Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
- (Topic 2)
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.

Answer: A

Explanation:
The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

NEW QUESTION 2
- (Topic 2)
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?

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

Answer: B

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

NEW QUESTION 3
- (Topic 1)
The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

A. enhance the organization's antivirus controls.
B. eliminate the risk of data loss.
C. complement the organization's detective controls.
D. reduce the need for a security awareness program.

Answer: C

Explanation:
A data loss prevention (DLP) solution is a type of detective control that monitors and prevents unauthorized transmission or leakage of sensitive data from the organization. A DLP solution can enhance the organization’s antivirus controls by detecting and blocking malicious code that attempts to exfiltrate data, but this is not its main benefit. A DLP solution cannot eliminate the risk of data loss, as there may be other sources of data loss that are not covered by the DLP solution, such as physical theft, accidental deletion, or natural disasters. A DLP solution also does not reduce the need for a security awareness program, as human factors are often the root cause of data loss incidents. A security awareness program can educate and motivate employees to follow security policies and best practices, and to report any suspicious or anomalous activities. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, page 79.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1003.

NEW QUESTION 4
- (Topic 1)
Which of the following is PRIMARILY determined by asset classification?

A. Insurance coverage required for assets
B. Level of protection required for assets
C. Priority for asset replacement
D. Replacement cost of assets

Answer: B

Explanation:
Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other

criteria such as risk appetite, business impact, availability and market value4. References = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

NEW QUESTION 5
- (Topic 1)
Which of the following is MOST helpful for determining which information security policies should be implemented by an organization?

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

Answer: A

Explanation:
Information security policies are high-level statements or rules that define the goals and objectives of information security in an organization, and provide the framework and direction for implementing and enforcing security controls and processes1. Information security policies should be aligned with the organization's business goals and objectives, and reflect the organization's risk appetite and tolerance2. Therefore, the most helpful activity for determining which information security policies should be implemented by an organization is a risk assessment.
A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks that an organization faces, and determining the appropriate risk responses3. A risk assessment helps to determine the following aspects of information security policies:
? The scope and applicability of the policies, based on the assets, threats, and vulnerabilities that affect the organization's security objectives and requirements.
? The level and type of security controls and processes that are needed to mitigate the risks, based on the likelihood and impact of the risk scenarios and the cost-benefit analysis of the risk responses.
? The roles and responsibilities of the stakeholders involved in the implementation and enforcement of the policies, based on the risk ownership and accountability.
? The metrics and indicators that are used to measure and monitor the effectiveness and compliance of the policies, based on the risk appetite and tolerance.
The other options, such as a business impact analysis (BIA), a vulnerability assessment, or industry best practices, are not as helpful as a risk assessment for determining which information security policies should be implemented by an organization, because they have the following limitations:
? A business impact analysis (BIA) is a process of identifying and evaluating the potential effects of disruptions or incidents on the organization's critical business functions and processes, and determining the recovery priorities and objectives. A BIA can help to support the risk assessment by providing information on the impact and criticality of the assets and processes, but it cannot identify or analyze the threats and vulnerabilities that pose risks to the organization, or determine the appropriate risk responses or controls.
? A vulnerability assessment is a process of identifying and measuring the weaknesses or flaws in the organization's systems, networks, or applications that could be exploited by threat actors. A vulnerability assessment can help to support the risk assessment by providing information on the vulnerabilities and exposures that affect the organization's security posture, but it cannot identify or analyze the threats or likelihood that could exploit the vulnerabilities, or determine the appropriate risk responses or controls.
? Industry best practices are the standards or guidelines that are widely accepted and followed by the information security community or the organization's industry sector, based on the experience and knowledge of the experts and practitioners. Industry best practices can help to inform and guide the development and implementation of information security policies, but they cannot replace or substitute the risk assessment, as they may not reflect the organization's specific context, needs, and objectives, or address the organization's unique risks and challenges.
References = 1: CISM Review Manual 15th Edition, page 29 2: CISM Review Manual 15th Edition, page 30 3: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 : CISM Review Manual 15th Edition, page 126

NEW QUESTION 6
- (Topic 1)
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 7
- (Topic 1)
Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.

