

Isaca

Exam Questions CISM

Certified Information Security Manager



NEW QUESTION 1

- (Topic 1)

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: B

Explanation:

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 2

- (Topic 1)

An organization is implementing an information security governance framework. To communicate the program's effectiveness to stakeholders, it is MOST important to establish:

- A. a control self-assessment (CSA) process.
- B. automated reporting to stakeholders.
- C. a monitoring process for the security policy.
- D. metrics for each milestone.

Answer: D

Explanation:

= Establishing metrics for each milestone is the best way to communicate the program's effectiveness to stakeholders, as it provides a clear and measurable way to track the progress, performance, and outcomes of the information security governance framework. Metrics are quantifiable indicators that can be used to evaluate the achievement of specific objectives, goals, or standards. Metrics can also help to demonstrate the value, benefits, and return on investment of the information security program, as well as to identify and address the gaps, issues, or risks. Metrics for each milestone should be aligned with the organization's strategy, vision, and mission, as well as with the expectations and needs of the stakeholders. Metrics for each milestone should also be SMART (specific, measurable, achievable, relevant, and time-bound), as well as consistent, reliable, and transparent.

The other options are not as important as establishing metrics for each milestone, as they do not provide a comprehensive and holistic way to communicate the program's effectiveness to stakeholders. A control self-assessment (CSA) process is a technique to involve the staff in assessing the design, implementation, and effectiveness of the information security controls. It can help to increase the awareness, ownership, and accountability of the staff, as well as to identify and mitigate the risks. However, a CSA process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not measure the overall performance or maturity of the information security program. Automated reporting to stakeholders is a method to provide timely, accurate, and consistent information to the stakeholders about the status, results, and issues of the information security program. It can help to facilitate the communication, collaboration, and decision making among the stakeholders, as well as to ensure the compliance and transparency of the information security program. However, automated reporting alone is not enough to communicate the program's effectiveness to stakeholders, as it does not evaluate the achievement or impact of the information security program. A monitoring process for the security policy is a process to ensure that the security policy is implemented, enforced, and reviewed in accordance with the organization's objectives, standards, and regulations. It can help to maintain the relevance, adequacy, and effectiveness of the security policy, as well as to incorporate the feedback, changes, and improvements. However, a monitoring process alone is not enough to communicate the program's effectiveness to stakeholders, as it does not cover the other aspects of the information security program, such as governance, risk management, incident management, or business continuity. References =

? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1018.

? CISM domain 1: Information security governance [Updated 2022], Infosec, 1.

? Key Performance Indicators for Security Governance, Part 1, ISACA Journal, Volume 6, 2020, 2.

NEW QUESTION 3

- (Topic 1)

An information security manager learns that IT personnel are not adhering to the information security policy because it creates process inefficiencies. What should the information security manager do FIRST?

- A. Conduct user awareness training within the IT function.
- B. Propose that IT update information security policies and procedures.
- C. Determine the risk related to noncompliance with the policy.
- D. Request that internal audit conduct a review of the policy development process,

Answer: C

Explanation:

The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to

communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

NEW QUESTION 4

- (Topic 1)

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: B

Explanation:

= 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 5

- (Topic 1)

Which of the following MUST happen immediately following the identification of a malware incident?

- A. Preparation
- B. Recovery
- C. Containment
- D. Eradication

Answer: C

Explanation:

Containment is the action that MUST happen immediately following the identification of a malware incident because it aims to isolate the affected systems or networks from the rest of the environment and prevent the spread or escalation of the malware. Containment can involve disconnecting the 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. Containment is part of the incident response process and should be performed as soon as possible after detecting a malware incident¹². Preparation (A) is the phase that happens before the identification of a malware incident, where the organization establishes the incident response plan, team, roles, resources, and tools. Preparation is essential for ensuring the readiness and capability of the organization to respond to malware incidents effectively and efficiently¹². Recovery (B) is the phase that happens after the containment and eradication of a malware incident, where the organization restores the normal operations of the systems or networks, verifies the functionality and security of the systems or networks, and implements the preventive and corrective measures to avoid or mitigate future malware incidents. Recovery is the final phase of the incident response process and should be performed after ensuring that the malware incident is fully resolved and the systems or networks are clean and secure¹². Eradication (D) is the phase that happens after the containment of a malware incident, where the organization removes the malware and its traces from the systems or networks, identifies the root cause and impact of the malware incident, and collects and preserves the evidence for analysis and investigation. Eradication is an important phase of the incident response process, but it does not happen immediately after the identification of a malware incident¹². References = 1: CISM Review Manual 15th Edition, page 308-3091; 2: Cybersecurity Incident Response Exercise Guidance - ISACA²

NEW QUESTION 6

- (Topic 1)

Which of the following is MOST effective in monitoring an organization's existing risk?

