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

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

Answer: C

Explanation:
The information security manager should first determine the risk related to noncompliance with the policy, as this will help to understand the impact and likelihood of the policy violation and the potential consequences for the organization. The information security manager can then use the risk assessment results to communicate the importance of the policy to the IT personnel, propose any necessary changes to the policy or the processes, or request an audit of the policy development process, depending on the situation. Conducting user awareness training, updating policies and procedures, or requesting an audit are possible actions that the information security manager can take after determining the risk, but they are not the first step. References = CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Assessment, page 86; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 59, page 60.

NEW QUESTION 4
- (Topic 1)
Which of the following 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 5
- (Topic 1)
Which of the following is MOST important when conducting a forensic investigation?

A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody

Answer: D

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

NEW QUESTION 6
- (Topic 1)
Which of the following BEST enables staff acceptance of information security policies?

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

Answer: A

Explanation:
= Strong senior management support is the best factor to enable staff acceptance of information security policies, as it demonstrates the commitment and leadership of the organization's top executives in promoting and enforcing a security culture. Senior management support can also help ensure that the information security policies are aligned with the business goals and values, communicated effectively to all levels of the organization, and integrated into the performance evaluation and reward systems. Senior management support can also help overcome any resistance or challenges from other stakeholders, such as business units, customers, or regulators123. References =
? 1: CISM Review Manual 15th Edition, page 26-274
? 2: CISM Practice Quiz, question 1102
? 3: Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, page 5-6

NEW QUESTION 7
- (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 8
- (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 9
- (Topic 1)
An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

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

Answer: C

Explanation:
A gap analysis is a process of comparing the current state of an organization’s security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:
? It helps to understand the scope and impact of the new service on the organization’s security objectives, risks, and controls.
? It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
? It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
? It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
? It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.
The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance, which can be derived from the gap analysis. References = 1: What is a Gap Analysis? |
Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:
* 1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

NEW QUESTION 10
- (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 10
- (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 12
- (Topic 1)
An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?

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

Answer: C

Explanation:
Before implementing any changes to the security incident response plan, the information security manager should first conduct a gap analysis to identify the current state of the plan and compare it with the new requirements. A gap analysis is a systematic process of evaluating the differences between the current and desired state of a system, process, or program. A gap analysis can help to identify the strengths and weaknesses of the existing plan, the gaps that need to be addressed, the priorities and dependencies of the actions, and the resources and costs involved. A gap analysis can also help to create a business case for the changes and justify the investment. A gap analysis can be conducted using various methods and tools, such as frameworks, standards, benchmarks, questionnaires, interviews, audits, or tests1234.
References =
? CISM Review Manual 15th Edition, page 1631
? CISM certified information security manager study guide, page 452
? How To Conduct An Information Security Gap Analysis3
? PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS4

NEW QUESTION 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 20
- (Topic 1)
When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

A. Data is encrypted in transit and at rest at the vendor site.
B. Data is subject to regular access log review.
C. The vendor must be able to amend data.
D. The vendor must agree to the organization's information security policy,

Answer: D

Explanation:
When granting remote access to confidential information to a vendor, the most important security consideration is to ensure that the vendor complies with the organization's information security policy. The information security policy defines the roles, responsibilities, rules, and standards for accessing, handling, and protecting the organization's information assets. The vendor must agree to the policy and sign a contract that specifies the terms and conditions of the access, the security controls to be implemented, the monitoring and auditing mechanisms, the incident reporting and response procedures, and the penalties for non-compliance or breach. The policy also establishes the organization's right to revoke the access at any time if the vendor violates the policy or poses a risk to the organization.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Policies, page 34; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 44, page 45.

NEW QUESTION 24
- (Topic 1)
Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?

A. The security strategy is promoted.
B. Fewer security incidents are reported.
C. Security behavior is improved.
D. More security incidents are detected.