D. Base mandatory review and exception approvals on inherent risk.

Answer: A

Explanation:
= Residual risk is the risk that remains after applying security controls. It reflects the actual exposure of the organization to noncompliance issues. Therefore, basing mandatory review and exception approvals on residual risk is the best approach for governing noncompliance with security requirements. It ensures that the organization is aware of the potential impact and likelihood of noncompliance and can make informed decisions about accepting, mitigating, or transferring the risk. References = CISM Review Manual 15th Edition, page 78.

NEW QUESTION 8
- (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 9
- (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 10
- (Topic 1)
Which of the following would be the BEST way for an information security manager to improve the effectiveness of an organization’s information security program?

A. Focus on addressing conflicts between security and performance.
B. Collaborate with business and IT functions in determining controls.
C. Include information security requirements in the change control process.
D. Obtain assistance from IT to implement automated security cantrals.

Answer: B

Explanation:
The best way for an information security manager to improve the effectiveness of an organization’s information security program is to collaborate with business and IT functions in determining controls. Collaboration is a key factor for ensuring that the information security program is aligned with the organization’s business objectives, risk appetite, and security strategy, and that it supports the business processes and activities. Collaboration also helps to gain the buy-in, involvement, and ownership of the business and IT functions, who are the primary stakeholders and users of the information security program. Collaboration also facilitates the communication, coordination, and integration of the information security program across the organization, and enables the information security manager to understand the needs, expectations, and challenges of the business and IT functions, and to propose the most appropriate and effective security controls and solutions.
Focusing on addressing conflicts between security and performance (A) is a possible way to improve the effectiveness of an information security program, but not the best one. Security and performance are often competing or conflicting goals, as security controls may introduce overhead, complexity, or delays that affect the efficiency, usability, or availability of the systems or processes. Addressing these conflicts may help to optimize the balance and trade-off between security and performance, and to enhance the user satisfaction and acceptance of the security controls. However, focusing on addressing conflicts between security and

performance does not necessarily improve the alignment, integration, or communication of the information security program with the business and IT functions, nor does it ensure the involvement or ownership of the stakeholders.
Including information security requirements in the change control process © is also a possible way to improve the effectiveness of an information security program, but not the best one. The change control process is a process that manages the initiation, approval, implementation, and review of changes to the systems or processes, such as enhancements, updates, or fixes. Including information security requirements in the change control process may help to ensure that the changes do not introduce new or increased security risks or impacts, and that they comply with the security policies, standards, and procedures. However, including information security requirements in the change control process does not necessarily improve the collaboration, communication, or coordination of the information security program with the business and IT functions, nor does it ensure the buy-in or involvement of the stakeholders.
Obtaining assistance from IT to implement automated security controls (D) is also a possible way to improve the effectiveness of an information security program, but not the best one. Automated security controls are security controls that are implemented by using software, hardware, or other technologies, such as encryption, firewalls, or antivirus, to perform security functions or tasks without human intervention. Obtaining assistance from IT to implement automated security controls may help to improve the efficiency, consistency, or reliability of the security controls, and to reduce the human errors, negligence, or malicious actions. However, obtaining assistance from IT to implement automated security controls does not necessarily improve the collaboration, communication, or integration of the information security program with the business and IT functions, nor does it ensure the ownership or involvement of the stakeholders. References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy Development, Subsection: Collaboration, page 24-251

NEW QUESTION 10
- (Topic 1)
Which of the following will BEST facilitate the integration of information security governance into enterprise governance?

A. Developing an information security policy based on risk assessments
B. Establishing an information security steering committee
C. Documenting the information security governance framework
D. Implementing an information security awareness program

Answer: B

Explanation:
Establishing an information security steering committee is the best way to facilitate the integration of information security governance into enterprise governance. The information security steering committee is a cross-functional group of senior managers who provide strategic direction, oversight, and support for the information security program. The committee ensures that the information security strategy is aligned with the enterprise strategy, objectives, and risk appetite. The committee also fosters collaboration and communication among various stakeholders and promotes a culture of security awareness and accountability. Developing an information security policy, documenting the information security governance framework, and implementing an information security awareness program are all important activities for implementing and maintaining information security governance, but they do not necessarily facilitate its integration into enterprise governance. These activities may be initiated or endorsed by the information security steering committee, but they are not sufficient to ensure that information security governance is embedded into the enterprise governance structure and
processes. References = CISM Review Manual 2023, page 34 1; CISM Practice Quiz 2

NEW QUESTION 12
- (Topic 1)
Which of the following is the MOST important consideration when establishing an organization's information security governance committee?