- A. Periodic updates to risk register
- B. Risk management dashboards
- C. Security information and event management (SIEM) systems
- D. Vulnerability assessment results

Answer: B

Explanation:

Risk management dashboards are the MOST effective in monitoring an organization's existing risk because they provide a visual and interactive representation of the key risk indicators (KRIs) and metrics that reflect the current risk posture and performance of the organization. Risk management dashboards can help to communicate the risk information to various stakeholders, identify trends and patterns, compare actual results with targets and thresholds, and support decision making and risk response¹². Periodic updates to risk register (A) are important to maintain the accuracy and relevance of the risk information, but they are not the most effective in monitoring the existing risk because they do not provide a real-time or dynamic view of the risk situation. Security information and event management (SIEM) systems © are effective in monitoring the security events and incidents that may indicate potential or actual threats to the organization, but they are not the most effective in monitoring the existing risk because they do not provide a comprehensive or holistic view of the risk context and impact. Vulnerability assessment results (D) are effective in monitoring the weaknesses and exposures of the organization's assets and systems, but they are not the most effective in monitoring the existing risk because they do not provide a quantitative or qualitative measure of the risk likelihood and consequence. References = 1: CISM Review Manual 15th Edition, page 316-3171; 2: CISM Domain 2: Information Risk Management (IRM) [2022 update]²

NEW QUESTION 7

- (Topic 1)

Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

- A. Increase the frequency of system backups.
- B. Review the mitigating security controls.
- C. Notify staff members of the threat.
- D. Assess the risk to the organization.

Answer: D

Explanation:

The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance. A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness. The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat © is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. References = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

NEW QUESTION 8

- (Topic 1)

Penetration testing is MOST appropriate when a:

- A. new system is about to go live.
- B. new system is being designed.
- C. security policy is being developed.
- D. security incident has occurred,

Answer: A

Explanation:

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

NEW QUESTION 9

- (Topic 1)

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: A

Explanation:

= 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 10

- (Topic 1)

Which of the following BEST enables staff acceptance of information security policies?

- A. Strong senior management support
- B. Computer-based training
- C. Arobust incident response program
- D. Adequate security funding

Answer: A

Explanation:

= 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 10

- (Topic 1)

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: B

Explanation:

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 13

- (Topic 1)

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: D

Explanation:

= 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 16

- (Topic 1)

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: D

Explanation:

Alignment between corporate and information security governance means that the information security program supports the organizational goals and objectives, and is integrated into the enterprise governance structure. The best evidence of alignment is the senior management sponsorship, which demonstrates the commitment and support of the top-level executives and board members for the information security program. Senior management sponsorship also ensures that the information security program has adequate resources, authority, and accountability to achieve its objectives and address the risks and issues that affect the organization. Senior management sponsorship also helps to establish a culture of security awareness and compliance throughout the organization, and to communicate the value and benefits of the information security program to the stakeholders.

References =

- ? CISM Review Manual 15th Edition, page 1631
- ? CISM 2020: Information Security & Business Process Alignment, video 22
- ? Certified Information Security Manager (CISM), page 33

NEW QUESTION 18

- (Topic 1)

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: D

Explanation:

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 19

- (Topic 1)

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: D

Explanation:

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 20

- (Topic 1)

Which of the following BEST supports information security management in the event of organizational changes in security personnel?

- A. Formalizing a security strategy and program
- B. Developing an awareness program for staff
- C. Ensuring current documentation of security processes
- D. Establishing processes within the security operations team

Answer: C

Explanation:

Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION 22

- (Topic 1)

Which of the following BEST ensures information security governance is aligned with corporate governance?