Answer: C

Explanation:
The greatest benefit of conducting an organization-wide security awareness program is to improve the security behavior of the employees, contractors, partners, and other stakeholders who interact with the organization's information assets. Security behavior refers to the actions and decisions that affect the confidentiality, integrity, and availability of information, such as following the security policies and procedures, reporting security incidents, avoiding risky practices, and applying security controls. By improving the security behavior, the organization can reduce the human-related risks and vulnerabilities, enhance the security culture and awareness, and support the security strategy and objectives.
The other options are not as beneficial as improving the security behavior, although they may also be outcomes or objectives of a security awareness program. Promoting the security strategy is important to communicate the vision, mission, and goals of the security function, as well as to align the security activities with the business needs and expectations. However, promoting the security strategy alone is not enough to ensure its implementation and effectiveness, as it also requires the involvement and commitment of the stakeholders, especially the senior management. Reporting fewer security incidents may indicate a lower level of security breaches or threats, but it may also reflect a lack of detection, reporting, or awareness mechanisms. Moreover, reporting fewer security incidents is not a reliable measure of the security performance or maturity, as it does not account for the impact, severity, or root causes of the incidents. Detecting more security incidents may indicate a higher level of security monitoring, alerting, or awareness capabilities, but it may also reflect a higher level of security exposures or attacks. Moreover, detecting more security incidents is not a desirable goal of a security awareness program, as it also implies a higher level of security incidents that need to be responded to and resolved. References =
? CISM Review Manual, 16th Edition, ISACA, 2022, pp. 201-202, 207-208.
? CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1006.
? The Benefits of Information Security and Privacy Awareness Training Programs, ISACA Journal, Volume 1, 2019, 1.

NEW QUESTION 26
- (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 32
- (Topic 1)
Which of the following activities is designed to handle a control failure that leads to a breach?

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

Answer: B

Explanation:
Incident management is the activity designed to handle a control failure that leads to a breach. Incident management is the process of identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. Incident management aims to minimize the impact of a breach, restore normal operations as quickly as possible, and prevent or reduce the likelihood of recurrence. Incident management involves several steps, such as:
? Establishing an incident response team with clear roles and responsibilities
? Developing and maintaining an incident response plan that defines the procedures, tools, and resources for handling incidents
? Implementing detection and reporting mechanisms to identify and communicate incidents
? Performing triage and analysis to assess the scope, severity, and root cause of incidents
? Containing and eradicating the threat and preserving evidence for investigation and legal purposes
? Recovering and restoring the affected systems and data to a secure state
? Evaluating and improving the incident response process and controls based on lessons learned and best practices
References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 223-232.

NEW QUESTION 34
- (Topic 1)
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

A. The time and location that the breach occurred

B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error

Answer: C

Explanation:
The underlying reason for the user error is the most important factor to determine during the post-incident review, as this helps the information security manager to understand the root cause of the breach, and to implement corrective and preventive actions to avoid similar incidents in the future. The underlying reason for the user error may be related to the lack of training, awareness, guidance, or motivation of the user, or to the complexity, usability, or design of the system or process that the user was using. By identifying the underlying reason for the user error, the information security manager can address the human factor of the information security program, and improve the security culture and behavior of the organization. The time and location that the breach occurred, evidence of previous incidents caused by the user, and appropriate disciplinary procedures for user error are not the most important factors to determine during the post-incident review, as they do not provide a comprehensive and holistic understanding of the breach, and may not help to prevent or reduce the likelihood or impact of future incidents.
References = CISM Review Manual 2023, page 1671; CISM Review Questions, Answers & Explanations Manual 2023, page 382; ISACA CISM - iSecPrep, page 233

NEW QUESTION 39
- (Topic 1)
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

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

Answer: B

Explanation:
= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.
References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

NEW QUESTION 44
- (Topic 1)
Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?

