Requiring third-party privacy policies
D. Obtaining industry references
Answer: (SHOW ANSWER)
The best option to reduce the risk of unauthorized sharing of information during the due diligence process is B). Establishing mutual non-disclosure agreements (NDAs). This is because NDAs are legal contracts that bind the parties to keep confidential any information that is exchanged or disclosed during the due diligence process. NDAs can help to protect the sensitive data, intellectual property, trade secrets, or business strategies of both the organization and the third party from being leaked, stolen, or misused by unauthorized parties.
NDAs can also specify the terms and conditions for the use, storage, and disposal of the information, as well as the consequences for breaching the agreement.
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 70, page 18

NEW QUESTION: 199
Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?
A. Determine the final root cause of the incident.
B. Remove all instances of the incident from the network.
C. Mitigate exploited vulnerabilities to prevent future incidents.
D. Isolate affected systems to prevent the spread of damage.
Answer: (SHOW ANSWER)
Isolating affected systems limits the damage and prevents the incident from impacting other parts of the organization.
"During containment, the primary objective is to isolate affected systems to prevent further damage."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Incident Response Process*

NEW QUESTION: 200
Which of the following MUST be established to maintain an effective information security governance framework?

A. Security controls automation
B. Defined security metrics
C. Change management processes
D. Security policy provisions
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: 201
Which of the following has the GREATEST impact on the effectiveness of an organization's security posture?
A. Incident metrics are frequently compared against industry benchmarks
B. New hires are mandated to attend security training
C. Security is embedded in organizational culture
D. Senior management has approved and endorsed security practices
Answer: (SHOW ANSWER)
When security is embedded in organizational culture, it becomes a shared responsibility, increasing adherence and effectiveness.
"A security-aware culture is a key component of an effective security program because it encourages responsible behavior and supports ongoing risk management."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Culture ISACA's practice questions identify security culture as the foundational element impacting the organization's entire security posture.

NEW QUESTION: 202
Which of the following provides the MOST comprehensive insight into ongoing threats facing an organization?
A. Business impact analysis (BIA)
B. Risk register
C. Penetration testing
D. Vulnerability assessment
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: 203
Which of the following BEST enables an organization to enhance its incident response plan processes and procedures?
A. Security risk assessments
B. Lessons learned analysis
C. Information security audits
D. Key performance indicators (KPIs)
Answer: (SHOW ANSWER)
Lessons learned analysis is the best way to enable an organization to enhance its incident response plan processes and procedures because it helps to identify the strengths and weaknesses of the current plan, capture the feedback and recommendations from the incident

responders and stakeholders, and implement the necessary improvements and corrective actions for future incidents. Security risk assessments are not directly related to enhancing the incident response plan, but rather to identifying and evaluating the security risks and controls of the organization. Information security audits are not directly related to enhancing the incident response plan, but rather to verifying and validating the compliance and effectiveness of the security policies and standards of the organization. Key performance indicators (KPIs) are not directly related to enhancing the incident response plan, but rather to measuring and reporting the performance and progress of the security objectives and initiatives of the organization.
References: https://www.isaca.org/resources/isaca-journal/issues /2017/volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2017 /volume-1/security-risk-assessment-for-a-cloud-based-enterprise-resource-planning-system https://www.isaca. org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security- using-iso-27004 https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the- effectiveness-of-your-information-security-management-system

NEW QUESTION: 204
Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?
A. Metrics to drive the information security program
B. Information security policies
C. A defined security organizational structure
D. An information security strategy
Answer: D (LEAVE A REPLY)
An information security strategy is the most important element to have in place as a basis for developing an effective information security program that supports the organization's business goals. An information security strategy is a high-level plan that defines the vision, mission, objectives, scope, and principles of information security for the organization1. It also aligns the information security program with the organization's strategy, culture, risk appetite, and governance framework2. An information security strategy provides the direction, guidance, and justification for the information security program, and ensures that the program is consistent, coherent, and comprehensive3. An information security strategy also helps to prioritize the information security initiatives, allocate the resources, and measure the performance and value of the information security program4.
The other options are not as important as an information security strategy, because they are either derived from or dependent on the strategy. Metrics are used to drive the information security program, but they need to be based on the strategy and aligned with the goals and objectives of the program. Information security policies are the rules and standards that implement the information security strategy and define the expected behavior and responsibilities

of the stakeholders. A defined security organizational structure is the way the information security roles and functions are organized and coordinated within the organization, and it should reflect the strategy and the governance model. References = 1: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 2: CISM Review Manual 15th Edition, Chapter 1, Section 1.2 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 4: CISM Review Manual 15th Edition, Chapter 1, Section 1.4 : CISM Review Manual 15th Edition, Chapter 1, Section 1.5 : CISM Review Manual 15th Edition, Chapter 1, Section 1.6 :
CISM Review Manual 15th Edition, Chapter 1, Section 1.7

NEW QUESTION: 205
Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:
A. a function of the likelihood and impact, should a threat exploit a vulnerability.
B. the magnitude of the impact, should a threat exploit a vulnerability.
C. a function of the cost and effectiveness of controls over a vulnerability.
D. the likelihood of a given threat attempting to exploit a vulnerability
Answer: (SHOW ANSWER)
= According to the CISM Manual1, risk is defined as the combination of the probability of an event and its consequence. Therefore, determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as a function of the likelihood and impact, should a threat exploit a vulnerability.
Likelihood is the probability or frequency of a threat occurring, while impact is the magnitude or severity of the harm or loss that would result from a threat exploiting a vulnerability. The higher the likelihood and impact, the higher the risk. The lower the likelihood and impact, the lower the risk.
The other options are not correct because they do not capture the full expression of risk. Option B only considers the impact, but not the likelihood, of a threat exploiting a vulnerability. Option C confuses the risk with the risk response, which is the action taken to reduce or mitigate the risk. Option D only considers the likelihood, but not the impact, of a threat attempting to exploit a vulnerability.
References = CISM Manual1, Chapter 2: Information Risk Management (IRM), Section 2.1: Risk Concepts2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 2

NEW QUESTION: 206
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.

Answer: (SHOW ANSWER)
= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =
1: CISM Review Manual 15th Edition, page 199-2004
2: CISM Practice Quiz, question 1011
3: Computer Security Incident Handling Guide5, page 2-3

NEW QUESTION: 207
Which of the following is the BEST way to compete for funding for an information security program in an organization with limited resources?
A. Demonstrate the effectiveness of business continuity plans (BCPs).
B. Report key performance indicator (KPI) trends.
C. Demonstrate that the program enables business activities.
D. Provide evidence of increased security events at peer organizations.
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: 208

Which of the following BEST enables an organization to maintain an appropriate security control environment?

A. Alignment to an industry security framework

B. Budgetary support for security

C. Periodic employee security training

D. Monitoring of the threat landscape

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: 209

An information security manager is alerted to multiple security incidents across different business units, with unauthorized access to sensitive data and potential data exfiltration from critical systems. Which of the following is the BEST course of action to appropriately classify and prioritize these incidents?

A. Assemble the incident response team to evaluate the incidents

B. Initiate the crisis communication plan to notify stakeholders of the incidents

C. Engage external incident response consultants to conduct an independent investigation

D. Prioritize the incidents based on data classification standards

Answer: D (LEAVE A REPLY)

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: 210

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Establish performance metrics for the team

B. Perform a post-incident review

C. Implement a SIEM solution

D. Perform a threat analysis

Answer: (SHOW ANSWER)

Performing a post-incident review (also known as a lessons-learned session) is the best way to ensure similar incidents are identified and addressed more efficiently in the future. This review

helps in understanding what went wrong, what went right, and how processes can be improved. The knowledge gained from the review can be incorporated into incident response plans and training.
"Post-incident reviews help determine root causes, assess the effectiveness of the response, and identify opportunities for improvement."
- CISM Review Manual 15th Edition, Chapter 4: Incident Management, Section: Post-incident Analysis Additionally, the ISACA CISM Practice Question Database emphasizes that post-incident reviews are essential for improving future response times and understanding patterns of threats.

NEW QUESTION: 211
Which of the following is the BEST reason to implement an information security architecture?
A. Serve as a post-deployment information security road map.
B. Assess the cost-effectiveness of the integration.
C. Fast-track the deployment of information security components.
D. Facilitate consistent implementation of security requirements.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 212
Which of the following should be done FIRST when a SIEM flags a potential event?
A. Validate the event is not a false positive.
B. Initiate the incident response plan.
C. Escalate the event to the business owner.
D. Implement compensating controls.
Answer: (SHOW ANSWER)
The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls.

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

NEW QUESTION: 213
Which of the following would provide the MOST effective security outcome in an organizations contract management process?
A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage
B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage
C. Extending security assessment to cover asset disposal on contract termination
D. Extending security assessment to include random penetration testing
Answer: (SHOW ANSWER)
Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves comparing and ranking different vendors or service providers based on their security capabilities or performance. Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

NEW QUESTION: 214
A data discovery project uncovers an unclassified process document. Of the following, who is BEST suited to determine the classification?
A. Security policy author
B. Information security manager
C. Data custodian

D. Creator of the document
Answer: (SHOW ANSWER)

NEW QUESTION: 215
Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?
A. Risk assessment
B. Business impact analysis (BIA)
C. Penetration test results
D. Vulnerability scan results
Answer: A (LEAVE A REPLY)
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: 216
A new application has entered the production environment with deficient technical security controls. Which of the following is MOST Likely the root cause?
A. Inadequate incident response controls
B. Lack of legal review
C. Inadequate change control
D. Lack of quality control
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: 217
Which of the following metrics provides the BEST evidence of alignment of information security governance with corporate governance?

A. Average return on investment (ROI) associated with security initiatives
B. Average number of security incidents across business units
C. Mean time to resolution (MTTR) for enterprise-wide security incidents
D. Number of vulnerabilities identified for high-risk information assets
Answer: A (LEAVE A REPLY)
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: 218
The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:
A. the internal audit manager.
B. the information security officer.
C. the steering committee.
D. the board of directors.
Answer: (SHOW ANSWER)
The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework. References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 219
Which type of policy BEST helps to ensure that all employees, contractors, and third-party users receive formal communication regarding an organization's security program?

A. Management review policy
B. Business continuity management policy
C. Information security training policy
D. Security incident management policy
Answer: (SHOW ANSWER)
The information security training policy ensures that everyone within the organization, including contractors and third-party users, receives the appropriate level of security awareness and training. This policy defines how the organization communicates its security requirements, expectations, and best practices.
"Information security training policies and programs ensure that all personnel are aware of and understand the security requirements and their individual responsibilities."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Security Awareness and Training The ISACA CISM practice questions emphasize that a clear training policy is the best way to communicate security practices to all involved parties.

NEW QUESTION: 220
The MOST important element in achieving executive commitment to an information security governance program is:

A. a defined security framework.
B. a process improvement model
C. established security strategies.
D. identified business drivers.
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: 221
Who is accountable for approving an information security governance framework?
A. The board of directors
B. The chief information security officer (CISO)
C. The enterprise risk committee
D. The chief information officer (CIO)
Answer: (SHOW ANSWER)
The board of directors is ultimately responsible for the governance of the organization, including the approval of the information security governance framework and the oversight of its implementation and performance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 2: Establish and Maintain an Information Security Governance Framework, Section:
Roles and Responsibilities of Senior Management and the Board of Directors1

NEW QUESTION: 222
Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?
A. Identify business requirements
B. Document disaster recovery procedures
C. Conduct a risk assessment
D. Perform a business impact analysis (BIA)
Answer: (SHOW ANSWER)
The Business Impact Analysis (BIA) is the first step in developing a disaster recovery plan because it identifies critical business processes, dependencies, and acceptable downtime.
"A BIA provides the foundation for disaster recovery planning by identifying business functions and their criticality."
- CISM Review Manual 15th Edition, Chapter 3: Program Development, Section: Disaster Recovery Planning* Risk assessments follow the BIA and inform recovery strategies, but the BIA must come first.

NEW QUESTION: 223
Which of the following should be done NEXT following senior management's decision to comply with new personal data regulations that are much more stringent than those currently followed to avoid massive fines?
A. Encrypt data in transit and at rest.
B. Complete a return on investment (ROI) analysis.
C. Create and implement a data minimization plan.
D. Conduct a gap analysis.
Answer: (SHOW ANSWER)
A gap analysis is a tool that helps to identify the current state of compliance and the desired state of compliance, as well as the actions needed to achieve the desired state. A gap analysis should

be done before implementing any specific controls or solutions, such as encryption, data minimization, or ROI analysis.
References = CISM Review Manual 15th Edition, page 65; Information Security Architecture: Gap Assessment and Prioritization, ISACA Journal, volume 2, 2018.

