

Isaca

Exam Questions CISM

Certified Information Security Manager



NEW QUESTION 1

- (Topic 2)

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

- A. Inform senior management
- B. Re-evaluate the risk
- C. Implement compensating controls
- D. Ask the business owner for the new remediation plan

Answer: B

Explanation:

The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability. This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.

The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner. The other choices are possible actions but not necessarily the first one.

A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network². A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets². A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences².

NEW QUESTION 2

- (Topic 2)

Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site. Which of the following issues would be of GREATEST concern to an information security manager?

- A. The application does not use a secure communications protocol
- B. The application is configured with restrictive access controls
- C. The business process has only one level of error checking
- D. Server-based malware protection is not enforced

Answer: D

Explanation:

Server-based malware protection is not enforced is the issue that would be of GREATEST concern to an information security manager, as it exposes the web-based application and its data to potential threats from malicious software that can compromise the confidentiality, integrity, and availability of the information. Server-based malware protection is a security control that monitors and blocks malicious activities on the server where the application runs, such as viruses, worms, trojans, ransomware, etc. Without server-based malware protection, the web-based application may be vulnerable to attacks that can damage or destroy the data stored on the server, or disrupt the normal functioning of the application. The other issues are also important, but not as critical as server-based malware protection. The application does not use a secure communications protocol may expose sensitive data in transit to eavesdropping or interception by unauthorized parties. The application is configured with restrictive access controls may limit the access rights of legitimate users to authorized resources, but it does not prevent unauthorized users from accessing them through other means. The business process has only one level of error checking may result in incorrect or inconsistent data entry or processing, but it does not guarantee data quality or accuracy. References = CISM Review Manual, 16th Edition, page 1751; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 812

NEW QUESTION 3

- (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 4

- (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 5

- (Topic 1)

Which of the following is MOST helpful for determining which information security policies should be implemented by an organization?

- A. Risk assessment
- B. Business impact analysis (BIA)
- C. Vulnerability assessment
- D. Industry best practices

Answer: A

Explanation:

Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes¹. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance². Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.

A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses³. A risk assessment helps to determine the following aspects of information security policies:

? The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.

? The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses.

? The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.

? The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.

The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations:

? A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.

? A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls.

? Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.

References = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page 30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

NEW QUESTION 6

- (Topic 1)

ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?

- A. Recommend canceling the outsourcing contract.
- B. Request an independent review of the provider's data center.
- C. Notify affected customers of the data breach.
- D. Determine the extent of the impact to the organization.

Answer: D

Explanation:

The CISO should first determine the extent of the impact to the organization by assessing the nature and scope of the data breach, the type and sensitivity of the data involved, the potential harm to the organization and its customers, and the legal and contractual obligations of the organization and the service provider. This will help the CISO to prioritize the appropriate actions and resources to respond to the incident and mitigate the risks. The other options are possible actions that the CISO may take after determining the impact, depending on the circumstances and the outcomes of the investigation. References = CISM Review Manual 15th Edition, page 2231; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1030

NEW QUESTION 7

- (Topic 1)

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

- A. Appropriate prioritization of information risk treatment
- B. Increased compliance with information security policy
- C. Appropriate assignment of information asset owners
- D. An accurate and complete information asset catalog

Answer: A

Explanation:

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

NEW QUESTION 8

- (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 9

- (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 10

- (Topic 1)

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

- A. Mature change management processes
- B. Senior management support
- C. Well-defined security policies

D. Unannounced testing

Answer: D

Explanation:

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

NEW QUESTION 10

- (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 14

- (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 19

- (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 23

- (Topic 1)

An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

- A. Determine security controls for the new service.
- B. Establish a compliance program,
- C. Perform a gap analysis against the current state
- D. Hire new resources to support the service.

Answer: C

Explanation:

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

? It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.

? It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.

? It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.

? It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.

? It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.

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

Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:

* 1. infosecrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

NEW QUESTION 24

- (Topic 1)

An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?