A. Cost of the attack to the organization
B. Location of the attacker
C. Method of operation used by the attacker
D. Details from intrusion detection system (IDS) logs

Answer: C

Explanation:
= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

NEW QUESTION 45
- (Topic 1)
An organization is close to going live with the implementation of a cloud-based application. Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?

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

Answer: B

Explanation:
The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.
Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.

Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information. The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project. Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk- averse approach, as it may hinder the organization's innovation and competitiveness. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

NEW QUESTION 46
- (Topic 1)
An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

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

Answer: A

Explanation:
The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization. Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.
Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.
Inviting IT members into regular procurement team meetings to influence best practice © is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.
Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts. References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, Page 141-1421

NEW QUESTION 47
- (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 48
- (Topic 1)
What should be the FIRST step when an Internet of Things (IoT) device in an organization's network is confirmed to have been hacked?

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

Answer: C

Explanation:
= Disconnecting the device from the network is the first step when an IoT device in an organization's network is confirmed to have been hacked, as it prevents the attacker from further compromising the device or using it as a pivot point to attack other devices or systems on the network. Disconnecting the device also helps preserve the evidence of the attack for later forensic analysis and remediation. Disconnecting the device should be done in accordance with the incident response plan and the escalation procedures123. References =
? 1: CISM Review Manual 15th Edition, page 2004
? 2: CISM Practice Quiz, question 1072
? 3: IoT Security: Incident Response, Forensics, and Investigations, section "IoT Incident Response"

NEW QUESTION 52
- (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 53
- (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 55
- (Topic 1)
Which of the following should be the PRIMARY consideration when developing an incident response plan?

A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents

Answer: C

Explanation:
Management support is the primary consideration when developing an incident response plan, as it is essential for obtaining the necessary resources, authority, and commitment for the plan. Management support also helps to ensure that the plan is aligned with the organization’s business objectives, risk appetite, and security strategy, and that it is communicated and enforced across the organization. Management support also facilitates the coordination and collaboration among different stakeholders, such as business units, IT functions, legal, public relations, and external parties, during an incident response.
The definition of an incident (A) is an important component of the incident response plan, as it provides the criteria and thresholds for identifying, classifying, and reporting security incidents. However, the definition of an incident is not the primary consideration, as it is derived from the organization’s security policies, standards, and procedures, and may vary depending on the context and impact of the incident.
Compliance with regulations (B) is also an important factor for the incident response plan, as it helps to ensure that the organization meets its legal and contractual obligations, such as notifying the authorities, customers, or partners of a security breach, preserving the evidence, and reporting the incident outcomes. However, compliance with regulations is not the primary consideration, as it is influenced by the nature and scope of the incident, and the applicable laws and regulations in different jurisdictions.
Previously reported incidents (D) are a valuable source of information and lessons learned for the incident response plan, as they help to identify the common types, causes, and impacts of security incidents, as well as the strengths and weaknesses of the current incident response processes and capabilities. However, previously reported incidents are not the primary consideration, as they are not predictive or comprehensive of the future incidents, and may not reflect the changing threat landscape and business environment. References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 181-1821
Learn more:

NEW QUESTION 58
- (Topic 1)
IT projects have gone over budget with too many security controls being added post- production. Which of the following would MOST help to ensure that relevant controls are applied to a project?

A. Involving information security at each stage of project management
B. Identifying responsibilities during the project business case analysis
C. Creating a data classification framework and providing it to stakeholders
D. Providing stakeholders with minimum information security requirements

Answer: A

Explanation:
The best way to ensure that relevant controls are applied to a project is to involve information security at each stage of project management. This will help to identify and address the security risks and requirements of the project from the beginning, and to integrate security controls into the project design, development, testing, and implementation. This will also help to avoid adding unnecessary or ineffective controls post- production, which can increase the project cost and complexity, and reduce the project performance and quality. By involving information security at each stage of project management, the information security manager can ensure that the project delivers the expected security value and aligns with the organization's security strategy and objectives. References = CISM Review Manual 15th Edition, page 41.