- A. A security steering committee including IT representation
- B. A consistent risk management approach
- C. An information security risk register
- D. Integration of security reporting into corporate reporting

Answer: D

Explanation:

The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with corporate governance by themselves. References = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

NEW QUESTION 26

- (Topic 1)

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

- A. Including service level agreements (SLAs) in vendor contracts
- B. Establishing communication paths with vendors
- C. Requiring security awareness training for vendor staff
- D. Performing integration testing with vendor systems

Answer: B

Explanation:

The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.

The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non-compliance. However, SLAs do not necessarily address the specific procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties. Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems. However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management. References = 1, 2, 3, 4, 5 <https://niccs.cisa.gov/education-training/catalog/skillssoft/cism-information-security-incident-management-part-1>
<https://niccs.cisa.gov/education-training/catalog/skillssoft/cism-information-security-incident-management-part-1>

NEW QUESTION 30

- (Topic 1)

Which of the following is the MOST important criterion when deciding whether to accept residual risk?

- A. Cost of replacing the asset
- B. Cost of additional mitigation
- C. Annual loss expectancy (ALE)
- D. Annual rate of occurrence

Answer: C

Explanation:

= Annual loss expectancy (ALE) is the most important criterion when deciding whether to accept residual risk, because it represents the expected monetary loss for an asset due to a risk over a one-year period. ALE is calculated by multiplying the annual rate of occurrence (ARO) of a risk event by the single loss expectancy (SLE) of the asset. ARO is the estimated frequency of a risk event occurring within a one-year period, and SLE is the estimated cost of a single occurrence of a

risk event. ALE helps to compare the cost and benefit of different risk responses, such as avoidance, mitigation, transfer, or acceptance. Risk acceptance is appropriate when the ALE is lower than the cost of other risk responses, or when the risk is unavoidable or acceptable within the organization's risk appetite and tolerance. ALE also helps to prioritize the risks that need more attention and resources.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 831; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 22, page 242

NEW QUESTION 31

- (Topic 1)

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

Explanation:

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 34

- (Topic 1)

Which of the following is the MOST important consideration when establishing an organization's information security governance committee?

- A. Members have knowledge of information security controls.
- B. Members are business risk owners.
- C. Members are rotated periodically.
- D. Members represent functions across the organization.

Answer: D

Explanation:

= The most important consideration when establishing an organization's information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization's business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization's mission, vision, and values. Having a diverse and representative committee also helps to foster a culture of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.

Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization's business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization's business objectives, and to allocate appropriate resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the organization's information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee's ability to monitor and evaluate the performance and progress of the information security program. References =

? ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37.

? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1014.

NEW QUESTION 36

- (Topic 1)

Which of the following is MOST important for building a 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: A

Explanation:

= 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 37

- (Topic 1)

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: D

Explanation:

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 38

- (Topic 1)

Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

- A. Threat management is enhanced.
- B. Compliance status is improved.
- C. Security metrics are enhanced.
- D. Proactive risk management is facilitated.

Answer: D

Explanation:

A vulnerability assessment process is a systematic and proactive approach to identify, analyze and prioritize the vulnerabilities in an information system. It helps to reduce the exposure of the system to potential threats and improve the security posture of the organization. By implementing a vulnerability assessment process, the organization can facilitate proactive risk management, which is the PRIMARY benefit of this process. Proactive risk management is the process of identifying, assessing and mitigating risks before they become incidents or cause significant impact to the organization. Proactive risk management enables the organization to align its security strategy with its business objectives, optimize its security resources and investments, and enhance its resilience and compliance.

* A. Threat management is enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Threat management is the process of identifying, analyzing and responding to the threats that may exploit the vulnerabilities in an information system. Threat management is enhanced by implementing a vulnerability assessment process, as it helps to reduce the attack surface and prioritize the most critical threats. However, threat management is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a reactive rather than proactive approach to risk management.

* B. Compliance status is improved. This is a secondary benefit of implementing a vulnerability assessment process. Compliance status is the degree to which an organization adheres to the applicable laws, regulations, standards and policies that govern its information security. Compliance status is improved by implementing a vulnerability assessment process, as it helps to demonstrate the organization's commitment to security best practices and meet the expectations of the stakeholders and regulators. However, compliance status is not the PRIMARY benefit of implementing a vulnerability assessment process, as it is a result rather than a driver of risk management.