NEW QUESTION: 224
After a recovery from a successful malware attack, instances of the malware continue to be discovered. Which phase of incident response was not successful?
A. EradicationB Recovery
B. Lessons learned review
C. Incident declaration
Answer: (SHOW ANSWER)
Eradication is the phase of incident response where the incident team removes the threat from the affected systems and restores them to a secure state. If this phase is not successful, the malware may persist or reappear on the systems, causing further damage or compromise. Therefore, eradication is the correct answer.
References:
https://www.securitymetrics.com/blog/6-phases-incident-response-plan
https://www.atlassian.com/incident-management/incident-response
https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

NEW QUESTION: 225
Which of the following is BEST used to determine the maturity of an information security program?
A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics
Answer: D (LEAVE A REPLY)
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: 226
Which of the following BEST determines an information asset's classification?
A. Value of the information asset in the marketplace
B. Criticality to a business process
C. Risk assessment from the data owner
D. Cost of producing the information asset
Answer: (SHOW ANSWER)
According to the CISM Review Manual, 15th Edition1, information asset classification is the process of assigning a level of sensitivity to information assets based on their importance to the organization and the potential impact of unauthorized disclosure, modification or destruction. The criticality of an information asset to a business process is one of the key factors that determines its classification level.
References = 1: CISM Review Manual, 15th Edition, ISACA, 2016, Chapter 2, page 61.

NEW QUESTION: 227
Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?
A. Review compliance requirements.
B. Communicate the exposure.
C. Declare an incident.
D. Change the encryption keys.
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: 228
Which of the following is a PRIMARY function of an incident response team?
A. To provide a single point of contact for critical incidents
B. To provide a risk assessment for zero-day vulnerabilities
C. To provide a business impact analysis (BIA)
D. To provide effective incident mitigation
Answer: (SHOW ANSWER)

NEW QUESTION: 229
Which of the following should be done FIRST to prioritize response to incidents?
A. Triage
B. Analysis
C. Escalation
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 230
An organization wants to migrate a proprietary application to be hosted by a third-party cloud hosting provider using a Platform as a Service (PaaS) model. Prior to selecting the cloud provider, what is MOST important for the organization to ensure?

A. The cloud provider can meet recovery point objectives (RPOs).
B. The cloud provider adheres to applicable regulations.
C. The cloud provider's service level agreement (SLA) includes availability requirements.
D. The hosting contract has a termination clause.
Answer: (SHOW ANSWER)
When outsourcing to a cloud provider, regulatory compliance is paramount-especially with sensitive or proprietary applications. Non-compliance could result in legal penalties, fines, or reputational damage.
While RPOs, SLAs, and contract clauses are critical components of vendor risk management, ensuring adherence to relevant laws and industry regulations (such as GDPR, HIPAA, PCI DSS) is the first priority in cloud migration decisions.
"Prior to selecting a cloud provider, legal, regulatory, and contractual requirements must be reviewed to ensure alignment."
- CISM Review Manual 15th Edition, Chapter 1: Information Security Governance, Section: Compliance Considerations in Cloud Computing*

NEW QUESTION: 231

Which of the following is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider?

A. Obtain an independent audit report.

B. Require the provider to follow stringent data classification procedures.

C. Include high penalties for security breaches in the contract.

D. Review the provider's information security policies.

Answer: (SHOW ANSWER)

Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction." CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of the enterprise." Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers. One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

NEW QUESTION: 232

Which of the following is the BEST indication that an organization has integrated information security governance with corporate governance?

A. Security performance metrics are measured against business objectives.

B. Impact is measured according to business loss when assessing IT risk.

C. Security policies are reviewed whenever business objectives are changed.

D. Service levels for security vendors are defined according to business needs.

Answer: (SHOW ANSWER)

Security performance metrics are quantitative or qualitative measures that indicate the effectiveness and efficiency of the information security program in achieving the organization's security goals and objectives.

Measuring security performance metrics against business objectives is the best indication that an organization has integrated information security governance with corporate governance, as it demonstrates that the security program is aligned with and supports the business strategy, value delivery, and risk management. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 233
Which of the following is the MOST important detail to capture in an organization's risk register?
A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria
D. Risk ownership
Answer: (SHOW ANSWER)
Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

NEW QUESTION: 234
Company A, a cloud service provider, is in the process of acquiring Company B to gain new benefits by incorporating their technologies within its cloud services.
Which of the following should be the PRIMARY focus of Company A's information security manager?
A. The organizational structure of Company B
B. The cost to align to Company A's security policies
C. Company A's security architecture
D. Company B's security policies
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: 235
An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?
A. Conduct an information security audit.
B. Validate the relevance of the information.
C. Perform a gap analysis.
D. Inform senior management

Answer: (SHOW ANSWER)

The information security manager's first course of action should be to validate the relevance of the information received from the threat intelligence service. This means verifying the source, credibility, accuracy, and timeliness of the information, as well as assessing the potential impact and likelihood of the threat for the organization. This will help the information security manager to determine the appropriate response and prioritize the actions to mitigate the threat. Conducting an information security audit, performing a gap analysis, and informing senior management are possible subsequent actions, but they are not the first course of action. An information security audit is a systematic and independent assessment of the effectiveness of the information security controls and processes. A gap analysis is a comparison of the current state of the information security program with the desired state or best practices. Informing senior management is a communication activity that should be done after validating the information and assessing the risk. References = CISM Review Manual, 16th Edition, pages 44-451; CISM Review Questions, Answers
& Explanations Manual, 10th Edition, page 632

The first step the information security manager should take upon learning of the potential threat is to validate the relevance of the information. This should involve researching the threat to evaluate its potential impact on the organization and to determine the accuracy of the threat intelligence. Once the information is validated, the information security manager can then take action, such as informing senior management, conducting an information security audit, or performing a gap analysis.

NEW QUESTION: 236

Which type of control is an incident response team?

A. Corrective

B. Directive

C. Detective

D. Preventive

Answer: (SHOW ANSWER)

NEW QUESTION: 237

Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?

A. The capabilities and expertise of the information security team

B. The organization's mission statement and roadmap

C. A prior successful information security strategy

D. The organization's information technology (IT) strategy

Answer: (SHOW ANSWER)

= The most useful source of information for a newly hired information security manager who has been tasked with developing and implementing an information security strategy is the organization's mission statement and roadmap. The mission statement defines the organization's

purpose, vision, values, and goals, and the roadmap outlines the organization's strategic direction, priorities, and initiatives. By reviewing the mission statement and roadmap, the information security manager can understand the organization's business objectives, risk appetite, and security needs, and align the information security strategy with them. The information security strategy should support and enable the organization's mission and roadmap, and provide the security governance, policies, standards, and controls to protect the organization's information assets and processes.

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

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

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

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

Information Security Strategy Development, page 23-241

NEW QUESTION: 238

A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.

B. Suspend the connection to the application in the firewall

C. Report the situation to the business owner of the application.

D. Initiate the organization's incident response process.

Answer: (SHOW ANSWER)

= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability.

The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application.

Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action.

Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application.

Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual

2023, page 211 1; CISM Practice Quiz 2

NEW QUESTION: 239

Which of the following is the PRIMARY reason to regularly update business continuity and disaster recovery documents?

A. To enforce security policy requirements

B. To maintain business asset inventories

C. To ensure audit and compliance requirements are met

D. To ensure the availability of business operations

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: 240
The PRIMARY advantage of involving end users in continuity planning is that they:
A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.
Answer: (SHOW ANSWER)
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION: 241
Management of a financial institution accepted an operational risk that consequently led to the temporary deactivation to a critical monitoring process. Which of the following should be the information security manager's GREATEST concern with this situation?
A. Impact on compliance risk.
B. Inability to determine short-term impact.
C. Impact on the risk culture.
D. Deviation from risk management best practices
Answer: C (LEAVE A REPLY)
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: 242
An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?
A. Determine which country's information security regulations will be used.
B. Merge the two existing information security programs.
C. Apply the existing information security program to the acquired company.
D. Evaluate the information security laws that apply to the acquired company.
Answer: (SHOW ANSWER)
The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

NEW QUESTION: 243
Which of the following provides the BEST assurance that security policies are applied across business operations?
A. Organizational standards are included in awareness training.
B. Organizational standards are enforced by technical controls.
C. Organizational standards are required to be formally accepted.
D. Organizational standards are documented in operational procedures.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 244
Which of the following is MOST important to include in a post-incident review following a data breach?
A. An evaluation of the effectiveness of the information security strategy
B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom
Answer: (SHOW ANSWER)
= A post-incident review is a process of analyzing and learning from a security incident, such as a data breach, to improve the security posture and resilience of an organization. A post-incident review should include the following elements12:
* A clear and accurate description of the incident, including its scope, impact, timeline, root cause, and contributing factors.
* A detailed assessment of the effectiveness and efficiency of the incident response process, including the roles and responsibilities, communication channels, coordination mechanisms, escalation procedures, tools and resources, documentation, and reporting.
* An evaluation of the adequacy of existing controls, such as policies, standards, procedures, technical measures, awareness, and training, to prevent, detect, and mitigate similar incidents in the future.

* A list of actionable recommendations and improvement plans, based on the lessons learned and best practices, to address the identified gaps and weaknesses in the security strategy, governance, risk management, and incident management.
* A follow-up and monitoring mechanism to ensure the implementation and verification of the recommendations and improvement plans.
The most important element to include in a post-incident review following a data breach is the evaluation of the adequacy of existing controls, because it directly relates to the security objectives and requirements of the organization, and provides the basis for enhancing the security posture and resilience of the organization.
Evaluating the existing controls helps to identify the vulnerabilities and risks that led to the data breach, and to determine the appropriate corrective and preventive actions to reduce the likelihood and impact of similar incidents in the future. Evaluating the existing controls also helps to align the security strategy and governance with the business goals and objectives, and to ensure the compliance with legal, regulatory, and contractual obligations.
The other elements, such as an evaluation of the effectiveness of the information security strategy, documentation of regulatory reporting requirements, and a review of the forensics chain of custody, are also important, but not as important as the evaluation of the existing controls. An evaluation of the effectiveness of the information security strategy is a broader and more strategic activity that may not be directly relevant to the specific incident, and may require more time and resources to conduct. Documentation of regulatory reporting requirements is a necessary and mandatory task, but it does not provide much insight or value for improving the security posture and resilience of the organization. A review of the forensics chain of custody is a technical and procedural activity that ensures the integrity and admissibility of the digital evidence collected during the incident investigation, but it does not address the root cause or the mitigation of the incident. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM Review Manual 15th Edition, page 147

NEW QUESTION: 245
An organization finds it necessary to quickly shift to a work-fromhome model with an increased need for remote access security.
Which of the following should be given immediate focus?
A. Moving to a zero trust access model
B. Enabling network-level authentication
C. Enhancing cyber response capability
D. Strengthening endpoint security
Answer: (SHOW ANSWER)
Strengthening endpoint security is the most immediate focus when shifting to a work-from-home model with an increased need for remote access security, as this reduces the risk of unauthorized access, data leakage, malware infection, and other threats that may compromise the confidentiality, integrity, and availability of the organization's information assets. Moving to a zero trust access model, enabling network-level authentication, and enhancing cyber response

capability are also important, but not as urgent as strengthening endpoint security, as they require more time, resources, and planning to implement effectively. References = CISM Review Manual 2023, page 1561; CISM Review Questions, Answers & Explanations Manual 2023, page 302; ISACA CISM - iSecPrep, page 153

NEW QUESTION: 246
Implementing the principle of least privilege PRIMARILY requires the identification of:
A. job duties
B. data owners
C. primary risk factors.
D. authentication controls
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: 247
The contribution of recovery point objective (RPO) to disaster recovery is to:
A. minimize outage periods.
B. eliminate single points of failure.
C. define backup strategy
D. reduce mean time between failures (MTBF).
Answer: (SHOW ANSWER)

The contribution of recovery point objective (RPO) to disaster recovery is to define backup strategy because it determines the maximum amount of data loss that is acceptable to an organization after a disruption, and guides the frequency and type of backups needed to restore the data to a usable format1. Minimize outage periods is not a contribution of RPO, but rather a contribution of recovery time objective (RTO), which defines the maximum amount of time that is acceptable to restore normal operations after a disruption2. Eliminate single points of failure is not a contribution of RPO, but rather a goal of high availability (HA), which ensures that systems or services are continuously operational and resilient3. Reduce mean time between failures (MTBF) is not a contribution of RPO, but rather a measure of reliability, which indicates the average time that a system or component operates without failure4. References: 1 https://www. druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs 2 https://www.druva.com /glossary/what-is-a-recovery-time-objective-definition-and-related-faqs 3 https://www.fortinet.com/resources /cyberglossary/high-availability 4 https://www.fortinet.com/resources/cyberglossary/mean-time-between- failures

NEW QUESTION: 248
Which of the following is the MOST important reason to consider organizational culture when developing an information security program?
A. It helps expedite approval for the information security budget.
B. Everyone in the organization is responsible for information security.
C. It helps the organization meet compliance requirements.
D. Security incidents have an adverse impact on the entire organization.
Answer: (SHOW ANSWER)

NEW QUESTION: 249
Which of the following is MOST helpful to identify whether information security policies have been followed?
A. Corrective controls
B. Preventive controls
C. Directive controls
D. Detective controls
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following is the GREATEST benefit of performing a tabletop exercise of the business continuity plan (BCP)?