NEW QUESTION 63
- (Topic 1)
A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.
D. Initiate the organization's incident response process.

Answer: D

Explanation:
= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability. The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application. Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action. Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application. Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual 2023, page 211 1; CISM Practice Quiz 2

NEW QUESTION 67
- (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 70
- (Topic 1)
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

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

Answer: B

Explanation:
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues. Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION 72
- (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 76
- (Topic 1)
Who is BEST suited to determine how the information in a database should be classified?

A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner

Answer: D

Explanation:
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements. Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331

NEW QUESTION 77
- (Topic 1)
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

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

Answer: D

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

NEW QUESTION 80
- (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 84
- (Topic 1)
Which of the following would be the MOST effective way to present quarterly reports to the board on the status of the information security program?

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

Answer: C

Explanation:
An information security dashboard is the most effective way to present quarterly reports to the board on the status of the information security program, because it provides a concise, visual, and high-level overview of the key performance indicators (KPIs), metrics, and trends of the information security program. An information security dashboard can help the board to quickly and easily understand the current state, progress, and performance of the information security program, and to identify any gaps, issues, or
areas of improvement. An information security dashboard can also help the board to align the information security program with the organization's business goals and strategies, and to support the decision-making and oversight functions of the board.
A capability and maturity assessment is a way of measuring the effectiveness and efficiency of the information security program, and of identifying the strengths and weaknesses of the program. However, a capability and maturity assessment is not the most effective way to present quarterly reports to the board, because it may not provide a clear and timely picture of the status of the information security program, and it may not reflect the changes and dynamics of the information security environment. A capability and maturity assessment is more suitable for periodic or annual reviews, rather than quarterly reports.
A detailed analysis of security program KPIs is a way of evaluating the performance and progress of the information security program, and of determining the extent to which the program meets the predefined objectives and targets. However, a detailed analysis of security program KPIs is not the most effective way to present quarterly reports to the board, because it may be too technical, complex, or lengthy for the board to comprehend and appreciate. A detailed analysis of security program KPIs is more suitable for operational or tactical level reporting, rather than strategic level reporting.
An information security risk register is a tool for recording and tracking the information security risks that affect the organization, and for documenting the risk assessment, treatment, and monitoring activities. However, an information security risk register is not the most effective way to present quarterly reports to the board, because it may not provide a comprehensive and balanced view of the information security program, and it may not highlight the achievements and benefits of the program. An information security risk register is more suitable for risk management or audit purposes, rather than performance reporting. References =
? ISACA, CISM Review Manual, 16th Edition, 2020, pages 47-48, 59-60, 63-64, 67-68.
? ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1019.
An information security dashboard is an effective way to present quarterly reports to the board on the status of the information security program. It allows the board to quickly view key metrics and trends at a glance and to drill down into more detailed information as needed. The dashboard should include metrics such as total incidents, patching compliance, vulnerability scanning results, and more. It should also include high-level overviews of the security program and its components, such as the security policy, security architecture, and security controls.

NEW QUESTION 85
- (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 90
- (Topic 1)
Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

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

Answer: A

Explanation:
When a new information security manager is developing an information security strategy for a non-regulated organization, reviewing the management's business goals and objectives would be the most helpful. This is because the information security strategy should be aligned with and support the organization's vision, mission, values, and strategic direction. The information security strategy should also enable the organization to achieve its desired outcomes, such as increasing revenue, reducing costs, enhancing customer satisfaction, or improving operational efficiency. By reviewing the management's business goals and objectives, the information security manager can understand the business context, needs, and expectations of the organization, and design the information security strategy accordingly. The information security manager can also communicate the value proposition and benefits of the information security strategy to the management and other stakeholders, and gain their support and commitment.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Strategy, page 211; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 48, page 452.

