

Isaca

Exam Questions CISM

Certified Information Security Manager



NEW QUESTION 1

- (Topic 1)

Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?

- A. Capability maturity model
- B. Vulnerability assessment
- C. IT security risk and exposure
- D. Business impact analysis (BIA)

Answer: A

Explanation:

A capability maturity model (CMM) is a framework that helps organizations assess and improve their processes and capabilities in various domains, such as software development, project management, information security, and others¹. A CMM defines a set of levels or stages that represent the degree of maturity or effectiveness of an organization's processes and capabilities in a specific domain. Each level has a set of criteria or characteristics that an organization must meet to achieve that level of maturity. A CMM also provides guidance and best practices on how to progress from one level to another, and how to measure and monitor the performance and improvement of the processes and capabilities².

A CMM is most helpful in determining an organization's current capacity to mitigate risks, because it provides a systematic and objective way to evaluate the strengths and weaknesses of the organization's processes and capabilities related to risk management. A CMM can help an organization identify the gaps and opportunities for improvement in its risk management practices, and prioritize the actions and resources needed to address them. A CMM can also help an organization benchmark its risk management maturity against industry standards or best practices, and demonstrate its compliance with regulatory or contractual requirements³.

The other options are not as helpful as a CMM in determining an organization's current capacity to mitigate risks, because they are either more specific, limited, or dependent on a CMM. A vulnerability assessment is a process of identifying and analyzing the vulnerabilities in an organization's systems, networks, or applications, and their potential impact on the organization's assets, operations, or reputation. A vulnerability assessment can help an organization identify the sources and levels of risk, but it does not provide a comprehensive or holistic view of the organization's risk management maturity or effectiveness⁴. IT security risk and exposure is a measure of the likelihood and impact of a security breach or incident on an organization's IT assets, operations, or reputation. IT security risk and exposure can help an organization quantify and communicate the level of risk, but it does not provide a framework or guidance on how to improve the organization's risk management processes or capabilities⁵. A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of a disruption or disaster on an organization's critical business functions, processes, or resources. A BIA can help an organization determine the priorities and requirements for business continuity and disaster recovery, but it does not provide a method or standard for assessing or enhancing the organization's risk management maturity or effectiveness. References = 1: CMMI Institute - What is CMMI? - Capability Maturity Model Integration 2: Capability Maturity Model and Risk Register Integration: The Right ... 3: Performing Risk Assessments of Emerging Technologies - ISACA 4: CISM Review Manual 15th Edition, Chapter 4, Section 4.2 5: CISM Review Manual 15th Edition, Chapter 4, Section 4.3 : CISM Review Manual 15th Edition, Chapter 4, Section 4.4

NEW QUESTION 2

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 3

- (Topic 1)

Which of the following BEST facilitates effective incident response testing?

- A. Including all business units in testing
- B. Simulating realistic test scenarios
- C. Reviewing test results quarterly
- D. Testing after major business changes

Answer: B

Explanation:

Effective incident response testing is a process of verifying and validating the incident response plan, procedures, roles, and resources that are designed to respond to and recover from information security incidents. The purpose of testing is to ensure that the incident response team and the organization are prepared, capable, and confident to handle any potential or actual incidents that could affect the business continuity, reputation, and value. The best way to facilitate effective

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

NEW QUESTION 4

- (Topic 1)

Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?

- A. To identify the organization's risk tolerance
- B. To improve security processes
- C. To align security roles and responsibilities
- D. To optimize security risk management

Answer: D

Explanation:

= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By aligning information security with the organization's strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner¹. Alignment also enables the information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives². Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability³. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information assets with the business objectives and risk appetite of the organization⁴. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

NEW QUESTION 5

- (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 6

- (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 7

- (Topic 1)

An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?

- A. Determine whether the organization can benefit from adopting the new standard.
- B. Obtain legal counsel's opinion on the standard's applicability to regulations,
- C. Perform a risk assessment on the new technology.
- D. Review industry specialists' analyses of the new standard.

Answer: A

Explanation:

= The first step that the information security manager should recommend when learning of a new standard related to an emerging technology is to determine whether the organization can benefit from adopting the new standard. This involves evaluating the business objectives, needs, and requirements of the organization, as well as the potential advantages, disadvantages, and challenges of implementing the new technology and the new standard. The information security manager should also consider the alignment of the new standard with the organization's existing policies, procedures, and standards, as well as the impact of the new standard on the organization's information security governance, risk management, program, and incident management. By conducting a preliminary analysis of the feasibility, suitability, and desirability of the new standard, the information security manager can provide a sound basis for further decision making and planning.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Standards, page 391; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 43, page 412.