- A. Create a business case for a new incident response plan.
- B. Revise the existing incident response plan.
- C. Conduct a gap analysis.
- D. Assess the impact to the budget,

Answer: C

Explanation:

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

References =

? CISM Review Manual 15th Edition, page 1631

? CISM certified information security manager study guide, page 452

? How To Conduct An Information Security Gap Analysis³

? PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS⁴

NEW QUESTION 26

- (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 28

- (Topic 1)

An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

- A. Red team exercise
- B. Black box penetration test
- C. Disaster recovery exercise
- D. Tabletop exercise

Answer: D

Explanation:

= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low-cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.

A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

A disaster recovery exercise (C) is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high-risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

NEW QUESTION 31

- (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 34

- (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 35

- (Topic 1)

Network isolation techniques are immediately implemented after a security breach to:

- A. preserve evidence as required for forensics
- B. reduce the extent of further damage.
- C. allow time for key stakeholder decision making.
- D. enforce zero trust architecture principles.

Answer: B

Explanation:

Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. References = CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1162

NEW QUESTION 37

- (Topic 1)

In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:

- A. evaluate results of the most recent incident response test.
- B. review the number of reported security incidents.
- C. ensure established security metrics are reported.
- D. assess progress of risk mitigation efforts.

Answer: D

Explanation:

According to the CISM Review Manual, an organization's security posture is the overall condition of its information security, which is determined by the effectiveness of its security program and the alignment of its security objectives with its business goals. To understand the security posture, the senior leadership needs to have a holistic view of the security risks and the actions taken to address them. Therefore, assessing the progress of risk mitigation efforts is the most important activity for the senior leadership, as it provides them with the information on how well the security program is performing and whether it is meeting the expected outcomes. Evaluating the results of the most recent incident response test, reviewing the number of reported security incidents, and ensuring established security metrics are reported are all useful activities for the senior leadership, but they are not sufficient to understand the security posture. They only provide partial or isolated information on the security performance, which may not reflect the overall security condition or the alignment with the business objectives. References = CISM Review Manual, 16th Edition, Chapter 1, Information Security Governance, pages 28-29.

NEW QUESTION 38

- (Topic 1)

Which of the following activities is designed to handle a control failure that leads to a breach?

- A. Risk assessment
- B. Incident management
- C. Root cause analysis
- D. Vulnerability management

Answer: B

Explanation:

Incident management is the activity designed to handle a control failure that leads to a breach. Incident management is the process of identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. Incident management aims to minimize the impact of a breach, restore normal operations as quickly as possible, and prevent or reduce the likelihood of recurrence. Incident management involves several steps, such as:

- ? Establishing an incident response team with clear roles and responsibilities
 - ? Developing and maintaining an incident response plan that defines the procedures, tools, and resources for handling incidents
 - ? Implementing detection and reporting mechanisms to identify and communicate incidents
 - ? Performing triage and analysis to assess the scope, severity, and root cause of incidents
 - ? Containing and eradicating the threat and preserving evidence for investigation and legal purposes
 - ? Recovering and restoring the affected systems and data to a secure state
 - ? Evaluating and improving the incident response process and controls based on lessons learned and best practices
- References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 223-232.

NEW QUESTION 40

- (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 45

- (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 46

- (Topic 1)

Which of the following provides the BEST assurance that security policies are applied across business operations?

- A. Organizational standards are included in awareness training.
- B. Organizational standards are enforced by technical controls.
- C. Organizational standards are required to be formally accepted.
- D. Organizational standards are documented in operational procedures.

Answer: D

Explanation:

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

NEW QUESTION 51

- (Topic 1)

Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

- A. Providing ongoing training to the incident response team
- B. Implementing proactive systems monitoring
- C. Implementing a honeypot environment
- D. Updating information security awareness materials

Answer: B

Explanation:

= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.

References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

NEW QUESTION 56

- (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 61

- (Topic 1)

Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?

- A. Establish key risk indicators (KRIs).
- B. Use quantitative risk assessment methods.
- C. Provide regular reporting on risk treatment to senior management
- D. Require steering committee approval of risk treatment plans.

Answer: D

Explanation:

= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management. However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter 2, Section 2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION 66

- (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 close to going live with the implementation of a cloud-based application. Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?