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

Answer: D

Explanation:
= The most important consideration when establishing an organization’s information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization’s business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization’s mission, vision, and values. Having a diverse and representative committee also helps to foster a culture of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.
Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization’s business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization’s business objectives, and to allocate appropriate resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the organization’s information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee’s ability to monitor and evaluate the performance and progress of the information security program. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1014.

NEW QUESTION 13
- (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 14
- (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 16
- (Topic 1)
The MOST important reason for having an information security manager serve on the change management committee is to:

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

Answer: D

Explanation:
The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2.
The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.
The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes.
Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk.
References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION 21
- (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 22
- (Topic 1)
Which of the following would BEST ensure that security is integrated during application development?

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

Answer: D

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

NEW QUESTION 24
- (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 28

- (Topic 1)
In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:

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

Answer: D

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

NEW QUESTION 29
- (Topic 1)
Which of the following BEST ensures timely and reliable access to services?

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

Answer: C

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

NEW QUESTION 34
- (Topic 1)
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?

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

Answer: A

Explanation:
= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios.
These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations.
References = CISM Review Manual 2023, page 189 1; CISM Practice Quiz 2

NEW QUESTION 37
- (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 42
- (Topic 1)
Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

A. Documentation of control procedures
B. Standardization of compliance requirements
C. Automation of controls
D. Integration of assurance efforts

Answer: B

Explanation:
= Standardization of compliance requirements is the best approach to reduce unnecessary duplication of compliance activities, as it allows for a common understanding of the objectives and expectations of various stakeholders, such as regulators, auditors, customers, and business partners. Standardization also facilitates the alignment of compliance activities with the organization's risk appetite and tolerance, and enables the identification and elimination of redundant or conflicting controls. References = CISM Review Manual, 27th Edition, page 721; CISM Review Questions, Answers & Explanations Database, 12th Edition, question 952 Learn more:

NEW QUESTION 47
- (Topic 1)
Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

A. Collect additional metrics.
B. Perform a cost-benefit analysis.
C. Submit funding request to senior management.
D. Begin due diligence on the outsourcing company.

Answer: B

Explanation:
The first step to gain approval for outsourcing to address a security gap is to perform a cost-benefit analysis, because it helps to evaluate the feasibility and viability of the outsourcing option and compare it with other alternatives. A cost-benefit analysis is a method of estimating and comparing the costs and benefits of a project or a decision, in terms of financial, operational, and strategic aspects. A cost-benefit analysis can help to:
? Identify and quantify the expected costs and benefits of outsourcing, such as the initial and ongoing expenses, the potential savings and revenues, the quality and efficiency of the service, the risks and opportunities, and the alignment with the business objectives and requirements
? Assess and prioritize the criticality and urgency of the security gap, and the impact and likelihood of the related threats and vulnerabilities
? Determine the optimal level and scope of outsourcing, such as the type, duration, and frequency of the service, the roles and responsibilities of the parties involved, and the performance and security standards and metrics
? Justify and communicate the rationale and value proposition of outsourcing, and provide evidence and support for the decision making process
? Establish and document the criteria and process for selecting and evaluating the outsourcing provider, and the contractual and legal terms and conditions
A cost-benefit analysis should be performed before submitting a funding request to senior management, because it can help to demonstrate the need and the return on investment of the outsourcing project, and to secure the budget and the resources. A cost-benefit analysis should also be performed before beginning due diligence on the outsourcing company, because it can help to narrow down the list of potential candidates and to focus on the most relevant and suitable ones. Collecting additional metrics may be a part of the cost-benefit analysis, but it is not the first step, because it requires a clear definition and understanding of the objectives and scope of the outsourcing project.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 173-174, 177-178.