NEW QUESTION 8

- (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 9

- (Topic 1)

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

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

Answer: D

Explanation:

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

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

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

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

References =

? CISM Review Manual 15th Edition, pages 1-301

? CISM Exam Content Outline2

? Risk Assessment for Technical Vulnerabilities³
? A Step-By-Step Guide to Vulnerability Assessment⁴

NEW QUESTION 10

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 10

- (Topic 1)

Which of the following should be the PRIMARY area of focus when mitigating security risks associated with emerging technologies?

- A. Compatibility with legacy systems
- B. Application of corporate hardening standards
- C. Integration with existing access controls
- D. Unknown vulnerabilities

Answer: D

Explanation:

= The primary area of focus when mitigating security risks associated with emerging technologies is unknown vulnerabilities. Emerging technologies are new and complex, and often involve multiple parties, interdependencies, and uncertainties. Therefore, they may have unknown vulnerabilities that could expose the organization to threats that are difficult to predict, detect, or prevent¹. Unknown vulnerabilities could also result from the lack of experience, knowledge, or best practices in implementing, operating, or securing emerging technologies². Unknown vulnerabilities could lead to serious consequences, such as data breaches, system failures, reputational damage, legal liabilities, or regulatory sanctions³. Therefore, it is important to focus on identifying, assessing, and addressing unknown vulnerabilities when mitigating security risks associated with emerging technologies.

The other options are not as important as unknown vulnerabilities, because they are either more predictable, manageable, or specific. Compatibility with legacy systems is a technical issue that could affect the performance, functionality, or reliability of emerging technologies, but it is not a security risk per se. It could be resolved by testing, upgrading, or replacing legacy systems⁴. Application of corporate hardening standards is a security measure that could reduce the attack surface and improve the resilience of emerging technologies, but it is not a sufficient or comprehensive solution. It could be limited by the availability, applicability, or effectiveness of the standards. Integration with existing access controls is a security requirement that could prevent unauthorized or inappropriate access to emerging technologies, but it is not a guarantee of security. It could be challenged by the complexity, diversity, or dynamism of the access scenarios. References = 1: Performing Risk Assessments of Emerging Technologies - ISACA 2: Assessing the Risk of Emerging Technology - ISACA 3: Factors Influencing Public Risk Perception of Emerging Technologies: A ... 4: CISM Review Manual 15th Edition, Chapter 3, Section 3.3 : CISM Review Manual 15th Edition, Chapter 3, Section 3.4 : CISM Review Manual 15th Edition, Chapter 3, Section 3.5

NEW QUESTION 12

- (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 14

- (Topic 1)

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

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 16

- (Topic 1)

Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?

- A. Metrics to drive the information security program
- B. Information security policies
- C. A defined security organizational structure
- D. An information security strategy

Answer: D

Explanation:

An information security strategy is the most important element to have in place as a basis for developing an effective information security program that supports the organization's business goals. An information security strategy is a high-level plan that defines the vision, mission, objectives, scope, and principles of information security for the organization¹. It also aligns the information security program with the organization's strategy, culture, risk appetite, and governance framework². An information security strategy provides the direction, guidance, and justification for the information security program, and ensures that the program is consistent, coherent, and comprehensive³. An information security strategy also helps to prioritize the information security initiatives, allocate the resources, and measure the performance and value of the information security program⁴.

The other options are not as important as an information security strategy, because they are either derived from or dependent on the strategy. Metrics are used to drive the information security program, but they need to be based on the strategy and aligned with the goals and objectives of the program. Information security policies are the rules and standards that implement the information security strategy and define the expected behavior and responsibilities of the stakeholders. A defined security organizational structure is the way the information security roles and functions are organized and coordinated within the organization, and it should reflect the strategy and the governance model. References = 1: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 2: CISM Review Manual 15th Edition, Chapter 1, Section 1.2 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 4: CISM Review Manual 15th Edition, Chapter 1, Section 1.4 : CISM Review Manual 15th Edition, Chapter 1, Section 1.5 : CISM Review Manual 15th Edition, Chapter 1, Section 1.6 : CISM Review Manual 15th Edition, Chapter 1, Section 1.7

NEW QUESTION 19

- (Topic 1)

Which of the following parties should be responsible for determining access levels to an application that processes client information?