- A. Implement the application and request the cloud service provider to fix the vulnerability.
- B. Assess whether the vulnerability is within the organization's risk tolerance levels.
- C. Commission further penetration tests to validate initial test results,
- D. Postpone the implementation until the vulnerability has been fixed.

Answer: B

Explanation:

The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.

Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.

Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information. The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project. Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk-averse approach, as it may hinder the organization's innovation and competitiveness. References =

? ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.

? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

NEW QUESTION 76

- (Topic 1)

Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

- A. Effective security eliminates risk to the business.
- B. Adopt a recognized framework with metrics.
- C. Security is a business product and not a process.
- D. Security supports and protects the business.

Answer: D

Explanation:

The message that security supports and protects the business is the most effective in obtaining senior management's commitment to information security management. This message emphasizes the value and benefits of security for the organization's strategic goals, mission, and vision. It also aligns security with the business needs and expectations, and demonstrates how security can enable and facilitate the business processes and functions. The other messages are not as effective because they either overstate the role of security (A), focus on technical aspects rather than business outcomes (B), or confuse the nature and purpose of security ©. References = CISM Review Manual 2022, page 23; CISM Item Development Guide 2022, page 9; CISM Information Security Governance Certified Practice Exam - CherCherTech

NEW QUESTION 81

- (Topic 1)

An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

- A. conduct an incident forensic analysis.
- B. follow the incident response plan
- C. notify the business process owner.
- D. follow the business continuity plan (BCP).

Answer: B

Explanation:

Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.

Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually

performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented. References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

NEW QUESTION 84

- (Topic 1)

What should be the FIRST step when an Internet of Things (IoT) device in an organization's network is confirmed to have been hacked?

- A. Monitor the network.
- B. Perform forensic analysis.
- C. Disconnect the device from the network,
- D. Escalate to the incident response team

Answer: C

Explanation:

= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures¹²³. References =

? 1: CISM Review Manual 15th Edition, page 2004

? 2: CISM Practice Quiz, question 1072

? 3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

NEW QUESTION 88

- (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 90

- (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 91

- (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 94

- (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 98

- (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 100

- (Topic 1)

A PRIMARY purpose of creating security policies is to:

- A. define allowable security boundaries.

- B. communicate management's security expectations.
- C. establish the way security tasks should be executed.
- D. implement management's security governance strategy.

Answer: D

Explanation:

A security policy is a formal statement of the rules and principles that govern the protection of information assets in an organization. A security policy defines the scope, objectives, roles and responsibilities, and standards of the information security program. A primary purpose of creating security policies is to implement management's security governance strategy, which is the framework that guides the direction and alignment of information security with the business goals and objectives. A security policy translates the management's vision and expectations into specific and measurable requirements and controls that can be implemented and enforced by the information security staff and other stakeholders. A security policy also helps to establish the accountability and authority of the information security function and to demonstrate the commitment and support of the senior management for the information security program.

References =

- ? CISM Review Manual 15th Edition, page 1631
- ? CISM 2020: IT Security Policies2
- ? CISM domain 1: Information security governance [Updated 2022]3
- ? What is CISM? - Digital Guardian4

NEW QUESTION 104

- (Topic 1)

An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy. A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

- A. the chief risk officer (CRO).
- B. business senior management.
- C. the information security manager.
- D. the compliance officer.

Answer: B

Explanation:

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

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

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

The compliance officer (D) is the officer who oversees the organization's compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

NEW QUESTION 108

- (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 111

- (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 112

- (Topic 1)

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

- A. Communicate disciplinary processes for policy violations.
- B. Require staff to participate in information security awareness training.
- C. Require staff to sign confidentiality agreements.
- D. Include information security responsibilities in job descriptions.

Answer: B

Explanation:

The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION 116

- (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 119

- (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 120

- (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 121

- (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 123

- (Topic 1)

Which of the following would be **MOST** helpful to identify worst-case disruption scenarios?