NEW QUESTION 51
- (Topic 1)
Which of the following is the BEST way to achieve compliance with new global regulations related to the protection of personal information?

A. Execute a risk treatment plan.
B. Review contracts and statements of work (SOWs) with vendors.
C. Implement data regionalization controls.
D. Determine current and desired state of controls.

Answer: D

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

NEW QUESTION 56
- (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 60
- (Topic 1)
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology

Answer: B

Explanation:
A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have a higher chance of achieving its objectives and improving the overall security posture of the organization.
References =
? CISM Review Manual 15th Edition, page 1631
? CISM 2020: Information Security & Business Process Alignment, video 22

NEW QUESTION 65
- (Topic 1)
A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:

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

Answer: A

Explanation:
= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.
The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

NEW QUESTION 69
- (Topic 1)
A PRIMARY purpose of creating security policies is to:

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

Answer: D

Explanation:
A security policy is a formal statement of the rules and principles that govern the protection of information assets in an organization. A security policy defines the scope, objectives, roles and responsibilities, and standards of the information security program. A primary purpose of creating security policies is to implement management's security governance strategy, which is the framework that guides the direction and alignment of information security with the business goals and objectives. A security policy translates the management's vision and expectations into specific and measurable requirements and controls that can be

implemented and enforced by the information security staff and other stakeholders. A security policy also helps to establish the accountability and authority of the information security function and to demonstrate the commitment and support of the senior management for the information security program.
References =
? CISM Review Manual 15th Edition, page 1631
? CISM 2020: IT Security Policies2
? CISM domain 1: Information security governance [Updated 2022]3
? What is CISM? - Digital Guardian4

NEW QUESTION 74
- (Topic 1)
An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy, A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

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

Answer: B

Explanation:
Risk acceptance is the decision to accept the level of residual risk after applying security controls, and to tolerate the potential impact and consequences of a security incident. Approval of risk acceptance should be provided by business senior management, as they are the owners and accountable parties of the business processes, activities, and assets that are exposed to the risk. Business senior management should also have the authority and responsibility to allocate the resources, personnel, and budget to implement and monitor the risk acceptance decision, and to report and escalate the risk acceptance status to the board of directors or the executive management.
The chief risk officer (CRO) (A) is a senior executive who oversees the organization’s risk management function, and provides guidance, direction, and support for the identification, assessment, treatment, and monitoring of risks across the organization. The CRO may be involved in the risk acceptance process, such as by reviewing, endorsing, or advising the risk acceptance decision, but the CRO is not the ultimate approver of risk acceptance, as the CRO is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The information security manager © is the manager who leads and coordinates the information security function, and provides guidance, direction, and support for the development, implementation, and maintenance of the information security program and activities. The information security manager may be involved in the risk acceptance process, such as by conducting the risk assessment, recommending the risk treatment options, or documenting the risk acceptance decision, but the information security manager is not the ultimate approver of risk acceptance, as the information security manager is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
The compliance officer (D) is the officer who oversees the organization’s compliance function, and provides guidance, direction, and support for the identification, assessment, implementation, and monitoring of the compliance requirements and obligations across the organization. The compliance officer may be involved in the risk acceptance process, such as by verifying, validating, or advising the risk acceptance decision, but the compliance officer is not the ultimate approver of risk acceptance, as the compliance officer is not the owner or accountable party of the business processes, activities, and assets that are exposed to the risk.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, Subsection: Risk Acceptance, page 95-961

NEW QUESTION 79
- (Topic 1)
An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?

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

Answer: C

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

NEW QUESTION 81
- (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 83
- (Topic 1)
Information security controls should be designed PRIMARILY based on:

A. a business impact analysis (BIA).
B. regulatory requirements.
C. business risk scenarios,
D. a vulnerability assessment.