- A. The business client
- B. The information security team
- C. The identity and access management team
- D. Business unit management

Answer: D

Explanation:

The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.

The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity

and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

NEW QUESTION 20

- (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 23

- (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 27

- (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 32

- (Topic 1)

Which of the following is MOST important to consider when determining asset valuation?

- A. Asset recovery cost
- B. Asset classification level
- C. Cost of insurance premiums
- D. Potential business loss

Answer: D

Explanation:

Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important

as potential business loss, as they do not capture the full value of the asset to the organization. References = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

NEW QUESTION 34

- (Topic 1)

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

- A. an inventory of critical data.
- B. criteria for escalation.
- C. a business impact analysis (BIA).
- D. critical infrastructure diagrams.

Answer: B

Explanation:

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

NEW QUESTION 39

- (Topic 1)

An online bank identifies a successful network attack in progress. The bank should FIRST:

- A. isolate the affected network segment.
- B. report the root cause to the board of directors.
- C. assess whether personally identifiable information (PII) is compromised.
- D. shut down the entire network.

Answer: A

Explanation:

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

NEW QUESTION 42

- (Topic 1)

How does an incident response team BEST leverage the results of a business impact analysis (BIA)?

- A. Assigning restoration priority during incidents
- B. Determining total cost of ownership (TCO)
- C. Evaluating vendors critical to business recovery
- D. Calculating residual risk after the incident recovery phase

Answer: A

Explanation:

The incident response team can best leverage the results of a business impact analysis (BIA) by assigning restoration priority during incidents. A BIA is a process that identifies and evaluates the criticality and dependency of the organization's business functions, processes, and resources, and the potential impacts and consequences of their disruption or loss. The BIA results provide the basis for determining the recovery objectives, strategies, and plans for the organization's business continuity and disaster recovery. By using the BIA results, the incident response team can prioritize the restoration of the most critical and time-sensitive business functions, processes, and resources, and allocate the appropriate resources, personnel, and time to minimize the impact and duration of the incident. Determining total cost of ownership (TCO) (B) is not a relevant way to leverage the results of a BIA, as it is not directly related to incident response. TCO is a financial metric that estimates the total direct and indirect costs of owning and operating an asset or a system over its lifecycle. TCO may be useful for evaluating the cost-effectiveness and return on investment of different security solutions or alternatives, but it does not help the incident response team to respond to or recover from an incident.

Evaluating vendors critical to business recovery (C) is also not a relevant way to leverage the results of a BIA, as it is not a primary responsibility of the incident response team. Evaluating vendors critical to business recovery is a part of the vendor management process, which involves selecting, contracting, monitoring, and reviewing the vendors that provide essential products or services to support the organization's business continuity and disaster recovery. Evaluating vendors critical to business recovery may be done before or after an incident, but not during an incident, as it does not contribute to the incident response or restoration activities.

Calculating residual risk after the incident recovery phase (D) is also not a relevant way to leverage the results of a BIA, as it is not a timely or effective use of the BIA results. Residual risk is the risk that remains after the implementation of risk treatment or mitigation measures. Calculating residual risk after the incident recovery phase may be done as a part of the incident review or improvement process, but not during the incident response or restoration phase, as it does not help the incident response team to resolve or contain the incident.

References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Business Impact Analysis, page 182-1831

NEW QUESTION 44

- (Topic 1)

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

- A. Defining information stewardship roles
- B. Defining security asset categorization
- C. Assigning information asset ownership
- D. Developing a records retention schedule

Answer: C

Explanation:

The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

NEW QUESTION 47

- (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 51

- (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 54

- (Topic 1)

Which of the following is the FIRST step to establishing an effective information security program?

- A. Conduct a compliance review.
- B. Assign accountability.
- C. Perform a business impact analysis (BIA).
- D. Create a business case.

Answer: D

Explanation:

According to the CISM Review Manual, the first step to establishing an effective information security program is to create a business case that aligns the program objectives with the organization's goals and strategies. A business case provides the rationale and justification for the information security program and helps to secure the necessary resources and support from senior management and other stakeholders. A business case should include the following elements:

- ? The scope and objectives of the information security program
- ? The current state of information security in the organization and the gap analysis
- ? The benefits and value proposition of the information security program
- ? The risks and challenges of the information security program
- ? The estimated costs and resources of the information security program
- ? The expected outcomes and performance indicators of the information security program
- ? The implementation plan and timeline of the information security program

References = CISM Review Manual, 16th Edition, Chapter 3, Section 2, pages 97-99.