A. It provides a low-cost method of assessing the BCP's completeness.
B. It identifies appropriate follow-up work to address shortcomings in the plan.
C. It allows for greater participation and planning from the business side.

D. It helps in assessing the availability of compatible backup hardware.
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which of the following is the MOST important factor in successfully implementing Zero Trust?
A. Preferring networks that have undergone penetration testing
B. Focusing on logging and monitoring of user behavior
C. Authenticating and authorizing strategic points of the architecture
D. Understanding each component of the network
Answer: (SHOW ANSWER)
Zero Trust requires granular authentication and authorization at every critical juncture. It assumes no implicit trust within the network and enforces strict access control.
"Zero Trust is based on continuous authentication and authorization at all strategic control points." - CISM Review Manual 15th Edition, Chapter 3: Security Architecture, Section: Zero Trust Principles*

NEW QUESTION: 252
Which of the following BEST determines the allocation of resources during a security incident response?
A. Senior management commitment
B. A business continuity plan (BCP)
C. An established escalation process
D. Defined levels of severity
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: 253
Which of the following provides the BEST input to determine the level of protection needed for an IT system?

A. Asset classification
B. Internal audit findings
C. Threat analysis
D. Vulnerability assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 254
Of the following, who is MOST appropriate to own the risk associated with the failure of a privileged access control?
A. Data owner
B. Business owner
C. Information security manager
D. Compliance manager
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: 255
Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?
A. Suspend the data exchange with the provider
B. Notify appropriate regulatory authorities of the breach.
C. Initiate the business continuity plan (BCP)
D. Validate the breach with the provider
Answer: (SHOW ANSWER)
The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other

options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider. References:
https://www.wired.com/story/sequoia-hr-data-breach/
https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a- long-outage/
https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117- p599mr

NEW QUESTION: 256
Which of the following activities MUST be performed by an information security manager for change requests?
A. Review change in business requirements for information security.
B. Perform penetration testing on affected systems.
C. Scan IT systems for operating system vulnerabilities.
D. Assess impact on information security risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 257
During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption, unauthorized alterations, and errors?
A. Configuration management
B. Password management
C. Change management
D. Version management
Answer: (SHOW ANSWER)
Change management is the process of planning, implementing, and monitoring changes to information systems in a controlled and coordinated manner. Change management proactively minimizes the likelihood of disruption, unauthorized alterations, and errors by ensuring that changes are aligned with the organization's objectives, policies, and procedures. Change management also involves identifying and mitigating the risks associated with changes, as well as communicating and documenting the changes to all relevant stakeholders12.

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

NEW QUESTION: 258
Which of the following is MOST important in increasing the effectiveness of incident responders?
A. Communicating with the management team
B. Integrating staff with the IT department
C. Testing response scenarios
D. Reviewing the incident response plan annually
Answer: (SHOW ANSWER)
= 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: 259
The information security manager of a multinational organization has been asked to consolidate the information security policies of its regional locations. Which of the following would be of GREATEST concern?

A. Varying threat environments
B. Disparate reporting lines
C. Conflicting legal requirements
D. Differences in work culture
Answer: (SHOW ANSWER)
Conflicting legal requirements would be of greatest concern when consolidating the information security policies of regional locations, as they may pose significant challenges and risks for the organization's compliance, privacy, and data protection obligations. Different jurisdictions may have different laws and regulations regarding information security, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. These laws and regulations may have different definitions, scopes, standards, and enforcement mechanisms for information security, which may create conflicts or inconsistencies when applying a unified policy across the organization. Therefore, the information security manager should conduct a thorough analysis of the legal requirements of each location, and ensure that the consolidated policy meets the highest level of compliance and avoids any violations or penalties.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task
1.22; CISM 2020: IT Security Policies; Information Security Due Diligence Questionnaire

NEW QUESTION: 260
The PRIMARY purpose for conducting cybersecurity risk assessments is to:
A. Assist in security reporting to senior management
B. Provide metrics to indicate cybersecurity program effectiveness
C. Verify compliance across multiple sectors
D. Understand the organization's current security posture
Answer: (SHOW ANSWER)
The main goal of a cybersecurity risk assessment is to gain visibility into the organization's current security posture, identify vulnerabilities, evaluate threats, and understand the potential impact of various risks.
"Risk assessments provide an understanding of the organization's threat landscape, asset vulnerabilities, and residual risk exposure."
- CISM Review Manual 15th Edition, Chapter 2: Risk Assessment and Risk Identification* While assessments support reporting and compliance, their primary role is situational awareness.

NEW QUESTION: 261
Which of the following parties should be responsible for determining access levels to an application that processes client information?
A. The business client
B. The information security tear

C. The identity and access management team
D. Business unit management
Answer: (SHOW ANSWER)
The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.
The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

NEW QUESTION: 262
Communicating which of the following would be MOST helpful to gain senior management support for risk treatment options?
A. Quantitative loss
B. Industry benchmarks
C. Threat analysis
D. Root cause analysis
Answer: (SHOW ANSWER)
communicating the quantitative loss associated with the risk scenarios and the risk treatment options would be the most helpful to gain senior management support, as it helps to demonstrate the value and effectiveness of the risk treatment options in terms of reducing the likelihood and impact of the risk. Quantitative loss also helps to compare the cost and benefit of the risk treatment options and to prioritize the most critical risks.

Industry benchmarks, threat analysis, and root cause analysis may be useful for understanding and assessing the risk, but they do not directly measure the performance of the risk treatment options.
References = Five Key Considerations When Developing Information Security Risk Treatment Plans, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NEW QUESTION: 263
Which of the following sources is MOST useful when planning a business-aligned information security program?
A. Security risk register
B. Information security policy
C. Business impact analysis (BIA)
D. Enterprise architecture (EA)
Answer: (SHOW ANSWER)
A business-aligned information security program is one that supports the organization's business objectives and aligns the information security strategy with the business functions. A business impact analysis (BIA) is a process that identifies the critical business processes, assets, and functions of an organization, and assesses their potential impact in the event of a disruption or loss. A BIA helps to prioritize the information security requirements and controls that are needed to protect the organization's critical assets and functions from various threats and risks. Therefore, a BIA is one of the most useful sources when planning a business-aligned information security program. References = CISM Review Manual 15th Edition, page 254; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 229.
The most useful source when planning a business-aligned information security program is a Business Impact Analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to an organization's operations, and helps to identify the security controls and measures that should be implemented to reduce the impact of those disruptions. The BIA should include an assessment of the organization's information security posture, including its security policies, risk register, and enterprise architecture. With this information, organizations can develop an information security program that is aligned to the organization's business objectives.

NEW QUESTION: 264
Application data integrity risk is MOST directly addressed by a design that includes:
A. reconciliation routines such as checksums, hash totals, and record counts.
B. strict application of an authorized data dictionary.
C. application log requirements such as field-level audit trails and user activity logs.
D. access control technologies such as role-based entitlements.
Answer: (SHOW ANSWER)
Reconciliation routines are methods to verify the integrity of data by comparing the input and output of a process or a system. They can detect errors, omissions, duplications or unauthorized modifications of data. They are more directly related to data integrity than the other options, which

are more concerned with data definition, logging or access control. References = CISM Review Manual, 16th Edition, Chapter 3, Section 3.4.21

NEW QUESTION: 265
Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?
A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.
D. Identify recovery time objectives (RTOs).
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: 266
Which of the following should be the PRIMARY objective of the information security incident response process?
A. Conducting incident triage
B. Communicating with internal and external parties
C. Minimizing negative impact to critical operations
D. Classifying incidents
Answer: (SHOW ANSWER)
The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents.

The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.
Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed.
However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION: 267
Which of the following BEST facilitates effective incident response testing?
A. Including all business units in testing
B. Simulating realistic test scenarios
C. Reviewing test results quarterly
D. Testing after major business changes
Answer: (SHOW ANSWER)
Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective testing is to simulate realistic test scenarios that reflect the most likely or critical threats

and vulnerabilities that could cause an incident, and the most relevant or significant impacts and consequences that could result from an incident. Simulating realistic test scenarios can help to evaluate the adequacy, accuracy, and applicability of the incident response plan, procedures, roles, and resources, as well as to identify and address any gaps, weaknesses, or errors that could hinder or compromise the incident response process. Simulating realistic test scenarios can also help to enhance the skills, knowledge, and experience of the incident response team and the organization, as well as to improve the communication, coordination, and collaboration among the stakeholders involved in the incident response process. Simulating realistic test scenarios can also help to measure and report the effectiveness and efficiency of the incident response process, and to provide feedback and recommendations for improvement and optimization. References = CISM Review Manual 15th Edition, page 2401; CISM Practice Quiz, question 1362

NEW QUESTION: 268

Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?

A. Projected Increase in maturity level

B. Estimated reduction in risk

C. Projected costs over time

D. Estimated increase in efficiency

Answer: (SHOW ANSWER)

The best thing to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its cost-effectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

NEW QUESTION: 269
Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?
A. Alignment with industry benchmarks
B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget
Answer: B (LEAVE A REPLY)
The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

NEW QUESTION: 270
Which of the following should be the FIRST step in developing an information security strategy?
A. Determine acceptable levels of information security risk
B. Create a roadmap to identify security baselines and controls
C. Perform a gap analysis based on the current state
D. Identify key stakeholders to champion information security
Answer: (SHOW ANSWER)
The first step in developing an information security strategy is to identify key stakeholders who can provide support, guidance and resources for information security initiatives. These stakeholders may include senior management, business unit leaders, legal counsel, audit and compliance officers and other relevant parties. By engaging these stakeholders early on, an information security manager can ensure that the strategy aligns with business objectives and expectations, as well as gain buy-in and commitment from them. Determining acceptable levels of risk, creating a roadmap and performing a gap analysis are all important steps in developing an information security strategy, but they should follow after identifying key stakeholders.

NEW QUESTION: 271
Which of the following is the BEST method to protect the confidentiality of data transmitted over the Internet?
A. Network address translation (NAT)
B. Message hashing
C. Transport Layer Security (TLS)
D. Multi-factor authentication
Answer: (SHOW ANSWER)

Transport Layer Security (TLS) is a protocol that provides encryption, authentication, and integrity for data transmitted over the Internet. TLS protects the confidentiality of data by encrypting it before sending it and decrypting it after receiving it. TLS also verifies the identity of the communicating parties by using certificates and prevents data tampering by using message authentication codes. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.3.2.11

NEW QUESTION: 272
Which of the following will BEST facilitate integrating the information security program into corporate governance?
A. A minimum security baseline
B. An up-to-date security strategy
C. Documentation of the threat landscape
D. Documentation of residual risk
Answer: (SHOW ANSWER)

NEW QUESTION: 273
A business continuity plan (BCP) should contain:
A. Hardware and software inventories
B. Data restoration procedures
C. Information about eradication activities
D. Criteria for activation
Answer: (SHOW ANSWER)
Criteria for activation are essential to ensure that the BCP is triggered appropriately in response to a disruption.
"The BCP should include clearly defined activation criteria to ensure that plans are invoked when necessary."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Planning* ISACA's practice questions confirm that criteria for activation are core to a BCP's effectiveness.

NEW QUESTION: 274

An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?