- A. Business impact analysis (BIA)
- B. Business process analysis
- C. SWOT analysis
- D. Cost-benefit analysis

Answer: A

Explanation:

A business impact analysis (BIA) is the process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization in the event of a disaster or crisis. A BIA also helps to identify the worst-case disruption scenarios, which are the scenarios that would cause the most severe impact to the organization in terms of financial, operational, reputational, or legal consequences. By conducting a BIA, the organization can assess the likelihood and impact of various disruption scenarios, and plan accordingly to mitigate

the risks and ensure business continuity and resilience. References = CISM Review Manual 15th Edition, page 181, page 183.

NEW QUESTION 126

- (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 127

- (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 131

- (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 136

- (Topic 1)

An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a

major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

- A. The information security manager
- B. The data owner
- C. The application owner
- D. The security engineer

Answer: C

Explanation:

= The application owner is primarily accountable for the associated task because they are responsible for ensuring that the application meets the business requirements and objectives, as well as the security and compliance standards. The application owner is also the one who defines the roles and responsibilities of the application team, including the security engineer, and oversees the development, testing, deployment, and maintenance of the application. The application owner should work with the cloud provider to address the security vulnerability and mitigate the risk. The information security manager, the data owner, and the security engineer are not primarily accountable for the associated task, although they may have some roles and responsibilities in supporting the application owner. The information security manager is responsible for establishing and maintaining the information security program and aligning it with the business objectives and strategy. The data owner is responsible for defining the classification, usage, and protection requirements of the data. The security engineer is responsible for implementing and testing the security controls and features of the application. References = CISM Review Manual 2023, Chapter 1, Section 1.2.2, page 18; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 115.

NEW QUESTION 137

- (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:

The primary benefit of implementing a vulnerability assessment process is to facilitate proactive risk management. A vulnerability assessment process is a systematic and periodic evaluation of the security posture of an information system or network, which identifies and measures the weaknesses and exposures that may be exploited by threats. By implementing a vulnerability assessment process, the organization can proactively identify and prioritize the risks, and implement appropriate controls and mitigation strategies to reduce the likelihood and impact of potential incidents. The other options are possible benefits of implementing a vulnerability assessment process, but they are not the primary one. References = CISM Review Manual 15th Edition, page 1731; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1029

NEW QUESTION 139

- (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 141

- (Topic 1)

Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?

- A. A capability and maturity assessment
- B. Detailed analysis of security program KPIs
- C. An information security dashboard
- D. An information security risk register

Answer: C

Explanation:

An information security dashboard is the most effective way to present quarterly reports to the board on the status of the information security program, because it provides a concise, visual, and high-level overview of the key performance indicators (KPIs), metrics, and trends of the information security program. An information security dashboard can help the board to quickly and easily understand the current state, progress, and performance of the information security program, and to identify any gaps, issues, or areas of improvement. An information security dashboard can also help the board to align the information security program with the organization's business goals and strategies, and to support the decision-making and oversight functions of the board.

A capability and maturity assessment is a way of measuring the effectiveness and efficiency of the information security program, and of identifying the strengths and weaknesses of the program. However, a capability and maturity assessment is not the most effective way to present quarterly reports to the board, because it may not provide a clear and timely picture of the status of the information security program, and it may not reflect the changes and dynamics of the information security environment. A capability and maturity assessment is more suitable for periodic or annual reviews, rather than quarterly reports.

A detailed analysis of security program KPIs is a way of evaluating the performance and progress of the information security program, and of determining the extent to which the program meets the predefined objectives and targets. However, a detailed analysis of security program KPIs is not the most effective way to present quarterly reports to the board, because it may be too technical, complex, or lengthy for the board to comprehend and appreciate. A detailed analysis of security program KPIs is more suitable for operational or tactical level reporting, rather than strategic level reporting.

An information security risk register is a tool for recording and tracking the information security risks that affect the organization, and for documenting the risk assessment, treatment, and monitoring activities. However, an information security risk register is not the most effective way to present quarterly reports to the board, because it may not provide a comprehensive and balanced view of the information security program, and it may not highlight the achievements and benefits of the program. An information security risk register is more suitable for risk management or audit purposes, rather than performance reporting. References = ? ISACA, CISM Review Manual, 16th Edition, 2020, pages 47-48, 59-60, 63-64, 67-68. ? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1019.