NEW QUESTION 58

- (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 63

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 64

- (Topic 1)

When developing an asset classification program, which of the following steps should be completed FIRST?

- A. Categorize each asset.
- B. Create an inventory
- C. &
- D. Create a business case for a digital rights management tool.
- E. Implement a data loss prevention (OLP) system.

Answer: B

Explanation:

Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified. An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification¹². Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset¹². Creating a business case for a digital rights management tool © is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets³. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media⁴. References = 1: CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA²; 3: What is Digital Rights Management? - Definition from Techopedia³; 4: What is Data Loss Prevention (DLP)? - Definition from Techopedia⁴

NEW QUESTION 67

- (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 71

- (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 72

- (Topic 1)

Which of the following is the BEST course of action for an information security manager to align security and business goals?

- A. Conducting a business impact analysis (BIA)
- B. Reviewing the business strategy
- C. Defining key performance indicators (KPIs)
- D. Actively engaging with stakeholders

Answer: D

Explanation:

= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them. By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION 77

- (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 81

- (Topic 1)

An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?

- A. Determine which country's information security regulations will be used.
- B. Merge the two existing information security programs.
- C. Apply the existing information security program to the acquired company.
- D. Evaluate the information security laws that apply to the acquired company.

Answer: D

Explanation:

The information security manager should first evaluate the information security laws that apply to the acquired company, as they may differ from the laws of the parent organization. This will help the information security manager to understand the legal and regulatory requirements, risks, and challenges that the acquired company faces in its operating environment. The information security manager can then determine the best approach to align the information security programs of

the two entities, taking into account the different laws and regulations, as well as the business objectives and strategies of the acquisition. References = : CISM Review Manual 15th Edition, page 32.

NEW QUESTION 82

- (Topic 1)

Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?

- A. Perform a risk assessment.
- B. Reduce security hardening settings.
- C. Inform business management of the risk.
- D. Document a security exception.

Answer: A

Explanation:

Security hardening is the process of applying security configuration settings to systems and software to reduce their attack surface and improve their resistance to threats¹. Security hardening settings are based on industry standards and best practices, such as the CIS Benchmarks², which provide recommended security configurations for various software applications, operating systems, and network devices. However, security hardening settings may not always be compatible with the business requirements and objectives of an organization, and may negatively impact the functionality, performance, or usability of the systems and software³. Therefore, before applying any security hardening settings, an information security manager should perform a risk assessment to evaluate the potential benefits and drawbacks of the settings, and to identify and prioritize the risks associated with them. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses. A risk assessment helps the information security manager to balance the security and business needs of the organization, and to communicate the risk level and impact to the relevant stakeholders. A risk assessment should be performed first, before taking any other actions, such as reducing security hardening settings, informing business management of the risk, or documenting a security exception, because it provides the necessary information and justification for making informed and rational decisions. References = 1: Basics of the CIS Hardening Guidelines | RSI Security 2: CIS Baseline Hardening and Security Configuration Guide | CalCom 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 145 : CISM Review Manual 15th Edition, page 146 : CISM Review Manual 15th Edition, page 147

NEW QUESTION 84

- (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 85

- (Topic 1)

Which of the following processes BEST supports the evaluation of incident response effectiveness?

- A. Root cause analysis
- B. Post-incident review
- C. Chain of custody
- D. Incident logging

Answer: B

Explanation:

A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement¹. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity².

A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders³. A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.

The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization ensure that the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the

effectiveness of the response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation. However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices. References = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: Post-Incident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

NEW QUESTION 86

- (Topic 1)

Which of the following is MOST critical when creating an incident response plan?

- A. Identifying vulnerable data assets
- B. Identifying what constitutes an incident
- C. Documenting incident notification and escalation processes
- D. Aligning with the risk assessment process

Answer: C

Explanation:

= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION 88

- (Topic 1)

Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

- A. Publish adopted information security standards.
- B. Perform annual information security compliance reviews.
- C. Implement an information security governance framework.
- D. Define penalties for information security noncompliance.