NEW QUESTION 92
- (Topic 1)
Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

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

Answer: B

NEW QUESTION 97
- (Topic 1)
Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA
B. To increase awareness of information security among key stakeholders
C. To ensure the stakeholders providing input own the related risk
D. To obtain input from as many relevant stakeholders as possible

Answer: D

Explanation:
The most important reason to conduct interviews as part of the business impact analysis (BIA) process is to obtain input from as many relevant stakeholders as possible. A BIA is a process of identifying and analyzing the potential effects of disruptive events on the organization's critical business functions, processes, and resources. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's continuity planning. Interviews are one of the methods to collect data and information for the BIA, and they involve direct and interactive communication with the stakeholders who are involved in or affected by the business functions, processes, and resources. By conducting interviews, the information security manager can obtain input from as many relevant stakeholders as possible, such as business owners, managers, users, customers, suppliers, regulators, and partners. This can help to ensure that the BIA covers the full scope and complexity of the organization's business activities, and that the BIA reflects the accurate, current, and comprehensive views and expectations of the stakeholders. Interviews can also help to validate, clarify, and supplement the data and information obtained from other sources, such as surveys, questionnaires, documents, or systems. Interviews can also help to build rapport, trust, and collaboration among the stakeholders, and to increase their awareness, involvement, and commitment to the information security and continuity planning.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Impact Analysis (BIA), pages 178-1801; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 65, page 602.

NEW QUESTION 101
- (Topic 1)
Which of the following is an information security manager's MOST important course of action when responding to a major security incident that could disrupt the business?

A. Follow the escalation process.
B. Identify the indicators of compromise.
C. Notify law enforcement.
D. Contact forensic investigators.

Answer: A

Explanation:
When responding to a major security incident that could disrupt the business, the information security manager's most important course of action is to follow the escalation process. The escalation process is a predefined set of steps and procedures that define who should be notified, when, how, and with what information in the event of a security incident. The escalation process helps to ensure that the appropriate stakeholders, such as senior management, business units, legal counsel, public relations, and external parties, are informed and involved in the incident response process. The escalation process also helps to coordinate the actions and decisions of the incident response team and the business continuity team, and to align the incident response objectives with the business priorities and goals. The escalation process should be documented and communicated as part of the incident response plan, and should be reviewed and updated regularly to reflect the changes in the organization's structure, roles, and responsibilities. References =
? CISM Review Manual 15th Edition, page 1631
? CISM 2020: Incident Management and Response, video 32
? Incident Response Models3

NEW QUESTION 106
- (Topic 1)
Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?

A. Parallel test
B. Full interruption test
C. Simulation test
D. Tabletop test

Answer: A

Explanation:
A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required. A parallel test involves processing the same transactions or data at both the primary and the alternate site simultaneously, and comparing the results for accuracy and consistency. A parallel test can validate the functionality, performance, and reliability of the alternate site without disrupting the normal operations at the primary site. A parallel test can also identify and resolve any issues or discrepancies between the two sites before a real disaster occurs. A parallel test can provide a high level of assurance and confidence that the alternate site can support the organization's continuity requirements.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP) Testing, page 1861; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 56, page 522.
A parallel test is the best method to evaluate the effectiveness of an alternate processing site when continuous uptime is required because it involves processing data at both the primary and alternate sites simultaneously without disrupting the normal operations1. A full interruption test would cause downtime and potential loss of data or revenue2. A simulation test would not provide a realistic assessment of the alternate site's capabilities3. A tabletop test would only involve a discussion of the procedures and scenarios without actually testing the site4.
1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM - ISACA Certified Information Security Manager Exam Prep - NICCS 3: Prepare for the ISACA Certified Information Security Manager Exam: CISM … 4: CISM: Certified Information Systems Manager | Official ISACA … - NICCS

NEW QUESTION 107
- (Topic 1)
Which of the following is MOST critical when creating an incident response plan?