Answer: C

Explanation:
Information security controls should be designed primarily based on business risk scenarios, because they help to identify and prioritize the most relevant and significant threats and vulnerabilities that may affect the organization's information assets and business objectives. Business risk scenarios are hypothetical situations that describe the possible sources, events, and consequences of a security breach, as well as the likelihood and impact of the occurrence. Business risk scenarios can help to:
? Align the information security controls with the business needs and requirements, and ensure that they support the achievement of the strategic goals and the mission and vision of the organization
? Assess the effectiveness and efficiency of the existing information security controls, and identify the gaps and weaknesses that need to be addressed or improved
? Select and implement the appropriate information security controls that can prevent, detect, or mitigate the risks, and that can provide the optimal level of protection and performance for the information assets
? Evaluate and measure the return on investment and the value proposition of the information security controls, and communicate and justify the rationale and benefits of the controls to the stakeholders and management Information security controls should not be designed primarily based on a business impact analysis (BIA), regulatory requirements, or a vulnerability assessment, because these are secondary or complementary factors that influence the design of the controls, but they do not provide the main basis or criteria for the design. A BIA is a method of estimating and comparing the potential effects of a disruption or a disaster on the critical business functions and processes, in terms of financial, operational, and reputational aspects. A BIA can help to determine the recovery objectives and priorities for the information assets, but it does not identify or address the specific risks and threats that may cause the disruption or the disaster. Regulatory requirements are the legal, contractual, or industry standards and obligations that the organization must comply with regarding information security. Regulatory requirements can help to establish the minimum or baseline level of information security controls that the organization must implement, but they do not reflect the specific or unique needs and challenges of the organization. A vulnerability assessment is a method of identifying and analyzing the weaknesses and flaws in the information systems and assets that may expose them to exploitation or compromise. A vulnerability assessment can help to discover and remediate the existing or potential security issues, but it does not consider the business context or impact of the issues.
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 119-120, 122-123, 125-126, 129-130.

NEW QUESTION 84
- (Topic 1)
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?

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

Answer: D

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

NEW QUESTION 87
- (Topic 1)
Which of the following is MOST important to include in a post-incident review following a data breach?

A. An evaluation of the effectiveness of the information security strategy
B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom

Answer: B

Explanation:
= A post-incident review is a process of analyzing and learning from a security incident, such as a data breach, to improve the security posture and resilience of an organization. A post-incident review should include the following elements12:
? A clear and accurate description of the incident, including its scope, impact, timeline, root cause, and contributing factors.
? A detailed assessment of the effectiveness and efficiency of the incident response process, including the roles and responsibilities, communication channels, coordination mechanisms, escalation procedures, tools and resources, documentation, and reporting.
? An evaluation of the adequacy of existing controls, such as policies, standards, procedures, technical measures, awareness, and training, to prevent, detect, and

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

NEW QUESTION 92
- (Topic 1)
Which of the following activities MUST be performed by an information security manager for change requests?

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

Answer: D

NEW QUESTION 96
- (Topic 1)
Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?

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

Answer: C

Explanation:
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234,
237-238.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.
? Advanced Persistent Threats and Nation-State Actors 1
? Book Review: Advanced Persistent Threats 2
? Advanced Persistent Threat (APT) Protection 3
? Establishing Advanced Persistent Security to Combat Long-Term Threats 4
? What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION 101
- (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 103
- (Topic 1)
When developing an asset classification program, which of the following steps should be completed FIRST?

A. Categorize each asset.
B. Create an inventor
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 106
- (Topic 1)
The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs.
B. are more objective than information security management.
C. can see the overall impact to the business.
D. can balance the technical and business risks.

Answer: A

Explanation:
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION 107
- (Topic 1)
Security administration efforts will be greatly reduced following the deployment of which of the following techniques?

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

Answer: B

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

NEW QUESTION 108
- (Topic 1)
An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?

A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.

Answer: D

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

NEW QUESTION 110
- (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 115
- (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 119
- (Topic 1)
An information security manager learns that a risk owner has approved exceptions to replace key controls with weaker compensating controls to improve process efficiency. Which of the following should be the GREATEST concern?

A. Risk levels may be elevated beyond acceptable limits.
B. Security audits may report more high-risk findings.
C. The compensating controls may not be cost efficient.
D. Noncompliance with industry best practices may result.