Answer: C

Explanation:

The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

NEW QUESTION 91

- (Topic 1)

Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

- A. Disaster recovery plan (DRP)
- B. Incident response plan
- C. Business continuity plan (BCP)
- D. Business contingency plan

Answer: C

Explanation:

= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources. Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:

- ? Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
- ? Restore the essential functions and services as quickly and efficiently as possible.
- ? Protect the health, safety, and welfare of the staff, customers, and partners.
- ? Meet the legal, regulatory, contractual, and ethical obligations of the organization.
- ? Learn from the disaster and improve the business continuity capabilities and readiness of the organization.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

NEW QUESTION 94

- (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 95

- (Topic 3)

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

- A. After the incident has been mitigated
- B. After the incident has been confirmed.
- C. After the potential incident has been toggled
- D. After the incident has been contained

Answer: B

Explanation:

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

NEW QUESTION 97

- (Topic 3)

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

- A. Post-implementation phase
- B. Implementation phase
- C. Development phase
- D. Design phase

Answer: C

Explanation:

The development phase is the stage of the system development life cycle (SDLC) where the system requirements, design, architecture, and implementation are performed. The development phase is most challenging to implement security controls because it involves complex and dynamic processes that may not be well understood or documented. Security controls are essential for ensuring the confidentiality, integrity, and availability of the system and its data, as well as for complying with regulatory and contractual obligations. However, security controls may also introduce additional costs, risks, and constraints to the development process, such as:

- ? Increased complexity and overhead of testing, verification, validation, and maintenance
- ? Reduced flexibility and agility of changing requirements or design
- ? Increased dependency on external vendors or third parties for security services or products
- ? Increased vulnerability to errors, defects, or vulnerabilities in the code or configuration
- ? Increased difficulty in measuring and reporting on security performance or effectiveness

Therefore, implementing security controls in the development phase requires careful planning, coordination, communication, and collaboration among all stakeholders involved in the SDLC. It also requires a clear understanding of the security objectives, scope, criteria, standards, policies, procedures, roles, responsibilities, and resources for the system. Moreover, it requires a proactive approach to identifying and mitigating potential threats or risks that may affect the security of the system.

References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: System Development Life Cycle (SDLC)2

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

NEW QUESTION 99

- (Topic 3)

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

- A. Conduct a business impact analysis (BIA)
- B. Identify the response and recovery learns.
- C. Review the communications plan.
- D. Develop response and recovery strategies.

Answer: A

Explanation:

Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)2. Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the

communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate solutions and procedures for restoring the critical business functions or processes. References: 2 <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business-impact-analysis-bia-and-disaster-recovery-planning-drp>

NEW QUESTION 104

- (Topic 3)

Which of the following metrics is MOST appropriate for evaluating the incident notification process?

- A. Average total cost of downtime per reported incident
- B. Elapsed time between response and resolution
- C. Average number of incidents per reporting period
- D. Elapsed time between detection, reporting, and response

Answer: D

Explanation:

Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.

References:

? <https://www.atlassian.com/incident-management/kpis/common-metrics>

? <https://securityscorecard.com/blog/how-to-use-incident-response-metrics/>

? https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

NEW QUESTION 108

- (Topic 3)

Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?

- A. Demonstrating the program's value to the organization
- B. Discussing governance programs found in similar organizations
- C. Providing the results of external audits
- D. Providing examples of information security incidents within the organization

Answer: A

Explanation:

The best way to obtain senior management support for an information security governance program is to demonstrate the program's value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. References:

? <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process>

? <https://www.sans.org/white-papers/992/>

? <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for-your-security-program.html>

NEW QUESTION 110

- (Topic 3)

Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?

- A. Conducting periodic vulnerability assessments
- B. Communicating business impact analysis (BIA) results
- C. Establishing effective stakeholder relationships
- D. Defining the organization's risk management framework

Answer: C

Explanation:

The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders.

NEW QUESTION 115

- (Topic 3)

Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

- A. Escalation processes
- B. Recovery time objective (RTO)
- C. Security audit reports
- D. Technological capabilities

Answer: A

Explanation:

Escalation processes are the most important security consideration when developing an incident response strategy with a cloud provider, as they define the roles, responsibilities, communication channels, and decision-making authority for both parties in the event of a security incident. Escalation processes help to ensure timely and effective response, coordination, and resolution of security incidents, as well as to avoid conflicts or confusion. (From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION 119

- (Topic 1)

The PRIMARY benefit of introducing a single point of administration in network monitoring is that it:

- A. reduces unauthorized access to systems.
- B. promotes efficiency in control of the environment.
- C. prevents inconsistencies in information in the distributed environment.
- D. allows administrative staff to make management decisions.