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

Answer: C

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

NEW QUESTION 109
- (Topic 3)
Which of the following BEST demonstrates that an anti-phishing campaign is effective?

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

Answer: D

Explanation:
The ultimate goal of an anti-phishing campaign is to reduce the risk and impact of phishing attacks on the organization. Therefore, the most relevant and reliable indicator of the effectiveness of an anti-phishing campaign is the decreased number of incidents that have occurred as a result of phishing. This metric shows how well the employees have learned to recognize and report phishing emails, and how well the security controls have prevented or mitigated the damage caused by phishing.
References = Five Ways to Achieve a Successful Anti-Phishing Campaign; Don't click: towards an effective anti-phishing training. A comparative literature review; CISA, NSA, FBI, MS-ISAC Publish Guide on Preventing Phishing Intrusions

NEW QUESTION 111
- (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 116
- (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 120
- (Topic 3)
Which of the following should include contact information for representatives of equipment and software vendors?

A. Information security program charter
B. Business impact analysis (BIA)
C. Service level agreements (SLAs)
D. Business continuity plan (BCP)

Answer: D

Explanation:
The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. References: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/business-continuity- management-lifecycle https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

NEW QUESTION 123
- (Topic 3)
Which of the following is the MOST effective way to ensure the security of services and solutions delivered by third-party vendors?

A. Integrate risk management into the vendor management process.
B. Conduct security reviews on the services and solutions delivered.
C. Review third-party contracts as part of the vendor management process.
D. Perform an audit on vendors' security controls and practices.

Answer: A

Explanation:
Integrating risk management into the vendor management process is the most effective way to ensure the security of services and solutions delivered by third-party vendors, as it enables the organization to identify, assess, treat, and monitor the risks associated with outsourcing. Risk management should be applied throughout the vendor life cycle, from selection, contracting, onboarding, monitoring, to termination. Risk management also helps the organization to define the security requirements, expectations, and responsibilities for the vendors, and to evaluate their performance and compliance. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2; Preparing Your First Supplier Audit Plan1.

NEW QUESTION 125
- (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 128
- (Topic 3)
Which of the following would BEST enable a new information security manager to obtain senior management support for an information security governance program?

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

Answer: A

Explanation:
The best way to obtain senior management support for an information security governance program is to demonstrate the program's value to the organization, such as how it can help achieve business objectives, reduce operational risks, enhance resilience, and comply with regulations. Demonstrating the value of information security governance can help senior management understand the benefits and costs of the program, and motivate them to participate in the decision-making process. The other options, such as discussing governance programs in similar organizations, providing external audit results, or providing examples of incidents, may not be sufficient or persuasive enough to obtain senior management support, as they may not reflect the specific needs and goals of the organization. References:
? https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process
? https://www.sans.org/white-papers/992/
? https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-get-management-support-for-your-security-program.html

NEW QUESTION 129
- (Topic 3)
Which of the following should be the FIRST step when performing triage of a malware incident?

A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware

Answer: A

Explanation:
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION 134
- (Topic 3)
Which of the following is the MOST effective way to identify changes in an information security environment?

A. Business impact analysis (BIA)
B. Annual risk assessments
C. Regular penetration testing
D. Continuous monitoring

Answer: D

Explanation:
Continuous monitoring is the most effective way to identify changes in an information security environment, as it provides ongoing awareness of the security status, vulnerabilities, and threats that may affect the organization's information assets and risk posture. Continuous monitoring also helps to evaluate the performance and effectiveness of the security controls and processes, and to detect and respond to any deviations or incidents in a timely manner. (From CISM Review Manual 15th Edition and NIST Special Publication 800-1371)
References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; NIST Special Publication 800-1371, page 1, section 1.1.

NEW QUESTION 136
- (Topic 3)
Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?

A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.
D. Provide security awareness training to board executives.