* C. Security metrics are enhanced. This is a secondary benefit of implementing a vulnerability assessment process. Security metrics are the quantitative and qualitative measures that indicate the effectiveness and efficiency of the information security processes and controls. Security metrics are enhanced by implementing a vulnerability assessment process, as it helps to provide objective and reliable data for security monitoring and reporting. However, security metrics are not the PRIMARY benefit of implementing a vulnerability assessment process, as they are a means rather than an end of risk management.

References =

- ? CISM Review Manual 15th Edition, pages 1-301
- ? CISM Exam Content Outline2
- ? Risk Assessment for Technical Vulnerabilities3
- ? A Step-By-Step Guide to Vulnerability Assessment4

NEW QUESTION 41

- (Topic 1)

In violation of a policy prohibiting the use of cameras at the office, employees have been issued smartphones and tablet computers with enabled web cameras. Which of the following should be the information security manager's FIRST course of action?

- A. Revise the policy.

- B. Perform a root cause analysis.
- C. Conduct a risk assessment,
- D. Communicate the acceptable use policy.

Answer: C

Explanation:

= The information security manager's first course of action in this situation should be to conduct a risk assessment, which is a process of identifying, analyzing, and evaluating the information security risks that arise from the violation of the policy prohibiting the use of cameras at the office. The risk assessment can help to determine the likelihood and impact of the unauthorized or inappropriate use of the cameras on the smartphones and tablet computers, such as capturing, transmitting, or disclosing sensitive or confidential information, compromising the privacy or security of the employees, customers, or partners, or violating the legal or regulatory requirements. The risk assessment can also help to identify and prioritize the appropriate risk treatment options, such as implementing technical, administrative, or physical controls to disable, restrict, or monitor the camera usage, enforcing the policy compliance and awareness, or revising the policy to reflect the current business needs and environment. The risk assessment can also help to communicate and report the risk level and status to the senior management and the relevant stakeholders, and to provide feedback and recommendations for improvement and optimization of the policy and the risk management process.

Revising the policy, performing a root cause analysis, and communicating the acceptable use policy are all possible courses of action that the information security manager can take after conducting the risk assessment, but they are not the first ones. Revising the policy is a process of updating and modifying the policy to align with the business objectives and strategy, to address the changes and challenges in the business and threat environment, and to incorporate the feedback and suggestions from the risk assessment and the stakeholders. Performing a root cause analysis is a process of investigating and identifying the underlying causes and factors that led to the violation of the policy, such as the lack of awareness, training, or enforcement, the inconsistency or ambiguity of the policy, or the conflict or gap between the policy and the business requirements or expectations. Communicating the acceptable use policy is a process of informing and educating the employees and the other users of the smartphones and tablet computers about the purpose, scope, and content of the policy, the roles and responsibilities of the users, the benefits and consequences of complying or violating the policy, and the methods and channels of reporting or resolving any policy issues or incidents. References = CISM Review Manual 15th Edition, pages 51-531; CISM Practice Quiz, question 1482

NEW QUESTION 45

- (Topic 1)

The MOST important reason for having an information security manager serve on the change management committee is to:

- A. identify changes to the information security policy.
- B. ensure that changes are tested.
- C. ensure changes are properly documented.
- D. advise on change-related risk.

Answer: D

Explanation:

The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts¹. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction².

The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies³. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes⁴.

The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks⁵. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes. Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk.

References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION 50

- (Topic 1)

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: D

Explanation:

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 54

- (Topic 1)

Which of the following would BEST ensure that security is integrated during application development?

- A. Employing global security standards during development processes
- B. Providing training on secure development practices to programmers
- C. Performing application security testing during acceptance testing
- D. Introducing security requirements during the initiation phase

Answer: D

Explanation:

Introducing security requirements during the initiation phase would BEST ensure that security is integrated during application development because it would allow the security objectives and controls to be defined and aligned with the business needs and risk appetite before any design or coding is done. This would also facilitate the security by design approach, which is the most effective method to enhance the security of applications and application development activities¹. Introducing security requirements early would also enable the collaboration between security professionals and developers, the identification and specification of security architectures, and the integration and testing of security controls throughout the development life cycle². Employing global security standards during development processes (A) would help to ensure the consistency and quality of security practices, but it would not necessarily ensure that security is integrated during application development. Providing training on secure development practices to programmers (B) would help to raise the awareness and skills of developers, but it would not ensure that security is integrated during application development. Performing application security testing during acceptance testing © would help to verify the security of the application before deployment, but it would not ensure that security is integrated during application development. It would also be too late to identify and remediate any security issues that could have been prevented or mitigated earlier in the development process. References = 1: Five Key Components of an Application Security Program - ISACA¹; 2: CISM Domain – Information Security Program Development | Infosec²

NEW QUESTION 59

- (Topic 1)

Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?

- A. Review the previous risk assessment and countermeasures.
- B. Perform a new risk assessment,
- C. Evaluate countermeasures to mitigate new risks.
- D. Transfer the new risk to a third party.

Answer: B

Explanation:

According to the CISM Review Manual, the information security manager's best course of action when security controls may no longer be adequate due to changes in the organization's environment is to perform a new risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the risks that affect the organization's information assets and business processes. A risk assessment should be performed periodically or whenever there are significant changes in the organization's environment, such as new threats, vulnerabilities, technologies, regulations, or business objectives. A risk assessment helps to determine the current level of risk exposure and the adequacy of existing security controls. A risk assessment also provides the basis for developing or updating the risk treatment plan, which defines the appropriate risk responses, such as implementing new or enhanced security controls, transferring the risk to a third party, accepting the risk, or avoiding the risk.

The other options are not the best course of action in this scenario. Reviewing the previous risk assessment and countermeasures may not reflect the current state of the organization's environment and may not identify new or emerging risks. Evaluating countermeasures to mitigate new risks may be premature without performing a new risk assessment to identify and prioritize the risks. Transferring the new risk to a third party may not be feasible or cost-effective without performing a new risk assessment to evaluate the risk level and the available risk transfer options.

References = CISM Review Manual, 16th Edition, Chapter 2, Section 1, pages 43-45.

NEW QUESTION 61

- (Topic 1)

The MOST appropriate time to conduct a disaster recovery test would be after:

- A. major business processes have been redesigned.
- B. the business continuity plan (BCP) has been updated.
- C. the security risk profile has been reviewed
- D. noncompliance incidents have been filed.

Answer: B

Explanation:

The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well

as identify any gaps, issues, or improvement opportunities¹²³. References =

? 1: CISM Review Manual 15th Edition, page 2114

? 2: CISM Practice Quiz, question 1042

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

NEW QUESTION 62

- (Topic 1)

Which of the following BEST ensures timely and reliable access to services?

- A. Nonrepudiation
- B. Authenticity
- C. Availability
- D. Recovery time objective (RTO)

Answer: C

Explanation:

= According to the CISM Review Manual, availability is the degree to which information and systems are accessible to authorized users in a timely and reliable manner¹. Availability ensures that services are delivered to the users as expected and agreed upon. Nonrepudiation is the ability to prove the occurrence of a claimed event or action and its originating entities¹. It ensures that the parties involved in a transaction cannot deny their involvement. Authenticity is the quality or state of being genuine or original, rather than a reproduction or fabrication¹. It ensures that the identity of a subject or resource is valid. Recovery time objective (RTO) is the maximum acceptable period of time that can elapse before the unavailability of a business function severely impacts the organization¹. It is a metric used to measure the recovery capability of a system or service, not a factor that ensures timely and reliable access to services. References = CISM Review Manual, 16th Edition, Chapter 2, Information Risk Management, pages 66-67.

NEW QUESTION 65

- (Topic 1)

Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?

- A. Compromise of critical assets via third-party resources
- B. Unavailability of services provided by a supplier
- C. Loss of customers due to unavailability of products
- D. Unreliable delivery of hardware and software resources by a supplier

Answer: A

Explanation:

= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios.

These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page 189 1; CISM Practice Quiz 2

NEW QUESTION 66

- (Topic 1)

During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

- A. Post-incident review
- B. Eradication
- C. Containment
- D. Identification

Answer: B

Explanation:

The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident¹. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems². The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed². The eradication phase is the first step in returning a compromised environment to its proper state².

The other phases of incident response are:

? Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources¹.

? Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency¹.

? Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage¹.

? Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence¹.

? Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement¹. References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2: What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

NEW QUESTION 68

- (Topic 1)

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: A

Explanation:

= 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 71

- (Topic 1)

An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

- A. Integrate information security risk assessments into the procurement process.
- B. Provide regular information security training to the procurement team.
- C. Invite IT members into regular procurement team meetings to influence best practice.
- D. Enforce the right to audit in procurement contracts with SaaS vendors.

Answer: A

Explanation:

The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization. Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.

Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.

Inviting IT members into regular procurement team meetings to influence best practice © is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.

Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, Page 141-1421

NEW QUESTION 74

- (Topic 1)

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: B

Explanation:

= 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 79

- (Topic 1)

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

Explanation:

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 82

- (Topic 1)

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: B

Explanation:

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 83

- (Topic 1)

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: B

Explanation:

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 86

- (Topic 1)

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: C

Explanation:

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 87

- (Topic 1)

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: A

Explanation:

= 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 90

- (Topic 1)

A security incident has been reported within an organization. When should an information security manager contact the information owner? After the:

- A. incident has been confirmed.
- B. incident has been contained.
- C. potential incident has been logged.
- D. incident has been mitigated.

Answer: A

Explanation:

= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.

The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. References =

? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.

? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

NEW QUESTION 95

- (Topic 1)

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: B

Explanation:

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 99

- (Topic 1)

An information security manager developing an incident response plan MUST ensure it includes:

- A. an inventory of critical data.
- B. criteria for escalation.

- C. a business impact analysis (BIA).
- D. critical infrastructure diagrams.

Answer: B

Explanation:

An incident response plan is a set of procedures and guidelines that define the roles and responsibilities of the incident response team, the steps to follow in the event of an incident, and the communication and escalation protocols to ensure timely and effective resolution of incidents. One of the essential components of an incident response plan is the criteria for escalation, which specify the conditions and thresholds that trigger the escalation of an incident to a higher level of authority or a different function within the organization. The criteria for escalation may depend on factors such as the severity, impact, duration, scope, and complexity of the incident, as well as the availability and capability of the incident response team. The criteria for escalation help to ensure that incidents are handled by the appropriate personnel, that management is kept informed and involved, and that the necessary resources and support are provided to resolve the incident. References = <https://blog.exigence.io/a-practical-approach-to-incident-management-escalation>
https://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Information_Security_Incident_Response_Escalation_Guideline.pdf

NEW QUESTION 100

- (Topic 1)

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: A

Explanation:

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 105

- (Topic 1)

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?

- A. Enforce the policy.
- B. Modify the policy.
- C. Present the risk to senior management.
- D. Create an exception for the deviation.

Answer: C

Explanation:

The information security manager's best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role-based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management's approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127- 128, 138-139, 143-144.

NEW QUESTION 108

- (Topic 1)

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: C

Explanation:

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 111

- (Topic 1)

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

Explanation:

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 115

- (Topic 1)

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: C

Explanation:

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 120

- (Topic 1)

Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?

- A. Number of blocked intrusion attempts
- B. Number of business cases reviewed by senior management
- C. Trends in the number of identified threats to the business
- D. Percentage of controls integrated into business processes

Answer: D

Explanation:

Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and

reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations. References = CISM Review Manual 2023, page 291; CISM Review Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

NEW QUESTION 123

- (Topic 1)

Which of the following **MUST** be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

- A. Security policy
- B. Risk management framework
- C. Risk appetite
- D. Security standards

Answer: C

Explanation:

= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION 124

- (Topic 1)

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: B

Explanation:

= 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 125

- (Topic 1)

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: C

Explanation:

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 126

- (Topic 1)

Which of the following activities **MUST** be performed by an information security manager for change requests?

- A. Perform penetration testing on affected systems.
- B. Scan IT systems for operating system vulnerabilities.
- C. Review change in business requirements for information security.
- D. Assess impact on information security risk.

Answer: D

NEW QUESTION 131

- (Topic 1)

Management decisions concerning information security investments will be **MOST** effective when they are based on:

- A. a process for identifying and analyzing threats and vulnerabilities.
- B. an annual loss expectancy (ALE) determined from the history of security events,
- C. the reporting of consistent and periodic assessments of risks.
- D. the formalized acceptance of risk analysis by management,

Answer: C

Explanation:

Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION 136

- (Topic 1)

Which of the following is **MOST** helpful for protecting an enterprise from advanced persistent threats (APTs)?