Answer: B

Explanation:

A single point of administration in network monitoring is a centralized system that allows network administrators to manage and monitor the entire network from one location. A single point of administration can provide several benefits, such as:

? Promoting efficiency in control of the environment: A single point of administration can simplify and streamline the network management tasks, such as configuration, troubleshooting, performance optimization, security updates, backup and recovery, etc. It can also reduce the time and cost of network maintenance and administration, as well as improve the consistency and quality of network services.

? Reducing unauthorized access to systems: A single point of administration can enhance the network security by implementing centralized authentication, authorization and auditing mechanisms. It can also enforce consistent security policies and standards across the network, and detect and respond to any unauthorized or malicious activities.

? Preventing inconsistencies in information in the distributed environment: A single point of administration can ensure the data integrity and availability by synchronizing and replicating the data across the network nodes. It can also provide a unified view of the network status and performance, and facilitate the analysis and reporting of network data.

? Allowing administrative staff to make management decisions: A single point of administration can support the decision-making process by providing relevant and timely information and feedback to the network administrators. It can also enable the administrators to implement changes and improvements to the network based on the business needs and objectives.

Therefore, the primary benefit of introducing a single point of administration in network monitoring is that it promotes efficiency in control of the environment, as it simplifies and streamlines the network management tasks and improves the network performance and quality. References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 205.

NEW QUESTION 124

- (Topic 3)

Which of the following should an information security manager do FIRST when there is a conflict between the organization's information security policy and a local regulation?

- A. Enforce the local regulation.
- B. Obtain legal guidance.
- C. Enforce the organization's information security policy.
- D. Obtain an independent assessment of the regulation.

Answer: B

Explanation:

The information security manager should first obtain legal guidance when there is a conflict between the organization's information security policy and a local regulation, because this will help to understand the implications and consequences of the conflict, and to identify the possible options and solutions for resolving it. The information security manager should also consult with the relevant stakeholders, such as senior management, business owners, and information owners, to determine the best course of action that aligns with the organization's objectives, risk appetite, and compliance obligations. Enforcing the local regulation or the organization's information security policy without legal guidance may expose the organization to legal liabilities, security risks, or operational disruptions. Obtaining an independent assessment of the regulation may be helpful, but it is not the first step to take.

References = CISM Review Manual, 16th Edition, page 691; A Guide to ISACA CISM Domains & Domain 1: Information Security Governance2

NEW QUESTION 127

- (Topic 3)

Which of the following is the BEST way to ensure the business continuity plan (BCP) is current?

- A. Manage business process changes.
- B. Update business impact analyses (BIAs) on a regular basis.
- C. Conduct periodic testing.
- D. Review and update emergency contact lists.

Answer: C

Explanation:

Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.

References: The CISM Review Manual 2023 states that “testing is a critical component of the BCP process” and that “testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations” (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this Answer “Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update” (p. 98). Additionally, the article Business Continuity Planning:

Testing an Organization’s Plan from the ISACA Journal 2019 states that “testing is essential to ensure that the BCP is current and effective” and that “testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks” (p. 1)

NEW QUESTION 129

- (Topic 3)

Which of the following should be done FIRST once a cybersecurity attack has been confirmed?

- A. Isolate the affected system.
- B. Notify senior management.
- C. Power down the system.
- D. Contact legal authorities.

Answer: A

Explanation:

Isolating the affected system is the first step in the incident response process, as it helps to contain the attack, prevent further damage, and preserve the evidence for analysis. Isolating the system can be done by disconnecting it from the network, blocking the malicious traffic, or applying quarantine rules.

References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.22; Cybersecurity Incident Response Exercise Guidance3

NEW QUESTION 130

- (Topic 3)

Which of the following is MOST important to maintain integration among the incident response plan, business continuity plan (BCP). and disaster recovery plan (DRP)?

- A. Asset classification
- B. Recovery time objectives (RTOs)
- C. Chain of custody
- D. Escalation procedures

Answer: B

Explanation:

Recovery time objectives (RTOs) are the maximum acceptable time that an organization can be offline or unavailable after a disruption. RTOs are important to maintain integration among the incident response plan, business continuity plan (BCP), and disaster recovery plan (DRP) because they help align the recovery goals and strategies of each plan. By defining clear and realistic RTOs, an organization can ensure that its IT infrastructure and systems are restored as quickly as possible after a disaster, minimizing the impact on business operations and customer satisfaction.