Answer: A

Explanation:
The best way to help ensure alignment of the information security program with organizational objectives is A. Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security

program is aligned with the organizational objectives by:
Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators
Allocating and prioritizing the resources and budget for information security initiatives and projects
Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security
An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources)
References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

NEW QUESTION 140
- (Topic 3)
Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?

A. Alignment with industry benchmarks
B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget

Answer: B

Explanation:
The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

NEW QUESTION 144
- (Topic 3)
Which of the following is a viable containment strategy for a distributed denial of service (DDoS) attack?

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

Answer: B

Explanation:
Redirecting the attacker’s traffic is a viable containment strategy for a distributed denial of service (DDoS) attack because it helps to divert the malicious traffic away from the target server and reduce the impact of the attack. A DDoS attack is an attempt by attackers to overwhelm a server or a network with a large volume of requests or packets, preventing legitimate users from accessing the service or resource. Redirecting the attacker’s traffic is a technique that involves changing the DNS settings or routing tables to send the attacker’s traffic to another destination, such as a sinkhole, a honeypot, or a scrubbing center. A sinkhole is a server that absorbs and discards the malicious traffic. A honeypot is a decoy server that mimics the target server and collects information about the attacker’s behavior and techniques. A scrubbing center is a service that filters out the malicious traffic and forwards only the legitimate traffic to the target server. Redirecting the attacker’s traffic helps to contain the DDoS attack by reducing the load on the target server and preserving its availability and performance. Therefore, redirecting the attacker’s traffic is the correct answer.
References:
? https://www.fortinet.com/resources/cyberglossary/implement-ddos-mitigation- strategy
? https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-response-strategy
? https://www.cloudflare.com/learning/ddos/glossary/sinkholing/.

NEW QUESTION 149
- (Topic 3)
An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?

A. Implementing automated vulnerability scanning in the help desk workflow
B. Changing the default setting for all security incidents to the highest priority
C. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system
D. Integrating incident response workflow into the help desk ticketing system

Answer: D

Explanation:
The best automated control to resolve the issue of security incidents not being appropriately escalated by the help desk is to integrate incident response workflow into the help desk ticketing system. This will ensure that the help desk staff follow the predefined steps and procedures for handling and escalating security incidents, based on the severity, impact, and urgency of each incident. The incident response workflow will also provide clear guidance on who to notify, when to notify, and how to notify the relevant stakeholders and authorities. This will improve the efficiency, effectiveness, and consistency of the incident response process.
References = CISM Review Manual, 16th Edition, page 2901; A Practical Approach to Incident Management Escalation2

NEW QUESTION 152
- (Topic 3)
Which of the following is MOST appropriate to communicate to senior management regarding information risk?

A. Emerging security technologies

B. Risk profile changes
C. Defined risk appetite
D. Vulnerability scanning progress

Answer: B

Explanation:
Risk profile changes are the most appropriate to communicate to senior management regarding information risk because they reflect the current level and nature of the risks that the organization faces and how they may affect its objectives and performance. Senior management needs to be aware of any changes in the risk profile so that they can make informed decisions and allocate resources accordingly. Risk profile changes also help senior management monitor the effectiveness of the risk management process and identify any gaps or weaknesses that need to be addressed.
References = Communicating Information Security Risk Simply and Effectively, Part 1, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NEW QUESTION 154
- (Topic 3)
Which of the following is MOST important to include in an information security status report management?

A. List of recent security events
B. Key risk indication (KRIs)
C. Review of information security policies
D. information security budget requests

Answer: B

Explanation:
Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-information-security-using-iso-27004

NEW QUESTION 159
- (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 163
- (Topic 3)
An email digital signature will:

A. protect the confidentiality of an email message.
B. verify to recipient the integrity of an email message.
C. automatically correct unauthorized modification of an email message.
D. prevent unauthorized modification of an email message.