An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

NEW QUESTION 144

- (Topic 1)

Which of the following BEST indicates that information security governance and corporate governance are integrated?

- A. The information security team is aware of business goals.
- B. The board is regularly informed of information security key performance indicators (KPIs),
- C. The information security steering committee is composed of business leaders.
- D. A cost-benefit analysis is conducted on all information security initiatives.

Answer: C

Explanation:

The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

NEW QUESTION 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 151

- (Topic 1)

Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

- A. Management's business goals and objectives
- B. Strategies of other non-regulated companies
- C. Risk assessment results
- D. Industry best practices and control recommendations

Answer: A

Explanation:

When a new information security manager is developing an information security strategy for a non-regulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

NEW QUESTION 152

- (Topic 1)

Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

- A. Enable multi-factor authentication on user and admin accounts.
- B. Review access permissions annually or whenever job responsibilities change
- C. Lock out accounts after a set number of unsuccessful login attempts.
- D. Delegate the management of access permissions to an independent third party.

Answer: B

NEW QUESTION 155

- (Topic 1)

When deciding to move to a cloud-based model, the FIRST consideration should be:

- A. storage in a shared environment.
- B. availability of the data.
- C. data classification.
- D. physical location of the data.

Answer: C

Explanation:

The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.

Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co-located with other customers' data, and may be subject to unauthorized access, modification, or deletion. Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies. However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment. References =

? ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108.

? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

NEW QUESTION 157

- (Topic 1)

Which of the following is the MOST important factor of a successful information security program?

- A. The program follows industry best practices.
- B. The program is based on a well-developed strategy.
- C. The program is cost-efficient and within budget,
- D. The program is focused on risk management.

Answer: D

Explanation:

A successful information security program is one that aligns with the business objectives and strategy, supports the business processes and functions, and protects the information assets from threats and vulnerabilities. The most important factor of such a program is that it is focused on risk management, which means that it identifies, assesses, treats, and monitors the information security risks that could affect the business continuity, reputation, and value. Risk management helps to prioritize the security activities and resources, allocate the appropriate budget and resources, implement the necessary controls and measures, and evaluate the effectiveness and efficiency of the program. Risk management also enables the program to adapt to the changing business and threat environment, and to continuously improve the security posture and performance. A program that follows industry best practices, is based on a well-developed strategy, and is cost-efficient and within budget are all desirable attributes, but they are not sufficient to ensure the success of the program without a risk management focus.

References = CISM Review Manual 15th Edition, page 411; CISM Practice Quiz, question 1242

NEW QUESTION 159

- (Topic 1)

An information security manager learns that a risk owner has approved exceptions to replace key controls with weaker compensating controls to improve process efficiency. Which of the following should be the GREATEST concern?

- A. Risk levels may be elevated beyond acceptable limits.
- B. Security audits may report more high-risk findings.

- C. The compensating controls may not be cost efficient.
- D. Noncompliance with industry best practices may result.

Answer: A

Explanation:

Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.

References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

NEW QUESTION 162

- (Topic 1)

Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

- A. To compare emerging trends with the existing organizational security posture
- B. To communicate worst-case scenarios to senior management
- C. To train information security professionals to mitigate new threats
- D. To determine opportunities for expanding organizational information security

Answer: A

Explanation:

The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks. References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

NEW QUESTION 163

- (Topic 1)

Which of the following is a desired outcome of information security governance?

- A. Penetration test
- B. Improved risk management
- C. Business agility
- D. A maturity model

Answer: C

Explanation:

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

NEW QUESTION 165

- (Topic 3)

Which of the following BEST demonstrates that an anti-phishing campaign is effective?

- A. Improved staff attendance in awareness sessions
- B. Decreased number of phishing emails received
- C. Improved feedback on the anti-phishing campaign
- D. Decreased number of incidents that have occurred

Answer: D

Explanation:

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

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

NEW QUESTION 170

.....

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](#)