Certified Information Security Manager
CISM

1

A PRIMARY purpose of creating security policies is to:

A. define allowable security boundaries.

B. communicate management's security expectations.

C. establish the way security tasks should be executed.

D. implement management's security governance strategy.

Answer: D Explanation

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

References =

CISM Review Manual 15th Edition, page 1631 CISM

2020: IT Security Policies2

CISM domain 1: Information security governance [Updated 2022]3 What is CISM? - Digital Guardian4

2

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

A. The business client

B. The information security tear

C. The identity and access management team

D. Business unit management

Answer: D Explanation

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

The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that

processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-
138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

3

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.

4

The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

A. enhance the organization's antivirus controls.

B. eliminate the risk of data loss.

C. complement the organization's detective controls.

D. reduce the need for a security awareness program.

Answer: C Explanation

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

5
In which cloud model does the cloud service buyer assume the MOST security responsibility ?
A. Disaster Recovery as a Service (DRaaS)
B. Infrastructure as a Service (laaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)
Answer: B Explanation
Infrastructure as a Service (IaaS) is a cloud model in which the cloud service provider (CSP) offers the basic computing resources, such as servers, storage, network, and virtualization, as a service over the internet. The cloud service buyer (CSB) is responsible for installing, configuring, managing, and securing the operating systems, applications, data, and middleware on top of the infrastructure. Therefore, the CSB assumes the most security responsibility in the IaaS model, as it has to protect the confidentiality, integrity, and availability of its own assets and information in the cloud environment. In contrast, in the other cloud models, the CSP takes over more security responsibility from the CSB, as it provides more layers of the service stack. In Disaster Recovery as a Service (DRaaS), the CSP offers the replication and recovery of the CSB's data and applications in the event of a disaster. In Platform as a Service (PaaS), the CSP offers the development and deployment tools, such as programming languages, frameworks, libraries, and databases, as a service. In Software as a Service (SaaS), the CSP offers the complete software applications, such as email, CRM, or ERP, as a service. In these models, the CSB has less control and visibility over the underlying infrastructure, platform, or software, and has to rely on the CSP's security measures and contractual agreements.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, page
140-1411

6
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.

7
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.

8

An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?

A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.

Answer: B Explanation
The information security manager should present a business case for additional controls to senior management, as this is the most effective way to communicate the risk and the need for mitigation. The information security manager should not instruct IT to deploy controls based on urgent business needs, as this may not align with the business objectives and may cause unnecessary costs and delays. The information security manager should not solicit bids for compensating control products, as this may not address the root cause of the risk and may not be the best solution. The information security manager should not recommend a different application, as this may not be feasible or desirable for the business. References = CISM Review Manual 2023, page 711; CISM Review Questions, Answers & Explanations Manual 2023, page 252

9

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

10

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

A. Risk levels may be elevated beyond acceptable limits.

B. Security audits may report more high-risk findings.

C. The compensating controls may not be cost efficient.

D. Noncompliance with industry best practices may result.

Answer: A Explanation

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

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

11

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

A. Business impact analysis (BIA)

B. Business process analysis

C. SWOT analysis

D. Cast-benefit analysis

Answer: A Explanation

A business impact analysis (BIA) is the process of identifying and evaluating the potential

effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization in the event of a disaster or crisis. A BIA also helps to identify the worst-case disruption scenarios, which are the scenarios that would cause the most severe impact to the organization in terms of financial, operational, reputational, or legal consequences. By conducting a BIA, the organization can assess the likelihood and impact of various disruption scenarios, and plan accordingly to mitigate the risks and ensure business continuity and resilience. References = CISM Review Manual 15th Edition, page 181, page 183.

12

An organization recently outsourced the development of a mission-critical business application. Which of the following would be the BEST way to test for the existence of backdoors?

A. Scan the entire application using a vulnerability scanning tool.

B. Run the application from a high-privileged account on a test system.

C. Perform security code reviews on the entire application.

D. Monitor Internet traffic for sensitive information leakage.

Answer: C Explanation

The best way to test for the existence of backdoors in a mission-critical business application that was outsourced to a third-party developer is to perform security code reviews on the entire application. A backdoor is a hidden or undocumented feature or function in a software application that allows unauthorized or remote access, control, or manipulation of the application or the system it runs on. Backdoors can be intentionally or unintentionally introduced by the developers, or maliciously inserted by the attackers, and they can pose serious security risks and threats to the organization and its data. Security code reviews are the process of examining and analyzing the source code of a software application to identify and eliminate any security vulnerabilities, flaws, or weaknesses, such as backdoors, that may compromise the functionality, performance, or integrity of the application or the system.

Security code reviews can be performed manually by the security experts, or automatically by the security tools, or both, and they can be done at different stages of the software development life cycle, such as design, coding, testing, or deployment. Security code reviews can help to detect and remove any backdoors in the application before they can be exploited by the attackers, and they can also help to improve the quality, reliability, and security of the application.

References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 87, page 812; CISM ITEM DEVELOPMENT GUIDE, page 63.

13

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

14

Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.

B. The contact list is regularly updated.

C. Minimum regulatory requirements are maintained.

D. Senior management approval has been documented.

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

15

Which of the following is the PRIMARY role of an information security manager in a software development project?

A. To enhance awareness for secure software design

B. To assess and approve the security application architecture

C. To identify noncompliance in the early design stage
D. To identify software security weaknesses
Answer: B Explanation
The primary role of an information security manager in a software development project is to assess and approve the security application architecture. The security application architecture is the design and structure of the software application that defines how the application components interact with each other and with external systems, and how the application implements the security requirements, principles, and best practices.
The information security manager is responsible for ensuring that the security application architecture is aligned with the organization's information security policies, standards, and guidelines, and that it meets the business objectives, functional specifications, and user expectations. The information security manager is also responsible for reviewing and evaluating the security application architecture for its completeness, correctness, consistency, and compliance, and for identifying and resolving any security issues, risks, or gaps. The information security manager is also responsible for approving the security application architecture before the software development project proceeds to the next phase, such as coding, testing, or deployment.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 80, page 742.

16
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.
Answer: D Explanation
= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =

1: CISM Review Manual 15th Edition, page 199-2004 2:
CISM Practice Quiz, question 1011
3: Computer Security Incident Handling Guide5, page 2-3

17
Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?
A. Establish key risk indicators (KRIs).
B. Use quantitative risk assessment methods.