A. Control owner responses based on a root cause analysis

B. The impact of noncompliance on the organization's risk profile

C. A noncompliance report to initiate remediation activities

D. A business case for transferring the risk

Answer: (SHOW ANSWER)

The impact of noncompliance on the organization's risk profile is the MOST important information for the information security manager to communicate to senior management, because it helps them understand the potential consequences of not adhering to the established controls and the need for corrective actions.

Noncompliance may expose the organization to increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 84: "The information security manager should report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process." CISM Review Manual, 16th Edition, ISACA, 2020, p. 85: "Noncompliance with information security policies, standards, and procedures may result in increased threats, vulnerabilities, and losses, as well as legal, regulatory, and contractual liabilities for the enterprise."

NEW QUESTION: 275

For an e-business that requires high availability, which of the following design principles is BEST?

A. Manual failover to the website of another e-business that meets the user's needs

B. A single point of entry allowing transactions to be received and processed quickly

C. Intelligent middleware to direct transactions from a downed system to an alternative

D. Availability of an adjacent cold site and a standby server with mirrored copies of critical data

Answer: (SHOW ANSWER)

Intelligent middleware enables dynamic rerouting and automated load balancing, which is crucial for high availability. This minimizes downtime and ensures continuity without manual intervention.

"Middleware solutions can provide automated failover capabilities, improving system resilience and availability."

- CISM Review Manual 15th Edition, Chapter 3: Program Development and Management, Section:

Availability and Resilience*

Manual failover and cold sites introduce delays, which are not suitable for e-business environments requiring near-zero downtime.

NEW QUESTION: 276

Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

A. Evaluate privacy technologies required for data protection.

B. Encrypt all personal data stored on systems and networks.

C. Update disciplinary processes to address privacy violations.

D. Create an inventory of systems where personal data is stored.

Answer: (SHOW ANSWER)

= The first step when establishing a new data protection program that must comply with applicable data privacy regulations is to create an inventory of systems where personal data is stored. Personal data is any information that relates to an identified or identifiable natural person, such as name, address, email, phone number, identification number, location data, biometric data, or online identifiers. Data privacy regulations are laws and rules that govern the collection, processing, storage, transfer, and disposal of personal data, and that grant rights and protections to the data subjects, such as the right to access, rectify, erase, or restrict the use of their personal data. Examples of data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Creating an inventory of systems where personal data is stored is essential for the data protection program, because it helps to:

Identify the sources, types, and locations of personal data that the organization collects and holds, and the purposes and legal bases for which they are used.

Assess the risks and impacts associated with the personal data, and the compliance requirements and obligations under the applicable data privacy regulations.

Implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, modification, or loss, such as encryption, pseudonymization, access control, backup, or audit logging.

Establish policies, procedures, and processes to manage the personal data throughout their life cycle, and to respond to the requests and complaints from the data subjects or the data protection authorities.

Monitor and review the performance and effectiveness of the data protection program, and report and resolve any data breaches or incidents.

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

NEW QUESTION: 277

Which of the following is the MOST important function of an information security steering committee?

A. Assigning data classifications to organizational assets

B. Developing organizational risk assessment processes

C. Obtaining multiple perspectives from the business

D. Defining security standards for logical access controls

Answer: C (LEAVE A REPLY)
An information security steering committee is a group of senior executives and managers from different business units and functions who provide strategic direction, oversight, and support for the information security program. The most important function of the committee is to obtain multiple perspectives from the business, as this helps to ensure that the information security program aligns with the business goals, needs, and culture, and that the security decisions reflect the interests and expectations of the stakeholders.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; Improve Security Governance With a Security Steering Committee2; The Role of the Corporate Information Security Steering Committee3

NEW QUESTION: 278
An organization's quality process can BEST support security management by providing:
A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.
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: 279
What should an information security manager verify FIRST when reviewing an information asset management program?
A. System owners have been identified.
B. Key applications have been secured.
C. Information assets have been classified.
D. Information assets have been inventoried.
Answer: (SHOW ANSWER)

According to the CISM Review Manual, information asset classification is the first step in an information asset management program, as it provides the basis for determining the level of protection required for each asset. System owners, key applications and information asset inventory are subsequent steps that depend on the classification of the assets.
References = CISM Review Manual, 27th Edition, Chapter 1, Section 1.4.2, page 381.

NEW QUESTION: 280

Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?

A. Security information and event management (SIEM)
B. Extended detection and response (XDR)
C. Endpoint detection and response (EDR)
D. Network intrusion detection system (NIDS)
Answer: (SHOW ANSWER)
A SIEM system provides the ability to collect, correlate, and analyze security events, enabling effective prioritization of incidents based on risk and impact. SIEM solutions also support tracking incidents from detection through resolution, as stated in the CISM Review Manual under incident management and monitoring.
Reference:ISACA CISM Review Manual, 16th Edition, Page 303-304, "SIEM and Incident Prioritization".

NEW QUESTION: 281
Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?
A. Parallel test
B. Full interruption test
C. Simulation test
D. Tabletop test
Answer: (SHOW ANSWER)
A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required. A parallel test involves processing the same transactions or data at both the primary and the alternate site simultaneously, and comparing the results for accuracy and consistency. A parallel test can validate the functionality, performance, and reliability of the alternate site without disrupting the normal operations at the primary site. A parallel test can also identify and resolve any issues or discrepancies between the two sites before a real disaster occurs. A parallel test can provide a high level of assurance and confidence that the alternate site can support the organization's continuity requirements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP) Testing, page 1861; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 56, page 522.

A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required because it involves processing data at both the primary and alternate sites simultaneously without disrupting the normal operations1. A full interruption test would cause downtime and potential loss of data or revenue2. A simulation test would not provide a realistic assessment of the alternate site's capabilities3. A tabletop test would only involve a discussion of the procedures and scenarios without actually testing the site4.
1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM - ISACA Certified Information Security Manager Exam Prep - NICCS 3: Prepare for the ISACA Certified Information Security Manager Exam: CISM ... 4: CISM: Certified Information Systems Manager | Official ISACA ... - NICCS

NEW QUESTION: 282
Which of the following is the PRIMARY reason that an information security manager should restrict the use of generic administrator accounts in a multi-user environment?
A. To prevent accountability issues
B. To ensure system audit trails are not bypassed
C. To ensure separation of duties is maintained
D. To prevent unauthorized user access
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?
A. The service level agreement (SLA) was not met.
B. The recovery time objective (RTO) was not met.
C. The root cause was not identified.
D. Notification to stakeholders was delayed.
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: 284

Which of the following BEST enables the restoration of operations after a limited ransomware incident occurs?

A. Documented eradication procedures

B. Reliable image backups

C. Root cause analysis

D. Impact assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 285

Which of the following BEST indicates that information assets are classified accurately?

A. Appropriate prioritization of information risk treatment

B. Increased compliance with information security policy

C. Appropriate assignment of information asset owners

D. An accurate and complete information asset catalog

Answer: (SHOW ANSWER)

The best indicator that information assets are classified accurately is appropriate prioritization of information risk treatment. Information asset classification is the process of assigning a level of sensitivity or criticality to information assets based on their value, impact, and legal or regulatory requirements. The purpose of information asset classification is to facilitate the identification and protection of information assets according to their importance and risk exposure. Therefore, if information assets are classified accurately, the organization can prioritize the information risk treatment activities and allocate the resources accordingly. The other options are not direct indicators of information asset classification accuracy, although they may be influenced by it. References = CISM Review Manual 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1031

NEW QUESTION: 286

Which of the following BEST enables an organization to effectively manage emerging cyber risk?

A. Periodic internal and external audits

B. Clear lines of responsibility

C. Sufficient cyber budget allocation

D. Cybersecurity policies

Answer: (SHOW ANSWER)

Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber

budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

NEW QUESTION: 287
The business value of an information asset is derived from:
A. the threat profile.
B. its criticality.
C. the risk assessment.
D. its replacement cost.
Answer: (SHOW ANSWER)
The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability (CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it. References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

NEW QUESTION: 288
An organization has discovered that a server processing real-time visual data could be vulnerable to a lateral movement stage in a ransomware attack. Which of the following controls BEST mitigates this vulnerability?
A. Network segmentation
B. Data loss prevention (DLP)
C. Encryption of data in transit
D. Intrusion detection system (IDS)
Answer: A (LEAVE A REPLY)

Network segmentation is the most effective control to prevent lateral movement. In ransomware attacks, attackers often breach one endpoint and move laterally across the network to reach critical assets.
Segmentation limits this movement by isolating systems into different zones or subnets, thereby reducing the attack surface and preventing unauthorized internal traversal.
DLP and encryption are primarily focused on data protection, not internal network movement.
IDS can detect intrusions but does not prevent movement like segmentation does.
"Network segmentation limits the scope of access for compromised systems and is a key strategy in preventing lateral movement in an attack."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Architecture, Section: Network Security* Real-world example: "In the NotPetya and WannaCry incidents, poor internal segmentation allowed malware to propagate rapidly."

NEW QUESTION: 289
Which of the following is the MOST effective way to ensure the security of services and solutions delivered by third-party vendors?
A. Integrate risk management into the vendor management process.
B. Conduct security reviews on the services and solutions delivered.
C. Review third-party contracts as part of the vendor management process.
D. Perform an audit on vendors' security controls and practices.
Answer: A (LEAVE A REPLY)
Integrating risk management into the vendor management process is the most effective way to ensure the security of services and solutions delivered by third-party vendors, as it enables the organization to identify, assess, treat, and monitor the risks associated with outsourcing. Risk management should be applied throughout the vendor life cycle, from selection, contracting, onboarding, monitoring, to termination. Risk management also helps the organization to define the security requirements, expectations, and responsibilities for the vendors, and to evaluate their performance and compliance. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2; Preparing Your First Supplier Audit Plan1.

NEW QUESTION: 290
Which is following should be an information security manager's PRIMARY focus during the development of a critical system storing highly confidential data?

A. Reducing the number of vulnerabilities detected
B. Ensuring the amount of residual risk is acceptable
C. Avoiding identified system threats
D. Complying with regulatory requirements
Answer: (SHOW ANSWER)
The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable.

Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

NEW QUESTION: 291
Detailed business continuity plans (BCPs) should be PRIMARILY based on:
A. capabilities of available local vendors.
B. strategies validated by senior management.
C. cost and resources needed to execute.
D. strategies that cover all applications.
Answer: (SHOW ANSWER)

NEW QUESTION: 292
Which of the following provides the MOST assurance that a third-party hosting provider will be able to meet availability requirements?
A. Right-to-audit clause
B. The third party's incident response plan
C. Service level agreement (SLA)
D. The third party's business continuity plan (BCP)
Answer: C (LEAVE A REPLY)
A Service Level Agreement (SLA) is the contractual document that specifies and guarantees the availability levels the third-party hosting provider must meet. It provides the clearest and most enforceable commitment to availability.
"SLAs establish measurable commitments that can be monitored and enforced, providing a high level of assurance that service availability will meet business requirements."
- CISM Review Manual 15th Edition, Chapter 3: Information Security Program Development and Management, Section: Outsourcing and Third-Party Management* ISACA's practice questions highlight SLAs as the most direct and reliable assurance for third-party service availability.

NEW QUESTION: 293

Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?
A. Enforce the local regulation.
B. Obtain legal guidance.
C. Enforce the organization's information security policy.
D. Obtain an independent assessment of the regulation.
Answer: (SHOW ANSWER)
The information security manager should first obtain legal guidance when there is a conflict between the organization's information security policy and a local regulation, because this will help to understand the implications and consequences of the conflict, and to identify the possible options and solutions for resolving it. The information security manager should also consult with the relevant stakeholders, such as senior management, business owners, and information owners, to determine the best course of action that aligns with the organization's objectives, risk appetite, and compliance obligations. Enforcing the local regulation or the organization's information security policy without legal guidance may expose the organization to legal liabilities, security risks, or operational disruptions. Obtaining an independent assessment of the regulation may be helpful, but it is not the first step to take.
References = CISM Review Manual, 16th Edition, page 691; A Guide to ISACA CISM Domains & Domain
1: Information Security Governance2

NEW QUESTION: 294
Which of the following is MOST important to have in place when conducting a security control assessment of a system?
A. Control specifications
B. Assurance test plan
C. Scanning tools
D. Security documentation
Answer: (SHOW ANSWER)

NEW QUESTION: 295
Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?
A. To identify the organization's risk tolerance
B. To improve security processes
C. To align security roles and responsibilities
D. To optimize security risk management
Answer: (SHOW ANSWER)
= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By

aligning information security with the organization's strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner1. Alignment also enables the information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives2. Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability3. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information assets with the business objectives and risk appetite of the organization4. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

NEW QUESTION: 296
A business continuity plan (BCP) should contain:
A. criteria for activation.
B. data restoration procedures.
C. hardware and software inventories.
D. information about eradication activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Recovery time objectives (RTOs) are BEST determined by:
A. business managers
B. business continuity officers
C. executive management
D. database administrators (DBAs).
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: 298
An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:
* A bad actor broke into a business-critical FTP server by brute forcing an administrative password

* The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
* The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
* After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail Which of the following could have been prevented by conducting regular incident response testing?