- A. Updated security policies
- B. Defined security standards
- C. Threat intelligence
- D. Regular antivirus updates

Answer: C

Explanation:

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

The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. References =

? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.

? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.

? Advanced Persistent Threats and Nation-State Actors 1

? Book Review: Advanced Persistent Threats 2

? Advanced Persistent Threat (APT) Protection 3

? Establishing Advanced Persistent Security to Combat Long-Term Threats 4

? What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION 139

- (Topic 1)

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: D

Explanation:

= 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 140

- (Topic 1)

What is the BEST way to reduce the impact of a successful ransomware attack?

- A. Perform frequent backups and store them offline.
- B. Purchase or renew cyber insurance policies.
- C. Include provisions to pay ransoms in the information security budget.
- D. Monitor the network and provide alerts on intrusions.

Answer: A

Explanation:

Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself. Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

NEW QUESTION 142

- (Topic 1)

Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?

- A. Availability of web application firewall logs.
- B. Capability of online virtual machine analysis
- C. Availability of current infrastructure documentation
- D. Capability to take a snapshot of virtual machines

Answer: D

Explanation:

A snapshot is a point-in-time copy of the state of a virtual machine (VM) that can be used to restore the VM to a previous state in case of a security incident or a disaster. A snapshot can capture the VM's disk, memory, and device configuration, allowing for a quick and easy recovery of the VM's data and functionality. Snapshots can also be used to create backups, clones, or replicas of VMs for testing, analysis, or migration purposes. Snapshots are a common service offering in Infrastructure as a Service (IaaS) models, where customers can provision and manage VMs on demand from a cloud service provider (CSP). A CSP that offers the capability to take snapshots of VMs can assist customers when recovering from a security incident by providing them with the following benefits¹²:

? Faster recovery time: Snapshots can reduce the downtime and data loss caused by a security incident by allowing customers to quickly revert their VMs to a known good state. Snapshots can also help customers avoid the need to reinstall or reconfigure their VMs after an incident, saving time and resources.

? Easier incident analysis: Snapshots can enable customers to perform online or offline analysis of their VMs after an incident, without affecting the production environment. Customers can use snapshots to examine the VM's disk, memory, and logs for evidence of compromise, root cause analysis, or forensic investigation. Customers can also use snapshots to test and validate their incident response plans or remediation actions before applying them to the production VMs.

? Enhanced security posture: Snapshots can improve the security posture of customers by enabling them to implement best practices such as backup and restore, disaster recovery, and business continuity. Snapshots can help customers protect their VMs from accidental or malicious deletion, corruption, or modification, as well as from environmental or technical disruptions. Snapshots can also help customers comply with regulatory or contractual requirements for data retention, availability, or integrity. References = What is Disaster Recovery as a Service? | CSA - Cloud Security Alliance, What Is Cloud Incident Response (IR)? CrowdStrike

NEW QUESTION 147

- (Topic 1)

Security administration efforts will be greatly reduced following the deployment of which of the following techniques?

- A. Discretionary access control
- B. Role-based access control
- C. Access control lists
- D. Distributed access control

Answer: B

Explanation:

Role-based access control (RBAC) is a policy-neutral access control mechanism that assigns access privileges to defined roles in the organization and then makes each user a member of the appropriate roles. RBAC reduces security administration efforts by simplifying the management of access rights across different users and resources. RBAC also enables consistent and efficient enforcement of the principle of least privilege, which grants users only the minimum rights required to perform their assigned tasks. RBAC can also facilitate the implementation of separation of duties, which prevents users from having conflicting or incompatible responsibilities. RBAC is among the most widely used methods in the information security tool kit¹. References = CIS Control 6: Access Control Management - Netwrix, CISSP certification: RBAC (Role based access control), What is RBAC? (Role Based Access Control) - IONOS

NEW QUESTION 149

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CISM Practice Exam Features:

- * CISM Questions and Answers Updated Frequently
- * CISM Practice Questions Verified by Expert Senior Certified Staff
- * CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISM Practice Test Here](#)