References = CISM Manual, Chapter 6: Incident Response Planning, Section 6.2: Recovery Time Objectives (RTOs), page 971

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

NEW QUESTION 132

- (Topic 3)

Which of the following is a viable containment strategy for a distributed denial of service (DDoS) attack?

- A. Block IP addresses used by the attacker
- B. Redirect the attacker's traffic
- C. Disable firewall ports exploited by the attacker.
- D. Power off affected servers

Answer: B

Explanation:

Redirecting the attacker’s traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker’s traffic is a technique that involves changing the DNS settings or routing tables to send the attacker’s traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker’s behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server. Redirecting the attacker’s traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker’s traffic is the correct answer.

References:

? <https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation- strategy>

? <https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy>

? <https://www.cloudflare.com/learning/ddos/glossary/sinkholing/>.

NEW QUESTION 134

- (Topic 3)

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

- A. Legal
- B. Information security
- C. Help desk
- D. Human resources (HR)

Answer: B

Explanation:

Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References =

CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner."

SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process."

IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access."

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

NEW QUESTION 137

- (Topic 3)

Senior management has just accepted the risk of noncompliance with a new regulation What should the information security manager do NEX*P

- A. Report the decision to the compliance officer
- B. Update details within the risk register.
- C. Reassess the organization's risk tolerance.
- D. Assess the impact of the regulation.

Answer: B

Explanation:

Updating details within the risk register is the next step for the information security manager to do after senior management has accepted the risk of noncompliance with a new regulation because it records and communicates the risk status, impact, and response strategy to the relevant stakeholders. Reporting the decision to the compliance officer is not the next step, but rather a possible subsequent step that involves informing and consulting with the compliance officer about the risk acceptance and its implications. Reassessing the organization's risk tolerance is not the next step, but rather a possible subsequent step that involves reviewing and adjusting the organization's risk appetite and thresholds based on the risk acceptance and its implications. Assessing the impact of the regulation is not the next step, but rather a previous step that involves analyzing and evaluating the potential consequences and likelihood of noncompliance with the regulation. References: <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004> <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-information-security-management-system>

NEW QUESTION 140

- (Topic 3)

An organization is experiencing a sharp increase in incidents related to phishing messages. The root cause is an outdated email filtering system that is no longer supported by the vendor. Which of the following should be the information security manager's FIRST course of action?

- A. Reinforce security awareness practices for end users.
- B. Temporarily outsource the email system to a cloud provider.
- C. Develop a business case to replace the system.
- D. Monitor outgoing traffic on the firewall.

Answer: C

Explanation:

Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics."

Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages."

Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

NEW QUESTION 141

- (Topic 3)

The MOST important information for influencing management's support of information security is:

- A. an demonstration of alignment with the business strategy.
- B. An identification of the overall threat landscape.
- C. A report of a successful attack on a competitor.

D. An identification of organizational risks.

Answer: A

Explanation:

The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. References: <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems>
<https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives>

NEW QUESTION 142

- (Topic 3)

Which of the following **MUST** be established to maintain an effective information security governance framework?

- A. Security controls automation
- B. Defined security metrics
- C. Change management processes
- D. Security policy provisions

Answer: D

Explanation:

Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. References:

? <https://www.iso.org/standard/74046.html>

? <https://www.nist.gov/cyberframework>

? <https://www.iso.org/standard/27001>

NEW QUESTION 144

- (Topic 3)

Which of the following is the **MOST** important consideration when developing key performance indicators (KPIs) for the information security program?

- A. Alignment with financial reporting
- B. Alignment with business initiatives
- C. Alignment with industry frameworks
- D. Alignment with risk appetite

Answer: B

Explanation:

Explore

The most important consideration when developing key performance indicators (KPIs) for the information security program is B. Alignment with business initiatives. This is because KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. KPIs should also reflect the needs, expectations, and challenges of the business stakeholders, and provide relevant, meaningful, and actionable information for decision making and improvement. KPIs should not be too technical, complex, or ambiguous, but rather focus on the key aspects of information security performance, such as risk, compliance, maturity, value, and effectiveness.