A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data
Answer: (SHOW ANSWER)

Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. References: https://www.isaca.org/resources/isaca-journal/issues/2017 /volume-5/incident-response-lessons-learned https://www.isaca.org/resources/isaca-journal/issues/2018 /volume-3/incident-response-lessons-learned

NEW QUESTION: 299

Which of the following is the MOST important characteristic of an effective information security metric?

A. The metric expresses residual risk relative to risk tolerance.
B. The metric is frequently reported to senior management.
C. The metric directly maps to an industry risk management framework.
D. The metric compares the organization's inherent risk against its risk appetite.
Answer: (SHOW ANSWER)

NEW QUESTION: 300

An organization is selecting security metrics to measure security performance, and a firewall specialist suggests tracking the number of external attacks blocked by the firewalls. Which of the following is the GREATEST concern with using this metric?

A. The number of blocked external attacks is not representative of the true threat profile.

B. The number of blocked external attacks will vary by month, causing inconsistent graphs.
C. The number of blocked external attacks is an indicator of the organization's popularity.
D. The number of blocked external attacks over time does not explain the attackers' motivations.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Metrics should provide meaningful insights into the organization's risk exposure and security performance.
Evaluating this option:
A). The number of blocked external attacks is not representative of the true threat profile: This is the BEST answer because counting attacks blocked does not reveal the effectiveness of security controls or the real risk environment.
B). The number of blocked external attacks will vary by month, causing inconsistent graphs: While variability is a concern, it does not make the metric invalid.
C). The number of blocked external attacks is an indicator of the organization's popularity: This is true but irrelevant to assessing the effectiveness of security measures.
D). The number of blocked external attacks over time does not explain the attackers' motivations: Understanding motivations is useful but not directly tied to evaluating the firewall metric's effectiveness.
Reference: CISM Job Practice Area 2 (Risk Management) emphasizes the need for meaningful and risk-based metrics.

NEW QUESTION: 301
An organization has suffered from a large-scale security event impacting a critical system. Following the decision to restore the system at an alternate location, which plan should be invoked?
A. Incident response plan
B. Business continuity plan (BCP)
C. Communications plan
D. Disaster recovery plan (DRP)
Answer: (SHOW ANSWER)

NEW QUESTION: 302

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

A. best practices.

B. control framework

C. regulatory requirements.

D. cost-benefit analysis,

Answer: (SHOW ANSWER)

Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls12.

CBA involves the following steps12:

Identify the objectives and scope of the analysis

Identify the alternatives and options for achieving the objectives

Identify and quantify the costs and benefits of each alternative

Compare the costs and benefits of each alternative using a common metric or criteria Select the alternative that maximizes the net benefit or minimizes the net cost Perform a sensitivity analysis to test the robustness and validity of the results Document and communicate the results and recommendations CBA is mainly driven by the information security manager's decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization. Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization's objectives, resources, and environment12. References = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

NEW QUESTION: 303

Senior management has expressed concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations Which of the following BEST indicates that the information security manager has tuned the system to address this concern?

A. Increasing false negatives

B. Decreasing false negatives

C. Decreasing false positives
D. Increasing false positives
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: 304
Which of the following provides the MOST effective response against ransomware attacks?
A. Automatic quarantine of systems
B. Thorough communication plans
C. Effective backup plans and processes
D. Strong password requirements
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Recovering from ransomware attacks often depends on having a robust data recovery strategy:
A). Automatic quarantine of systems: This can limit the spread of ransomware but does not address recovery.
B). Thorough communication plans: Communication is important during incidents but does not directly mitigate ransomware.
C). Effective backup plans and processes: This is the BEST option because having backups ensures that encrypted data can be restored, minimizing downtime and data loss.
D). Strong password requirements: This helps prevent unauthorized access but is not sufficient to combat ransomware once it has entered the system.
Reference: CISM Job Practice Area 4 (Information Security Incident Management) stresses the importance of backup and recovery strategies to mitigate ransomware risks.

NEW QUESTION: 305

Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?

A. Risk assessment results

B. Audit findings

C. Key risk indicators (KRIs)

D. Baseline controls

Answer: (SHOW ANSWER)

Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance.

Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs) are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. References = CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization." CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478:

"Baseline controls are the minimum security requirements that apply to all systems within the organization.

They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

NEW QUESTION: 306

To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?

A. Gap analysis results

B. Level of residual risk

C. Level of risk treatment

D. Configuration parameters

Answer: (SHOW ANSWER)

Level of residual risk is the amount of risk that remains after applying risk treatment options, such as avoidance, mitigation, transfer, or acceptance. The information security manager should compare the level of residual risk with the organization's risk appetite, which is the amount of risk that the organization is willing to accept in pursuit of its objectives. The comparison will help to

determine whether the risk treatment options are sufficient, excessive, or inadequate, and whether further actions are needed to align the risk level with the risk appetite.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 49: "Residual risk is the risk that remains after risk treatment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 43: "Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value." CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "The information security manager should compare the residual risk with the risk appetite and determine whether the risk treatment options are sufficient, excessive, or inadequate."

NEW QUESTION: 307
Which of the following BEST protects against emerging advanced persistent threat (APT) actors?
A. Honeypot environment
B. Updated security awareness materials
C. Ongoing incident response training
D. Proactive monitoring
Answer: (SHOW ANSWER)
Proactive monitoring (e.g., threat hunting, real-time log analysis, anomaly detection) is the most effective defense against Advanced Persistent Threats (APTs), which are stealthy, well-resourced, and long-term attacks.
APT actors:
Use zero-day exploits
Maintain long-term unauthorized access
Avoid detection
Traditional controls often fail. Proactive monitoring detects anomalies early, allowing for faster mitigation.
"Ongoing monitoring and detection programs are essential for identifying and responding to persistent and evolving threats."
- CISM Review Manual 15th Edition, Chapter 4: Threat Management, Section: APT Detection Techniques*

NEW QUESTION: 308
Which of the following BEST supports investments in an information security program?
A. Gap analysis results
B. Business cases
C. Risk assessment results
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)

NEW QUESTION: 309
Which of the following will BEST enable an effective information asset classification process?

A. Including security requirements in the classification process
B. Analyzing audit findings
C. Reviewing the recovery time objective (RTO) requirements of the asset
D. Assigning ownership
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: 310
An organization's automated security monitoring tool generates an excessively large amount of falsq positives. Which of the following is the BEST method to optimize the monitoring process?

A. Report only critical alerts.
B. Change reporting thresholds.
C. Reconfigure log recording.
D. Monitor incidents in a specific time frame.
Answer: (SHOW ANSWER)
Changing reporting thresholds is the best method to optimize the monitoring process when the automated security monitoring tool generates an excessively large amount of false positives. Changing reporting thresholds means adjusting the criteria or parameters that trigger the alerts, such as the severity level, the frequency, the source, or the destination of the events. Changing reporting thresholds can help to reduce the number of false positives, filter out the irrelevant or benign events, and focus on the most critical and suspicious events that require further investigation or response.
References = Cybersecurity tool sprawl leading to burnout, false positives: report, Security tools' effectiveness hampered by false positives

NEW QUESTION: 311
An organization's HR department requires that employee account privileges be removed from all corporate IT systems within three days of termination to comply with a government regulation However, the systems all have different user directories, and it currently takes up to four weeks to remove the privileges Which of the following would BEST enable regulatory compliance?
A. Multi-factor authentication (MFA) system
B. Identity and access management (IAM) system
C. Privileged access management (PAM) system

D. Governance, risk, and compliance (GRC) system

Answer: (SHOW ANSWER)

= An identity and access management (IAM) system is a set of processes, policies, and technologies that enable an organization to manage the identities and access rights of its users across different systems and applications1. An IAM system can help an organization to comply with the government regulation by automating the provisioning and deprovisioning of user accounts, enforcing consistent access policies, and integrating different user directories2. An IAM system can also provide audit trails and reports to demonstrate compliance with the regulation3. A multi-factor authentication (MFA) system is a method of verifying the identity of a user by requiring two or more factors, such as something the user knows, has, or is4. An MFA system can enhance the security of user authentication, but it does not address the issue of removing user privileges from different systems within three days of termination. A privileged access management (PAM) system is a solution that manages and monitors the access of privileged users, such as administrators, to critical systems and resources. A PAM system can reduce the risk of unauthorized or malicious use of privileged accounts, but it does not solve the problem of managing the access of regular users across different systems. A governance, risk, and compliance (GRC) system is a software platform that integrates the functions of governance, risk management, and compliance management. A GRC system can help an organization to align its objectives, policies, and processes with the relevant regulations, standards, and best practices, but it does not directly enable the removal of user privileges from different systems within three days of termination. References = 1: CISM Review Manual (Digital Version), page 24 2: 1 3: 2 4: CISM Review Manual (Digital Version), page 25 : CISM Review Manual (Digital Version), page 26 : CISM Review Manual (Digital Version), page 27

NEW QUESTION: 312

The PRIMARY purpose of conducting a business impact analysis (BIA) is to determine the:

A. scope of the incident response plan.

B. scope of the business continuity program.

C. recovery time objective (RTO).

D. resources needed for business recovery.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 313

When testing an incident response plan for recovery from a ransomware attack, which of the following is MOST important to verify?

A. Digital currency is immediately available.

B. Network access requires two-factor authentication.

C. Data backups are recoverable from an offsite location.

D. An alternative network link is immediately available.

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: 314
If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:
A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.
Answer: (SHOW ANSWER)
Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court. The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12. Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server- backup utilities is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody.
Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks involved in the incident, but it may also introduce changes or errors that could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12.
Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected

machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files, or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4:
Information Security Incident Management (ISIM) [2022 update]2

NEW QUESTION: 315
Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?
A. Integrity
B. Authenticity
C. Confidentiality
D. Nonrepudiation
Answer: (SHOW ANSWER)
Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References: https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

NEW QUESTION: 316
Which of the following BEST facilitates the development of a comprehensive information security policy?
A. Alignment with an established information security framework
B. An established internal audit program
C. Security key performance indicators (KPIs)
D. Areview of recent information security incidents
Answer: (SHOW ANSWER)
Alignment with an established information security framework is the BEST way to facilitate the development of a comprehensive information security policy, because it provides a consistent and structured approach to define, implement, and maintain the policy across the organization. An information security framework is a set of best practices, standards, and guidelines that help to ensure the effectiveness, efficiency, and compliance of the information security policy.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "An information security framework is a set of best practices, standards, and guidelines that provide a consistent and structured approach

to information security governance." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "The information security policy should be aligned with an established information security framework to ensure its effectiveness, efficiency, and compliance."

NEW QUESTION: 317
Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?
A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site
Answer: C (LEAVE A REPLY)
= 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: 318
Which of the following is the BEST way to ensure the capability to restore clean data after a ransomware attack?
A. Purchase cyber insurance
B. Encrypt sensitive production data
C. Perform Integrity checks on backups
D. Maintain multiple offline backups

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: 319

Which of the following BEST facilitates the effective execution of an incident response plan?

A. The plan is based on risk assessment results.

B. The response team is trained on the plan

C. The plan is based on industry best practice.

D. The incident response plan aligns with the IT disaster recovery plan (DRP).

Answer: (SHOW ANSWER)

The effective execution of an incident response plan depends largely on the competence and readiness of the response team, who are responsible for carrying out the tasks and activities defined in the plan. Therefore, the best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan, and that they are

familiar with their roles, responsibilities, procedures, and tools. Training the response team on the plan will also help to improve their confidence, communication, coordination, and collaboration during an incident response. The other options are not the best ways to facilitate the effective execution of an incident response plan, although they may be important factors for developing or improving the plan. The plan should be based on risk assessment results and industry best practice, but these do not guarantee that the plan will be executed effectively. The incident response plan should align with the IT disaster recovery plan, but this does not ensure that the response team is prepared and capable of executing the plan. References = CISM Review Manual, 16th Edition, page 1031 The best way to facilitate the effective execution of an incident response plan is to ensure that the response team is trained on the plan. An incident response plan is a set of instructions that defines the roles, responsibilities, procedures, and tools for detecting, responding to, and recovering from security incidents. An incident response team is a group of individuals that are assigned to perform specific tasks and activities during an incident response process. The response team may include security analysts, IT staff, legal counsel, public relations, and other stakeholders. To execute an incident response plan effectively, the response team needs to be trained on the plan, which means they need to be familiar with the following aspects of the plan:

The scope and objectives of the plan The roles and responsibilities of each team member The communication and escalation protocols The incident classification and prioritization criteria The incident response procedures and tools The incident documentation and reporting requirements The incident review and improvement processes By training the response team on the plan, the organization can ensure that the team members are prepared and confident to handle any security incidents that may occur, and that they can perform their tasks efficiently and consistently. The other options are not the best way to facilitate the effective execution of an incident response plan, although they may be some steps or outcomes of the process.