Answer: B

Explanation:
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References: https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com/searchsecurity/definition/digital-signature

NEW QUESTION 167
- (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 170
- (Topic 2)
To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls

Answer: B

Explanation:
To support effective risk decision making, it is most important to have risk reporting procedures in place. Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid-level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION 174
- (Topic 2)
Which of the following presents the GREATEST challenge to the recovery of critical systems and data following a ransomware incident?

A. Lack of encryption for backup data in transit
B. Undefined or undocumented backup retention policies
C. Ineffective alert configurations for backup operations
D. Unavailable or corrupt data backups

Answer: D

Explanation:
A ransomware incident is a type of cyberattack that encrypts the victim's data and demands a ransom for its decryption. Ransomware can cause significant disruption and damage to critical systems and data, as well as financial losses and reputational harm. To recover from a ransomware incident, the organization needs to have reliable and accessible backups of its data, preferably in an encrypted format. However, if the backups are unavailable or corrupt, the organization will face a major challenge in restoring its data and operations. Therefore, option D is the most challenging factor for the recovery of critical systems and data following a ransomware incident. References = CISA MS-ISAC Ransomware Guide1, page 9; How to Write an Incident Response Plan for Ransomware Recovery2.

NEW QUESTION 179
- (Topic 2)
Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

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

D. Incident response and recovery plans are documented in simple language

Answer: B

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

NEW QUESTION 181
- (Topic 2)
The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.

Answer: D

Explanation:
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident. Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.
Re-evaluating the impact of incidents is not the primary objective of performing a post- incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re-evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.
Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal. Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal. References =
? ISACA CISM: PRIMARY goal of a post-incident review should be to?
? CISM Exam Overview - Vinsys
? CISM Review Manual, Chapter 4, page 176
? CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

NEW QUESTION 183
- (Topic 2)
Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.
B. Internal compliance requirements are being met.
C. Risk management objectives are being met.
D. Business needs are being met.

Answer: D

Explanation:
The primary purpose of business continuity and disaster recovery plans is to ensure that the organization can resume its critical business functions within the stated recovery time objectives (RTOs) after a disruptive event. RTOs are based on the business needs and the impact analysis of each function or process. Therefore, meeting the business needs is the best indicator that the plans are effective. Regulatory requirements, internal compliance requirements, and risk management objectives are important factors that influence the development and testing of the plans, but they are not the ultimate measure of their effectiveness. References = CISM Certified Information Security Manager Study Guide, Chapter 9: Business Continuity and Disaster Recovery, page 3071; CISM Foundations: Module 4 Course, Part Two: Business Continuity and Disaster Recovery Plans2; Imperva, Business Continuity & Disaster Recovery Planning (BCP & DRP)3

NEW QUESTION 186
- (Topic 2)
Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site

Answer: C

Explanation:
= The organizational tolerance to service interruption is the most important consideration when defining a recovery strategy in a business continuity plan (BCP), as it reflects the degree of risk that the organization is willing to accept in the event of a disaster. The organizational tolerance to service interruption determines the acceptable level of downtime, data loss, or disruption that the organization can tolerate, and thus guides the selection of recovery objectives, strategies, and resources. Legal and regulatory requirements are external factors that influence the recovery strategy, but are not the primary consideration. Likelihood of a disaster is a factor that affects the recovery strategy, but is not the most important one. Geographical location of the backup site is a factor that affects the recovery strategy, but is not as critical as organizational tolerance to service interruption. References = CISM Review Manual, 16th Edition, page 1731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 792

Learn more: 1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION 187
- (Topic 2)
Which of the following is the MOST effective way to prevent information security incidents?

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

Answer: B

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

NEW QUESTION 191
- (Topic 2)
A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:

A. developing a security program that meets global and regional requirements.
B. ensuring effective communication with local regulatory bodies.
C. using industry best practice to meet local legal regulatory requirements.
D. monitoring compliance with defined security policies and standards.

Answer: A

Explanation:
= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. References = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

NEW QUESTION 195
.....

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