Answer: A

Explanation:
Replacing key controls with weaker compensating controls may introduce new vulnerabilities or increase the likelihood or impact of existing threats, thus raising the risk levels beyond the acceptable limits defined by the risk appetite and tolerance of the organization. This may expose the organization to unacceptable losses or damages, such as financial, reputational, legal, or operational. Therefore, the information security manager should be most concerned about the potential elevation of risk levels and ensure that the risk owner is aware of the consequences and accountable for the decision.
References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Treatment, page 941.

NEW QUESTION 121
- (Topic 1)
Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.

Answer: B

Explanation:
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
? 1: Information Security Incident Response Escalation Guideline2, page 4
? 2: A Practical Approach to Incident Management Escalation1, section “Step 2: Log the escalation and record the related incident problems that occurred”
? 3: Computer Security Incident Handling Guide4, page 18

NEW QUESTION 123
- (Topic 1)
Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

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

Answer: A

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

NEW QUESTION 126
- (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 127
- (Topic 1)
Which of the following is the BEST indication ofa successful information security culture?

A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.

Answer: B

Explanation:
The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281.

NEW QUESTION 132
- (Topic 3)
Which of the following BEST indicates the organizational benefit of an information security solution?

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

Answer: D

Explanation:
The best option to indicate the organizational benefit of an information security solution is D. Costs and benefits of the solution calculated over time. This is because costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. ROSI can also help to justify the allocation and optimization of the resources and budget for the information security solution, and to compare and prioritize different security alternatives. ROSI can be calculated by using various methods and formulas, such as the annualized loss expectancy (ALE), the annualized rate of occurrence (ARO), and the cost-benefit analysis (CBA).
Costs and benefits of the solution calculated over time, also known as the return on security investment (ROSI), can help to measure and demonstrate the value and effectiveness of the information security solution in terms of reducing risks, enhancing performance, and achieving strategic goals. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.3, page 1311; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 99, page 26; How to Calculate Return on Security Investment (ROSI) - Infosec2

NEW QUESTION 137
- (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 141
- (Topic 3)
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

A. Authority of the subscriber to approve access to its data
B. Right of the subscriber to conduct onsite audits of the vendor
C. Commingling of subscribers' data on the same physical server
D. Escrow of software code with conditions for code release

Answer: A

Explanation:
Authority of the subscriber to approve access to its data is the greatest concern for an information security manager if omitted from the contract, as it may expose the subscriber’s data to unauthorized or inappropriate access by the vendor or third parties. The subscriber should have the right to control who can access its data, for what purposes, and under what conditions. The contract should also specify the vendor’s obligations to protect the confidentiality, integrity, and availability of the subscriber’s data, and to notify the subscriber of any breaches or incidents.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2201; Drafting and Negotiating Effective Cloud Computing Agreements2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

NEW QUESTION 146
- (Topic 3)
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

A. perform a risk assessment.
B. review the state of security awareness.
C. review information security policies.
D. perform a gap analysis.

Answer: A

Explanation:
According to the CISM Review Manual, performing a risk assessment is the most important course of action for an information security manager during the due diligence phase of an acquisition, as it helps to identify and evaluate the potential threats, vulnerabilities and impacts that may affect the information assets of the target organization. A risk assessment also provides the basis for performing a gap analysis, reviewing the information security policies and awareness, and developing a remediation plan.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.1, page 1411.

NEW QUESTION 150
- (Topic 3)
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

A. To facilitate the continuous improvement of the IT organization
B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan

Answer: B

Explanation:
The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.
The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3: Information security program development and management [2022
update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION 151
- (Topic 3)
The PRIMARY consideration when responding to a ransomware attack should be to ensure:

A. backups are available.
B. the most recent patches have been applied.
C. the ransomware attack is contained
D. the business can operate

Answer: D

Explanation:
Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
? https://www.cisa.gov/stopransomware/ransomware-guide
? https://csrc.nist.gov/Projects/ransomware-protection-and-response
? https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect- respond

NEW QUESTION 155
- (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 156
- (Topic 3)
Which of the following should be the PRIMARY basis for establishing metrics that measure the effectiveness of an information security program?