The plan being based on risk assessment results is a desirable practice, as it ensures that the plan is aligned with the organization's risk profile and addresses the most relevant and likely threats and vulnerabilities.

However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The plan being based on industry best practice is a desirable practice, as it ensures that the plan follows established standards and guidelines for incident response. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan. The incident response plan aligning with the IT disaster recovery plan (DRP) is a desirable practice, as it ensures that the plans are consistent and coordinated in terms of objectives, scope, roles, procedures, and tools. However, it does not guarantee that the plan will be executed effectively unless the response team is trained on the plan

NEW QUESTION: 320

Which of the following business units should own the data that populates an identity management system?

A. Information security
B. Information technology
C. Legal
D. Human resources (HR)
Answer: (SHOW ANSWER)

NEW QUESTION: 321
An information security manager has identified that security risks are not being treated in a timely manner.
Which of the following
A. Provide regular updates about the current state of the risks.
B. Re-perform risk analysis at regular intervals.
C. Assign a risk owner to each risk
D. Create mitigating controls to manage the risks.
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: 322
The PRIMARY benefit of integrating information security activities into change management processes is to:
A. protect the business from collusion and compliance threats.
B. ensure required controls are included in changes.
C. provide greater accountability for security-related changes in the business.
D. protect the organization from unauthorized changes.
Answer: (SHOW ANSWER)

NEW QUESTION: 323
Which of the following should be done FIRST when implementing a security program?
A. Perform a risk analysis
B. Implement data encryption.

C. Create an information asset inventory.
D. Determine the value of information assets.
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: 324
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?
A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology
Answer: (SHOW ANSWER)
A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have a higher chance of achieving its objectives and improving the overall security posture of the organization.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

NEW QUESTION: 325
An information security manager is updating the organization's incident response plan. Which of the following is the BEST way to validate that the process and procedures provided by IT and business units are complete, accurate, and known by all responsible teams?
A. Review the test objectives with stakeholders.
B. Conduct a data breach incident tabletop exercise.
C. Conduct an incident response plan survey.
D. Review data breach incident triage steps.
Answer: (SHOW ANSWER)
Conducting a tabletop exercise is the best method to validate the completeness, accuracy, and awareness of incident response procedures. The CISM Review Manual details that tabletop exercises simulate scenarios, allowing teams to test responses, clarify responsibilities, and reveal gaps in the process in a controlled environment.
Reference:ISACA CISM Review Manual, 16th Edition, Page 295, "Testing and Validating Incident Response Plans".

NEW QUESTION: 326
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?
A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials
Answer: (SHOW ANSWER)
= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.
References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

NEW QUESTION: 327
Which of the following should be the NEXT step after a security incident has been reported?
A. Recovery
B. Containment
C. Investigation

D. Escalation
Answer: (SHOW ANSWER)

NEW QUESTION: 328
Before approving the implementation of a new security solution, senior management requires a business case.
Which of the following would BEST support the justification for investment?
A. The solution contributes to business strategy.
B. The solution improves business risk tolerance levels.
C. The solution improves business resiliency.
D. The solution reduces the cost of noncompliance with regulations.
Answer: (SHOW ANSWER)
The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 329
Which of the following should an information security manager do FIRST upon confirming a privileged user's unauthorized modifications to a security application?
A. Report the risk associated with the policy breach.
B. Enforce the security configuration and require the change to be reverted.
C. Implement compensating controls to address the risk.
D. Implement a privileged access management system.
Answer: (SHOW ANSWER)
The first thing that an information security manager should do upon confirming a privileged user's unauthorized modifications to a security application is to enforce the security configuration and require the change to be reverted. This is because the unauthorized modification may have compromised the security of the application and the data it protects, and may have violated the security policies and standards of the organization. By enforcing the security configuration and requiring the change to be reverted, the information security manager can restore the security posture of the application and prevent further unauthorized modifications.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance

with the security policies and standards of the organization" and that "the information security manager should monitor and review the security configuration of information systems on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Enforcing the security configuration and requiring the change to be reverted is the correct answer because it is the most immediate and effective action to address the unauthorized modification and to maintain the security of the application" (p. 63). Additionally, the Effective Interactive Privileged Access Review article from the ISACA Journal 2018 states that "any unauthorized changes to the production environment should be reverted back to the original state and the incident should be reported to the appropriate authority" (p. 4)1.

NEW QUESTION: 330

Which of the following should be triggered FIRST when unknown malware has infected an organization's critical system?

A. Incident response plan
B. Disaster recovery plan (DRP)
C. Business continuity plan (BCP)
D. Vulnerability management plan
Answer: (SHOW ANSWER)
The document that should be triggered first when unknown malware has infected an organization's critical system is the incident response plan because it defines the roles and responsibilities, procedures and protocols, tools and techniques for responding to and managing a security incident effectively and efficiently. Disaster recovery plan (DRP) is not a good document for this purpose because it focuses on restoring the organization' s critical systems and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Business continuity plan (BCP) is not a good document for this purpose because it focuses on restoring the organization's critical business functions and operations after a major disruption or disaster, which may not be necessary or appropriate at this stage. Vulnerability management plan is not a good document for this purpose because it focuses on identifying and evaluating the security weaknesses or exposures of the organization's systems and assets, which may not be relevant or helpful at this stage.
References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons- learned https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 331
Senior management recently approved a mobile access policy that conflicts with industry best practices.
Which of the following is the information security manager's BEST course of action when developing security standards for mobile access to the organization's network?
A. Align the standards with the organizational policy.

B. Align the standards with industry best practices.
C. Resolve the discrepancy before developing the standards.
D. Perform a cost-benefit analysis of aligning the standards to policy.
Answer: (SHOW ANSWER)
The Information Security Manager's primary responsibility is to ensure that the organization's information assets are adequately protected. In this scenario, there is a conflict between the approved mobile access policy and industry best practices. Developing security standards based on a flawed policy could lead to significant security vulnerabilities.
Why the other options are not the best course of action:
A). Align the standards with the organizational policy: This would perpetuate the misalignment with best practices, potentially leaving the organization exposed to risks.
B). Align the standards with industry best practices: While this is ideal from a security perspective, it directly contradicts the approved policy, which could create operational and compliance issues.
D). Perform a cost-benefit analysis of aligning the standards to policy: A cost-benefit analysis might be useful at some point, but it does not address the fundamental issue of a policy that is not in line with best practices.
Key CISM Principles Reflected:
Alignment with Organizational Objectives: Security standards and policies should support and enable the organization's business objectives.
Risk Management: Identifying, assessing, and mitigating risks are essential elements of information security management.
Governance: Effective governance ensures that information security activities are aligned with the organization's strategies and objectives.
In summary: The Information Security Manager should proactively engage senior management to highlight the discrepancy between the approved policy and industry best practices. The goal is to revise the policy to ensure it adequately addresses security risks while supporting the organization's objectives. Once the policy is aligned with best practices, the security standards can be developed accordingly.

NEW QUESTION: 332
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

A. Communicate disciplinary processes for policy violations.
B. Require staff to participate in information security awareness training.
C. Require staff to sign confidentiality agreements.
D. Include information security responsibilities in job descriptions.
Answer: B (LEAVE A REPLY)
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: 333
The BEST way to integrate information security governance with corporate governance is to ensure:
A. the information security steering committee monitors compliance with security policies.
B. management teams embed information security into business processes.
C. awareness programs include industry best practice for information security governance.
D. the information security program is included in regular external audits.
Answer: (SHOW ANSWER)
The best way to integrate information security governance with corporate governance is for management teams to embed information security into business processes. The CISM Review Manual explains that aligning security objectives and activities with organizational goals and business processes ensures that security is a core part of business operations and strategy, not an isolated activity.
Reference:ISACA CISM Review Manual, 16th Edition, Page 38-39, "Integration of Information Security with Business Processes".

NEW QUESTION: 334
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?

A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan
Answer: (SHOW ANSWER)
The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability.
This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner.
The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

NEW QUESTION: 335
Which of the following should an information security manager do FIRST after identifying suspicious activity on a PC that is not in the organization's IT asset inventory?
A. Isolate the PC from the network
B. Perform a vulnerability scan
C. Determine why the PC is not included in the inventory
D. Reinforce information security training
Answer: (SHOW ANSWER)
The first thing an information security manager should do after identifying suspicious activity on a PC that is not in the organization's IT asset inventory is to determine why the PC is not included in the inventory. This will help to identify the source and scope of the threat, as well as the potential impact and risk to the organization. The IT asset inventory is a list of all the hardware, software, data, and other resources that are owned, controlled, or used by an organization. It helps to establish accountability, visibility, and control over the IT assets, as well as to support security policies and procedures.
If a PC is not included in the inventory, it may indicate that it has been compromised by an unauthorized user or entity, or that it has been moved or transferred without proper authorization. It may also indicate that there are gaps or errors in the inventory management process, such as

missing records, duplicate entries, outdated information, or inaccurate classification. These issues can pose significant challenges for information security management, such as:
* Lack of visibility into the IT environment and assets
* Difficulty in detecting and responding to incidents
* Increased risk of data breaches and cyberattacks
* Non-compliance with regulatory requirements and standards
* Reduced trust and confidence among stakeholders
Therefore, an information security manager should take immediate steps to investigate why the PC is not included in the inventory and take appropriate actions to remediate the situation.
References = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Inventory Management1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 336
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?
A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.
Answer: (SHOW ANSWER)
The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

NEW QUESTION: 337
An online bank identifies a successful network attack in progress. The bank should FIRST:
A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (PII) is compromised.
D. shut down the entire network.
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: 338
A security incident has been reported within an organization. When should an information security manager contact the information owner?
A. After the incident has been contained
B. After the incident has been mitigated
C. After the incident has been confirmed
D. After the potential incident has been logged
Answer: (SHOW ANSWER)
The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 339
Which of the following is the MOST effective way to identify changes in an information security environment?
A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring
Answer: (SHOW ANSWER)
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

NEW QUESTION: 340
Which of the following should an information security manager do FIRST when creating an organization's disaster recovery plan (DRP)?

A. Conduct a business impact analysis (BIA)
B. Identify the response and recovery learns.
C. Review the communications plan.
D. Develop response and recovery strategies.
Answer: (SHOW ANSWER)
Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)2. Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate solutions and procedures for restoring the critical business functions or processes.
References: 2 https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business-impact-analysis- bia-and-disaster-recovery-planning-drp

NEW QUESTION: 341
Which of the following should be the PRIMARY consideration when developing an incident response plan?
A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents
Answer: (SHOW ANSWER)
Management support is the primary consideration when developing an incident response plan, as it is essential for obtaining the necessary resources, authority, and commitment for the plan. Management support also helps to ensure that the plan is aligned with the organization's business objectives, risk appetite, and security strategy, and that it is communicated and enforced across the organization. Management support also facilitates the coordination and collaboration among different stakeholders, such as business units, IT functions, legal, public relations, and external parties, during an incident response.
The definition of an incident (A) is an important component of the incident response plan, as it provides the criteria and thresholds for identifying, classifying, and reporting security incidents. However, the definition of an incident is not the primary consideration, as it is derived from the organization's security policies, standards, and procedures, and may vary depending on the context and impact of the incident.
Compliance with regulations (B) is also an important factor for the incident response plan, as it helps to ensure that the organization meets its legal and contractual obligations, such as notifying

the authorities, customers, or partners of a security breach, preserving the evidence, and reporting the incident outcomes.
However, compliance with regulations is not the primary consideration, as it is influenced by the nature and scope of the incident, and the applicable laws and regulations in different jurisdictions.
Previously reported incidents (D) are a valuable source of information and lessons learned for the incident response plan, as they help to identify the common types, causes, and impacts of security incidents, as well as the strengths and weaknesses of the current incident response processes and capabilities. However, previously reported incidents are not the primary consideration, as they are not predictive or comprehensive of the future incidents, and may not reflect the changing threat landscape and business environment.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 181-1821 Learn more:

NEW QUESTION: 342
An organization has an ongoing security awareness training program. Employee participation has been decreasing over the year, while the number of malware and phishing incidents from email has been increasing. What is the information security manager's BEST course of action?
A. Report the findings to senior management with recommendations.
B. Implement a phishing reporting tool in the email system.
C. Include regular phishing campaigns after each training session.
D. Make the training program mandatory for all employees.
Answer: (SHOW ANSWER)
If participation in security awareness training is decreasing while incidents are rising, making the training program mandatory for all employees is the best course of action. The CISM Review Manual notes that mandatory training ensures organizational-wide coverage and directly addresses the lack of participation, which is likely contributing to increased incidents.
Reference:ISACA CISM Review Manual, 16th Edition, Page 220-221, "Awareness and Training - Ensuring Coverage".