KPIs are measurable values that demonstrate how effectively the information security program is achieving its objectives and delivering value to the organization. KPIs should be aligned with the business initiatives, such as the strategic goals, the mission, the vision, and the values of the organization, and support the achievement of the desired outcomes and benefits. (From CISM Manual or related resources)

References = CISM Review Manual 15th Edition, Chapter 1, Section 1.3.2, page 281; CISM Domain – Information Security Program Development | Infosec2; KPIs in Information Security: The 10 Most Important Security Metrics3

NEW QUESTION 147

- (Topic 3)

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do **FIRST**?

- A. Set up communication channels for the target audience.
- B. Determine the needs and requirements of each audience.
- C. Create a comprehensive singular communication
- D. Invoke the organization's incident response plan.

Answer: D

Explanation:

The information security manager should do **FIRST** invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a comprehensive singular communication are all important steps for communicating effectively with the board,

regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the relevant information to the target audience according to the plan. References = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012 Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

NEW QUESTION 149

- (Topic 3)

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

- A. Business continuity plan (BCP)
- B. Cost-benefit analysis
- C. Classification scheme
- D. Senior management support

Answer: D

Explanation:

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

The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality. References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1:

Incident Response Plan2

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

NEW QUESTION 152

- (Topic 2)

Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

- A. Risk acceptance by the business has been documented
- B. Teams and individuals responsible for recovery have been identified
- C. Copies of recovery and incident response plans are kept offsite
- D. Incident response and recovery plans are documented in simple language

Answer: B

Explanation:

Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities. This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

NEW QUESTION 156

- (Topic 2)

Which of the following has the GREATEST influence on an organization's information security strategy?

- A. The organization's risk tolerance
- B. The organizational structure
- C. Industry security standards
- D. Information security awareness

Answer: A

Explanation:

An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives. Therefore, an organization's risk tolerance has the greatest influence on its information security strategy. The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.

An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION 158

- (Topic 2)

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

- A. Helping to determine the recovery point objective (RPO)
- B. Providing a basis for implementing a need-to-know policy
- C. Supporting segregation of duties
- D. Defining resource ownership

Answer: B

Explanation:

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

- Defining the value and protection requirements of different types of information
- Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
- Establishing the roles and responsibilities of information owners, custodians, and users
- Enforcing access controls and encryption for the information
- Documenting the security policies and procedures for the information

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

Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level.

RPO is the acceptable amount of data loss in case of a disruption³. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud⁴. Defining resource ownership is not a benefit, but rather a component of information asset classification.

Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group⁵. References: 1: Information Classification - Advisera 2: Need-to-Know Principle - NIST 3: Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST :

Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy - UCI

NEW QUESTION 161

- (Topic 2)

The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:

- A. the organization has the required funds to implement the plan.
- B. compliance with legal and regulatory requirements.
- C. staff participation in information security efforts.
- D. the plan aligns with corporate governance.

Answer: D

Explanation:

The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly¹. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization². The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives³. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation⁴. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253: CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA, 2017, page 27.

Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION 166

- (Topic 2)

Which of the following is the MOST effective way to prevent information security incidents?

- A. Implementing a security information and event management (SIEM) tool
- B. Implementing a security awareness training program for employees
- C. Deploying a consistent incident response approach
- D. Deploying intrusion detection tools in the network environment

Answer: B

Explanation:

The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management (SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

NEW QUESTION 170

- (Topic 2)

An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?

- A. Install the OS, patches, and application from the original source.
- B. Restore the OS, patches, and application from a backup.
- C. Restore the application and data from a forensic copy.
- D. Remove all signs of the intrusion from the OS and application.

Answer: A

Explanation:

After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of

the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.

References =

? ISACA, CISM Review Manual, 16th Edition, 2020, page 2401

? ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132

The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

NEW QUESTION 171

- (Topic 2)

Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?

- A. Embedding compliance requirements within operational processes
- B. Engaging external experts to provide guidance on changes in compliance requirements
- C. Performing periodic audits for compliance with legal and regulatory requirements
- D. Assigning the operations manager accountability for meeting compliance requirements

Answer: A

Explanation:

Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.

Regulatory compliance involves following external legal mandates set forth by state, federal, or international government². Compliance requirements may vary depending on the industry, location, and nature of the organization². Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct².

NEW QUESTION 176

.....

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 First Try
- * CISM Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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