A. Residual risk
B. Regulatory requirements
C. Risk tolerance
D. Control objectives

Answer: C

Explanation:
The primary basis for establishing metrics that measure the effectiveness of an information security program should be the risk tolerance of the organization, which is the degree of risk that the organization is willing to accept or avoid in pursuit of its objectives. Metrics based on risk tolerance can help to evaluate whether the information security program is aligned with the business strategy, supports the risk management process, and delivers value to the organization. Residual risk, regulatory requirements, and control objectives are also important factors to consider when developing metrics, but they are not as fundamental as the risk tolerance.
References = CISM Review Manual, 16th Edition, page 69

NEW QUESTION 159
- (Topic 3)
Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. a function of the likelihood and impact, should a threat exploit a vulnerability.
B. the magnitude of the impact, should a threat exploit a vulnerability.
C. a function of the cost and effectiveness of controls over a vulnerability.
D. the likelihood of a given threat attempting to exploit a vulnerability

Answer: A

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

NEW QUESTION 161
- (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 163
- (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 167
- (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 169
- (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 173
- (Topic 3)
Which of the following is the MOST important function of an information security steering committee?

A. Assigning data classifications to organizational assets
B. Developing organizational risk assessment processes
C. Obtaining multiple perspectives from the business
D. Defining security standards for logical access controls

Answer: C

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

NEW QUESTION 177
- (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 178
- (Topic 3)
Which of the following is MOST important to have in place for an organization's information security program to be effective?

A. Documented information security processes
B. A comprehensive IT strategy
C. Senior management support
D. Defined and allocated budget

Answer: C

Explanation:
Senior management support is the most important factor to have in place for an organization’s information security program to be effective because it helps to establish the vision, direction, and goals of the program, as well as to allocate the necessary resources and authority to implement and maintain it. Senior management support also helps to foster a security culture within the organization, where security is seen as a shared responsibility and a business enabler. Senior management support also helps to ensure compliance with internal and external security policies and standards, as well as to communicate the value and impact of security to stakeholders. Therefore, senior management support is the correct answer.
References:
? https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
? https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Book let.pdf
? https://www.cdse.edu/Portals/124/Documents/student-guides/IF011-guide.pdf?ver=UA7IDZRN_y066rLB8oAW_w%3d%3d

NEW QUESTION 180
- (Topic 3)
An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.
D. Determine compensating controls.

Answer: C

Explanation:
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third-party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION 185
- (Topic 3)
Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a public-facing web server?

A. Execution of unauthorized commands
B. Prevention of authorized access
C. Defacement of website content
D. Unauthorized access to resources

Answer: B

Explanation:
Prevention of authorized access is the greatest threat posed by a distributed denial of service (DDoS) attack on a public-facing web server because it prevents legitimate users or customers from accessing the web services or resources, causing disruption, dissatisfaction, and potential loss of revenue or reputation. Execution of unauthorized commands is not a threat posed by a DDoS attack, but rather by a remote code execution (RCE) attack. Defacement of website content is not a threat posed by a DDoS attack, but rather by a web application attack. Unauthorized access to resources is not a threat posed by a DDoS attack, but rather by a brute force attack or an authentication bypass attack. References: https://www.isaca.org/resources/isaca- journal/issues/2017/volume-6/the-value-of-penetration-testing https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION 186

- (Topic 3)
Which of the following has the MOST influence on the information security investment process?

A. IT governance framework
B. Information security policy
C. Organizational risk appetite
D. Security key performance indicators (KPIs)

Answer: C

NEW QUESTION 190
- (Topic 3)
Which of the following is necessary to ensure consistent protection for an organization's information assets?

A. Data ownership
B. Classification model
C. Regulatory requirements
D. Control assessment

Answer: B

Explanation:
A classification model is necessary to ensure consistent protection for an organization’s information assets, because it defines the criteria for assigning different levels of sensitivity and criticality to the information assets, and determines the appropriate security controls and handling procedures for each level. Data ownership, regulatory requirements, and control assessment are also important aspects of information security management, but they are not sufficient to ensure consistent protection without a classification model. References = CISM Review Manual, 16th Edition, page 67

NEW QUESTION 194
- (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 199
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISM Practice Exam Features:

* CISM Questions and Answers Updated Frequently

* CISM Practice Questions Verified by Expert Senior Certified Staff

* CISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year