NEW QUESTION: 343
When an organization experiences a disruptive event, the business continuity plan (BCP) should be triggered PRIMARILY based on:
A. expected duration of outage.
B. management direction.
C. type of security incident.
D. the root cause of the event.
Answer: (SHOW ANSWER)
The expected duration of outage is the primary factor that should trigger the BCP because it indicates how long the organization can tolerate the disruption of its critical business processes and functions before it causes unacceptable consequences. The expected duration of outage is determined by the recovery time objectives (RTOs) that are defined for each critical business

process and function based on the business impact analysis (BIA). The BCP should be triggered when the expected duration of outage exceeds or is likely to exceed the RTOs.
References: The CISM Review Manual 2023 defines RTO as "the maximum acceptable time that a service can be unavailable or disrupted before it causes unacceptable consequences" and states that "the RTO is determined based on the impact of service interruption on the enterprise's business processes, reputation, customers, and stakeholders" (p. 189). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Expected duration of outage is the correct answer because it is the primary factor that should trigger the BCP, as it reflects the maximum time that the organization can afford to lose its critical business processes and functions without causing unacceptable consequences" (p. 96). Additionally, the article Invoking your business continuity plan: five triggers, six decision points from the ITWeb website states that "the expected duration of outage is the most important consideration when deciding to invoke the BCP, as it indicates how long the organization can sustain the disruption before it impacts its business objectives, operations, reputation, and legal obligations" (p. 2)

NEW QUESTION: 344
Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?
A. Providing training from third-party forensics firms
B. Obtaining industry certifications for the response team
C. Conducting tabletop exercises appropriate for the organization
D. Documenting multiple scenarios for the organization and response steps
Answer: (SHOW ANSWER)
The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.
According to the Certified Information Security Manager (CISM) Study Manual, "Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan." While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.
Reference:

Certified Information Security Manager (CISM) Study Manual, 15th Edition, Page 324.

NEW QUESTION: 345
An organization learns that a third party has outsourced critical functions to another external provider. Which of the following is the information security manager's MOST important course of action?
A. Engage an independent audit of the third party's external provider.
B. Recommend canceling the contract with the third party.
C. Evaluate the third party's agreements with its external provider.
D. Conduct an external audit of the contracted third party.
Answer: C (LEAVE A REPLY)
According to the CISM Review Manual, the information security manager should evaluate the third party's agreements with its external provider to ensure that the security requirements and controls are adequate and consistent with the organization's expectations. Engaging or conducting an audit may be a subsequent step, but not the most important one. Recommending canceling the contract may be premature and impractical.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.2, page 1431.

NEW QUESTION: 346
Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?
A. Available annual budget
B. Cost-benefit analysis of mitigating controls
C. Recovery time objective (RTO)
D. Maximum tolerable outage (MTO)
Answer: (SHOW ANSWER)
Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk events." CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise." CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

NEW QUESTION: 347
Which of the following BEST enables the assignment of risk and control ownership?
A. Aligning to an industry-recognized control framework
B. Adopting a risk management framework
C. Obtaining senior management buy-in
D. Developing an information security strategy
Answer: (SHOW ANSWER)
Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.
References:
* https://www.protechtgroup.com/en-au/blog/risk-control-management
* https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_risk_ownership_right.ashx
* https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

NEW QUESTION: 348
An organization plans to leverage popular social network platforms to promote its products and services.
Which of the following is the BEST course of action for the information security manager to support this initiative?
A. Establish processes to publish content on social networks.
B. Assess the security risk associated with the use of social networks.
C. Conduct vulnerability assessments on social network platforms.
D. Develop security controls for the use of social networks.
Answer: (SHOW ANSWER)

The best course of action for the information security manager to support the initiative of leveraging popular social network platforms to promote the organization's products and services is to assess the security risk associated with the use of social networks. Security risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a security risk assessment, the information security manager can provide valuable input to the decision-making process regarding the benefits and costs of using social networks, as well as the appropriate security controls and mitigation strategies to reduce the risk to an acceptable level. The other options are not the best course of action, although they may be part of the security risk management process. Establishing processes to publish content on social networks is an operational task that should be performed after assessing the security risk and implementing the necessary controls. Conducting vulnerability assessments on social network platforms is a technical activity that may not be feasible or effective, as the organization does not have control over the platforms' infrastructure and configuration. Developing security controls for the use of social networks is a preventive measure that should be based on the results of the security risk assessment and aligned with the organization's risk appetite and tolerance

NEW QUESTION: 349
When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?
A. Business process owner
B. Business continuity coordinator
C. Senior management
D. Information security manager
Answer: (SHOW ANSWER)
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: 350

Which of the following is the GREATEST benefit of information asset classification?

A. Helping to determine the recovery point objective (RPO)

B. Providing a basis for implementing a need-to-know policy

C. Supporting segregation of duties

D. Defining resource ownership

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: 351
Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?
A. Create a security exception.
B. Perform a gap analysis to determine needed resources.
C. Perform a vulnerability assessment.
D. Assess the risk to business operations.
Answer: (SHOW ANSWER)
The information security manager should first assess the risk to business operations that are caused by the information security issues reported by internal audit. This will help to prioritize the remediation actions and allocate the necessary resources. Creating a security exception, performing a gap analysis, or performing a vulnerability assessment are possible subsequent steps, but they are not the first action to take.
References = CISM Review Manual, 16th Edition, page 48

NEW QUESTION: 352

Of the following, who is in the BEST position to evaluate business impacts?
A. Senior management
B. Information security manager
C. IT manager
D. Process manager
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: 353
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST to support this initiative?
A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.
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: 354
Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?
A. Documentation of control procedures
B. Standardization of compliance requirements
C. Automation of controls
D. Integration of assurance efforts
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: 355
Information security controls should be designed PRIMARILY based on:
A. a business impact analysis (BIA).
B. regulatory requirements.
C. business risk scenarios,
D. a vulnerability assessment.
Answer: (SHOW ANSWER)
Information security controls should be designed primarily based on business risk scenarios, because they help to identify and prioritize the most relevant and significant threats and vulnerabilities that may affect the organization's information assets and business objectives. Business risk scenarios are hypothetical situations that describe the possible sources, events, and consequences of a security breach, as well as the likelihood and impact of the occurrence. Business risk scenarios can help to:
Align the information security controls with the business needs and requirements, and ensure that they support the achievement of the strategic goals and the mission and vision of the organization Assess the effectiveness and efficiency of the existing information security controls, and identify the gaps and weaknesses that need to be addressed or improved Select and implement the appropriate information security controls that can prevent, detect, or mitigate the risks, and that can provide the optimal level of protection and performance for the information assets Evaluate and measure the return on investment and the value proposition of the information security controls, and communicate and justify the rationale and benefits of the controls to the stakeholders and management Information security controls should not be designed primarily based on a business impact analysis (BIA), regulatory requirements, or a vulnerability assessment, because these are secondary or complementary factors that influence the design of the controls, but they do not provide the main basis or criteria for the design. A BIA is a method of estimating and comparing the potential effects of a disruption or a disaster on the critical business functions and processes, in terms of financial, operational, and reputational aspects. A BIA can help to determine the recovery objectives and priorities for the information assets, but it does not identify or address the specific risks and threats that may cause the disruption or the disaster. Regulatory requirements are the legal, contractual, or industry standards and obligations that the organization must comply with regarding information security. Regulatory requirements can help to establish the minimum or baseline level of information security controls that the organization must implement, but they do not reflect the specific or unique needs and challenges of the organization. A vulnerability assessment is a method of identifying and analyzing the weaknesses and flaws in the information systems and assets that may expose them to exploitation or compromise. A vulnerability assessment can help to discover and remediate the existing or potential security issues, but it does not consider the business context or impact of the issues. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 119-120, 122-123, 125-126, 129-130.

NEW QUESTION: 356

An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?

A. Document risk acceptances.

B. Revise the organization's security policy.

C. Assess the consequences of noncompliance.

D. Conduct an information security audit.

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: 357

Which of the following is the BEST approach for data owners to use when defining access privileges for users?

A. Define access privileges based on user roles.

B. Adopt user account settings recommended by the vendor.

C. Perform a risk assessment of the users' access privileges.

D. Implement an identity and access management (IDM) tool.

Answer: (SHOW ANSWER)

This approach is the best because it ensures that users have the minimum level of access required to perform their job functions, which reduces the risk of unauthorized access or misuse of data. User roles are defined based on the business needs and responsibilities of the users, and they can be easily managed and audited.

References: The CISM Review Manual 2023 states that "the data owner is responsible for defining the access privileges for each user role" and that "the data owner should ensure that the principle of least privilege is applied to all users" (p. 82). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Defining access privileges based on user roles is the best approach because it allows the data owner to assign the minimum level of access required for each role and to review and update the roles periodically" (p. 23).

NEW QUESTION: 358

Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?

A. Low number of false positives

B. Low number of false negatives

C. High number of false positives

D. High number of false negatives

Answer: D (LEAVE A REPLY)

A false negative is a security incident that was not detected by the SIEM system, which presents the greatest risk as it allows attackers to compromise the organization's assets and data without being noticed or stopped.

A high number of false negatives can indicate that the SIEM system is not configured properly, has insufficient data sources, or lacks effective analytics and correlation rules. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 359

Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.

B. Internal compliance requirements are being met.

C. Risk management objectives are being met.

D. Business needs are being met.

Answer: D (LEAVE A REPLY)

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: 360

A risk assessment exercise has identified the threat of a denial of service (DoS) attack Executive management has decided to take no further action related to this risk. The MO ST likely reason for this decision is

A. the risk assessment has not defined the likelihood of occurrence

B. the reported vulnerability has not been validated

C. executive management is not aware of the impact potential

D. the cost of implementing controls exceeds the potential financial losses.

Answer: (SHOW ANSWER)

The most likely reason for executive management to take no further action related to the risk of a denial of service (DoS) attack is that the cost of implementing controls exceeds the potential financial losses. This means that the risk is acceptable or tolerable for the organization, and that the benefits of reducing the risk do not outweigh the costs of applying the controls. This decision is based on a cost-benefit analysis, which is a common technique for evaluating and comparing different risk response options. A cost-benefit analysis considers the following factors:

The estimated impact of the risk, which is the potential loss or damage that the organization may suffer if the risk materializes. The impact can be expressed in quantitative or qualitative terms, such as monetary value, reputation, customer satisfaction, legal liability, etc.

The estimated likelihood of occurrence, which is the probability or frequency that the risk will occur within a given time period. The likelihood can be expressed in numerical or descriptive terms, such as percentage, rating, high, medium, low, etc.

The estimated cost of controls, which is the total amount of resources that the organization needs to invest in order to implement and maintain the controls. The cost can include direct and indirect expenses, such as hardware, software, personnel, training, maintenance, etc.

The estimated benefit of controls, which is the reduction in the impact or likelihood of the risk as a result of implementing the controls. The benefit can be expressed in the same terms as the impact or likelihood, such as monetary value, percentage, rating, etc.

A cost-benefit analysis can be performed using various methods, such as net present value (NPV), return on investment (ROI), internal rate of return (IRR), etc. The general principle is to compare the cost and benefit of each control option, and select the one that provides the highest net benefit or the lowest net cost. A control option is considered feasible and desirable if its benefit exceeds its cost, or if its cost is lower than the impact of the risk.

In this case, executive management has decided to take no further action related to the risk of a DoS attack, which implies that the cost of implementing controls exceeds the potential financial losses. This could be because the impact or likelihood of the risk is low, or because the cost or complexity of the controls is high, or both. For example, the organization may have a robust backup and recovery system, a diversified network infrastructure, a strong customer loyalty, or a low dependency on online services, which reduce the impact or likelihood of a DoS attack. Alternatively, the organization may face technical, financial, or operational challenges in implementing effective controls, such as firewalls, load balancers, traffic filters, or cloud services, which increase the cost or complexity of the controls. Therefore, executive management may have concluded that the risk is acceptable or tolerable, and that taking no further action is the most rational and economical choice.
The other options are not the most likely reasons for executive management to take no further action related to the risk of a DoS attack, as they indicate a lack of proper risk assessment or validation. The risk assessment should define the likelihood of occurrence and the reported vulnerability should be validated, as these are essential steps for identifying and analyzing the risk. Executive management should be aware of the impact potential, as this is a key factor for evaluating and prioritizing the risk. If any of these options were true, executive management would not have enough information or evidence to make an informed and justified decision about the risk response. References = CISM Review Manual, Chapter 2, pages 67-69 CISM Exam Content Outline | CISM Certification | ISACA, Domain 2, Task 2.2 Information Security Risk Management for CISM - Pluralsight, Module 2, Section 2.3 CISM: Information Risk Management Part 2 from Skillsoft - NICCS, Section 2.4 Executive management may not take action related to a risk if they have determined that the cost of implementing necessary controls to mitigate the risk exceeds the potential financial losses that the organization may incur if the risk were to materialize. In cases such as this, it is important for the information security team to provide the executive team with thorough cost-benefit analysis that outlines the cost of implementing the controls versus the expected losses from the risk.

NEW QUESTION: 361
What type of control is being implemented when a security information and event management (SIEM) system is installed?
A. Preventive
B. Deterrent
C. Detective
D. Corrective
Answer: C (LEAVE A REPLY)
A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns

any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. 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: 362
Which of the following is the BEST method for determining whether a firewall has been configured to provide a comprehensive perimeter defense9
A. A validation of the current firewall rule set
B. A port scan of the firewall from an internal source
C. A ping test from an external source
D. A simulated denial of service (DoS) attack against the firewall
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: 363

What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?
A. Vendor service level agreements (SLAs)
B. Independent review of the vendor
C. Local laws and regulations
D. Backup and restoration of data
Answer: C (LEAVE A REPLY)
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: 364
An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?
A. Set up communication channels for the target audience.
B. Determine the needs and requirements of each audience.
C. Create a comprehensive singular communication
D. Invoke the organization's incident response plan.
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: 365
Which of the following is the PRIMARY role of the information security manager in application development?
A. To ensure security is integrated into the system development life cycle (SDLC)
B. To ensure compliance with industry best practice
C. To ensure enterprise security controls are implemented
D. To ensure control procedures address business risk
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: 366
A penetration test against an organization's external web application shows several vulnerabilities. Which of the following presents the GREATEST concern?
A. A rules of engagement form was not signed prior to the penetration test
B. Vulnerabilities were not found by internal tests
C. Vulnerabilities were caused by insufficient user acceptance testing (UAT)
D. Exploit code for one of the vulnerabilities is publicly available
Answer: (SHOW ANSWER)
Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.
References:
https://www.imperva.com/learn/application-security/penetration-testing/
https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web- application-for-vulnerabilities/

NEW QUESTION: 367
What should a global information security manager do FIRST when informed that a new regulation with significant impact will go into effect soon?
A. Perform a vulnerability assessment.
B. Perform a privacy impact assessment (PIA).
C. Perform a business impact analysis (BIA).
D. Perform a gap analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 368
An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?
A. Identification of risk
B. Analysis of control gaps

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

NEW QUESTION: 369
Which of the following should be the MOST important consideration when establishing information security policies for an organization?
A. Job descriptions include requirements to read security policies.
B. The policies are updated annually.
C. Senior management supports the policies.
D. The policies are aligned to industry best practices.
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: 370

Which of the following should be of GREATEST concern regarding an organization's security controls?

A. Some controls are performing outside of an acceptable range.
B. No key control indicators (KCIs) have been implemented.
C. Control ownership has not been updated.
D. Control gap analysis is outdated.
Answer: (SHOW ANSWER)
Key Control Indicators (KCIs) are essential to measuring the effectiveness and performance of security controls. Without them:
The organization cannot assess if controls are working as intended
It's difficult to demonstrate due diligence
Risks may go unnoticed
While other answers point to operational concerns, the complete absence of KCIs presents a critical governance gap that compromises the organization's ability to monitor and manage control health.
"KCIs provide actionable metrics that support proactive control management and are fundamental to governance and assurance."
- CISM Review Manual 15th Edition, Chapter 1: Governance Metrics and Reporting*

NEW QUESTION: 371
Which of the following is the GREATEST benefit of incorporating information security governance into the corporate governance framework?
A. Heightened awareness of information security strategies
B. Improved process resiliency in the event of attacks
C. Promotion of security-by-design principles to the business
D. Management accountability for information security
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: 372
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?
A. Configuration management
B. Risk management
C. Access control management
D. Change management
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: 373
Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?
A. Decrease in the number of security incidents
B. Increase in the frequency of security incident escalations
C. Reduction in the impact of security incidents
D. Increase in the number of reported security incidents
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: 374
Which of the following is MOST important to the successful implementation of an information security program?
A. Adequate security resources are allocated to the program.
B. Key performance indicators (KPIs) are defined.
C. A balanced scorecard is approved by the steering committee.

D. The program is developed using global security standards.

Answer: (SHOW ANSWER)

The successful implementation of an information security program depends largely on the availability and allocation of adequate security resources, such as budget, staff, technology, and training. Without sufficient resources, the program may not be able to achieve its objectives, comply with the security strategy, or address the security risks. Key performance indicators (KPIs), a balanced scorecard, and global security standards are also important elements of an information security program, but they are not as critical as the resource allocation.

References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION: 375

During which of the following development phases is it MOST challenging to implement security controls?

A. Post-implementation phase

B. Implementation phase

C. Development phase

D. Design phase

Answer: (SHOW ANSWER)

The development phase is the stage of the system development life cycle (SDLC) where the system requirements, design, architecture, and implementation are performed. The development phase is most challenging to implement security controls because it involves complex and dynamic processes that may not be well understood or documented. Security controls are essential for ensuring the confidentiality, integrity, and availability of the system and its data, as well as for complying with regulatory and contractual obligations. However, security controls may also introduce additional costs, risks, and constraints to the development process, such as: Increased complexity and overhead of testing, verification, validation, and maintenance Reduced flexibility and agility of changing requirements or design Increased dependency on external vendors or third parties for security services or products Increased vulnerability to errors, defects, or vulnerabilities in the code or configuration Increased difficulty in measuring and reporting on security performance or effectiveness Therefore, implementing security controls in the development phase requires careful planning, coordination, communication, and collaboration among all stakeholders involved in the SDLC. It also requires a clear understanding of the security objectives, scope, criteria, standards, policies, procedures, roles, responsibilities, and resources for the system. Moreover, it requires a proactive approach to identifying and mitigating potential threats or risks that may affect the security of the system.

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

System Development Life Cycle (SDLC)2

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: https://store.isaca.org/s

/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 376
Which of the following is MOST important for an information security manager to consider when developing a business continuity plan (BCP) for ransomware attacks?
A. Impacted networks can be detached at the network switch level.
B. Backups are maintained offline and regularly tested.
C. Production data is continuously replicated between primary and secondary sites.
D. Backups are maintained on multiple sites and regularly reviewed.
Answer: (SHOW ANSWER)

NEW QUESTION: 377
Following a successful attack, an information security manager should be confident the malware @ continued to spread at the completion of which incident response phase?
A. Containment
B. Recovery
C. Eradication
D. Identification
Answer: (SHOW ANSWER)
According to the CISM Review Manual (Digital Version), page 212, the incident response process consists of six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Containment is the phase where the incident response team isolates the affected systems or networks to prevent further damage or spread of the malware. Eradication is the phase where the incident response team removes the malware and any traces of its activity from the affected systems or networks. Recovery is the phase where the incident response team restores the normal operations of the systems or networks. Identification is the phase where the incident response team detects and analyzes the signs of the incident. Therefore, the information security manager should be confident that the malware has not continued to spread at the completion of the containment phase, which is the earliest phase where the incident response team can stop the propagation of the malware. References = 1: CISM Review Manual (Digital Version), page 212

NEW QUESTION: 378

Which of the following is the BEST approach to incident response for an organization migrating to a cloud- based solution?

A. Adopt the cloud provider's incident response procedures.

B. Transfer responsibility for incident response to the cloud provider.

C. Continue using the existing incident response procedures.

D. Revise incident response procedures to encompass the cloud environment.

Answer: (SHOW ANSWER)

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: 379

An organization's information security manager reads on social media that a recently purchased vendor product has been compromised and customer data has been posted online. What should the information security manager do FIRST?

A. Perform a business impact analysis (BIA).

B. Notify local law enforcement agencies of a breach.

C. Activate the incident response program.

D. Validate the risk to the organization.

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: 380

Which of the following BEST indicates the organizational benefit of an information security solution?

A. Cost savings the solution brings to the information security department
B. Reduced security training requirements
C. Alignment to security threats and risks
D. Costs and benefits of the solution calculated over time

Answer: (SHOW ANSWER)

The best option to indicate the organizational benefit of an information security solution is D. Costs and benefits of the solution calculated over time. This is because costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. ROSI can also help to justify the allocation and optimization of the resources and budget for the information security solution, and to compare and prioritize different security alternatives.
ROSI can be calculated by using various methods and formulas, such as the annualized loss expectancy (ALE), the annualized rate of occurrence (ARO), and the cost-benefit analysis (CBA). Costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the

information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.3, page 1311; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 99, page 26; How to Calculate Return on Security Investment (ROSI) - Infosec2

NEW QUESTION: 381
Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?
A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure
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: 382
Which of the following BEST enables the integration of information security governance into corporate governance?
A. Well-decumented information security policies and standards
B. An information security steering committee with business representation
C. Clear lines of authority across the organization
D. Senior management approval of the information security strategy
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: 383
Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?
A. Conduct an information security audit on the third-party vendor.
B. Ensure security is involved in the procurement process.
C. Review the third-party contract with the organization's legal department.
D. Communicate security policy with the third-party vendor.
Answer: (SHOW ANSWER)

NEW QUESTION: 384
Which of the following is MOST important when defining how an information security budget should be allocated?
A. Regulatory compliance standards
B. Information security strategy
C. Information security policy
D. Business impact assessment
Answer: (SHOW ANSWER)
Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are-shaping-up.html
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

NEW QUESTION: 385
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?
A. The time and location that the breach occurred

B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error
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: 386
An information security manager believes that information has been classified inappropriately, = the risk of a breach. Which of the following is the information security manager's BEST action?
A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.
D. Complete a risk assessment and refer the results to the data owners.
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: 387
Which of the following is a PRIMARY responsibility of the information security goxernance function?
A. Administering information security awareness training
B. Defining security strategies to support organizational programs
C. Ensuring adequate support for solutions using emerging technologies
D. Advising senior management on optimal levels of risk appetite and tolerance
Answer: (SHOW ANSWER)
Defining security strategies to support organizational programs is a primary responsibility of the information security governance function, as it involves providing strategic direction for security activities and ensuring that objectives are achieved. According to ISACA, information security governance is a subset of corporate governance that provides guidance for aligning information

security with business objectives, managing information security risks, and using information resources responsibly12.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12

NEW QUESTION: 388
Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?
A. Implement mitigating actions immediately.
B. Invoke the incident response plan.
C. Inform senior management of the breach.
D. Validate the breach.
Answer: (SHOW ANSWER)
The first step when a potential breach is discovered is to validate the breach. According to the CISM Review Manual, Domain 4, the information security manager must confirm the event to avoid unnecessary escalation or resource allocation. This validation ensures that the incident is real and justifies further response actions. Invoking the incident response plan or informing management comes after the breach is validated.
Reference:ISACA CISM Review Manual, 16th Edition, Page 280, "Incident Detection and Validation".

NEW QUESTION: 389
The BEST way to report to the board on the effectiveness of the information security program is to present:
A. a report of cost savings from process improvements.
B. peer-group industry benchmarks.
C. a dashboard illustrating key performance metrics.
D. a summary of the most recent audit findings.
Answer: (SHOW ANSWER)