Product Questions: 793
Version: 43.0

Topic 1, Exam Pool A

Question: 1

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

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

Answer: C

Explanation:

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

Question: 2

During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

A. Post-incident review
B. Eradication
C. Containment
D. Identification

Answer: B

Explanation:

The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2. The other phases of incident response are:
Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.
Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.
Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1. Reference = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2: What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

Question: 3

Which of the following is PRIMARILY determined by asset classification?

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

Answer: B

Explanation:

Asset classification is the process of assigning a value to information assets based on their importance to the organization and the potential impact of their compromise, loss or damage1. Asset classification helps to determine the level of protection required for assets, which is proportional to their value and sensitivity2. Asset classification also facilitates risk assessment and management, as well as compliance with legal, regulatory and contractual requirements3. Asset classification does not primarily determine the insurance coverage, priority for replacement, or replacement cost of assets, as these factors depend on other criteria such as risk appetite, business impact, availability and market value4. Reference = 1: CISM - Information Asset Classification Flashcards | Quizlet 2: CISM Exam Content Outline | CISM Certification | ISACA 3: CIS Control 1: Inventory and Control of Enterprise Assets 4: CISSP versus the CISM Certification | ISC2

Question: 4

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

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

Answer: D

Explanation:

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

Question: 5

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

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

Answer: B

Explanation:

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

Question: 6

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems

Answer: A

Explanation:

The best way to support the incident management process for attacks on an organization's supply chain is to establish communication paths with vendors. This means that the organization and its vendors have clear and agreed-upon channels, methods, and protocols for exchanging information and coordinating actions in the event of an incident that affects the supply chain. Communication paths with vendors can help to identify the source, scope, and impact of the incident, as well as to share best practices, lessons learned, and recovery strategies. Communication paths with vendors can also facilitate the escalation and resolution of the incident, as well as the reporting and documentation of the incident. Communication paths with vendors are part of the incident response plan (IRP), which is a component of the information security program (ISP) 12345.
The other options are not the best ways to support the incident management process for attacks on the organization's supply chain. Including service level agreements (SLAs) in vendor contracts can help to define the expectations and obligations of the parties involved in the supply chain, as well as the penalties for non-compliance. However, SLAs do not necessarily address the specific procedures and requirements for incident management, nor do they ensure effective communication and collaboration among the parties. Requiring security awareness training for vendor staff can help to reduce the likelihood and severity of incidents by enhancing the knowledge and skills of the vendor personnel who handle the organization's data and systems. However, security awareness training does not guarantee that the vendor staff will follow the appropriate incident management processes, nor does it address the communication and coordination issues that may arise during an incident. Performing integration testing with vendor systems can help to ensure the compatibility and functionality of the systems that are part of the supply chain, as well as to identify and mitigate any vulnerabilities or errors that could lead to incidents. However, integration testing does not cover all the possible scenarios and risks that could affect the supply chain, nor does it provide the necessary communication and response mechanisms for incident management. Reference = 1, 2, 3, 4, 5
https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident-management-part-1 https://niccs.cisa.gov/education-training/catalog/skillsoft/cism-information-security-incident-management-part-1

Question: 7

Which of the following BEST ensures information security governance is aligned with corporate governance?

A. A security steering committee including IT representation
B. A consistent risk management approach
C. An information security risk register
D. Integration of security reporting into corporate reporting

Answer: D

Explanation:

The best way to ensure information security governance is aligned with corporate governance is to integrate security reporting into corporate reporting. This will enable the board and senior management to oversee and monitor the performance and effectiveness of the information security program, as well as the alignment of information security objectives and strategies with business goals and risk appetite. Security reporting should provide relevant, timely, accurate, and actionable information to support decision making and accountability. The other options are important components of information security governance, but they do not ensure alignment with corporate governance by themselves. Reference = CISM Review Manual 15th Edition, page 411; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1027

Question: 8

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

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

Answer: A

Explanation:

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

Question: 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. Reference = 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

Question: 10

Which of the following should be the MOST important consideration when establishing information security policies for an organization?

A. Job descriptions include requirements to read security policies.
B. The policies are updated annually.
C. Senior management supports the policies.
D. The policies are aligned to industry best practices.

Answer: C

Explanation:

The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization’s leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization’s goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.

Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing information security policies. The policies should be relevant and applicable to the employees’ roles and functions, and should be reinforced by regular training and awareness programs.

The policies should be updated periodically to reflect the changes in the organization’s environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.

The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization’s specific context, needs, and expectations, and should be consistent with the organization’s vision, mission, and values. Reference =

ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.

ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1009.

Question: 11

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

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

Answer: D

Explanation:

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

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

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

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

Reference =

CISM Review Manual 15th Edition, pages 1-301

CISM Exam Content Outline2

Risk Assessment for Technical Vulnerabilities3

A Step-By-Step Guide to Vulnerability Assessment4

Question: 12

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. Reference = CISM Review Manual 15th Edition, page

1731; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1029

Question: 13

When properly implemented, secure transmission protocols protect transactions:

A. from eavesdropping.
B. from denial of service (DoS) attacks.
C. on the client desktop.
D. in the server's database.

Answer: A

Explanation:

Secure transmission protocols are network protocols that ensure the integrity and security of data transmitted across network connections. The specific network security protocol used depends on the type of protected data and network connection. Each protocol defines the techniques and procedures required to protect the network data from unauthorized or malicious attempts to read or exfiltrate information1. One of the most common threats to network data is eavesdropping, which is the interception and analysis of network traffic by an unauthorized third party. Eavesdropping can compromise the confidentiality, integrity, and availability of network data, and can lead to data breaches, identity theft, fraud, espionage, and sabotage2. Therefore, secure transmission protocols protect transactions from eavesdropping by using encryption, authentication, and integrity mechanisms to prevent unauthorized access and modification of network data. Encryption is the process of transforming data into an unreadable format using a secret key, so that only authorized parties can decrypt and access the data. Authentication is the process of verifying the identity and legitimacy of the parties involved in a network communication, using methods such as passwords, certificates, tokens, or biometrics. Integrity is the process of ensuring that the data has not been altered or corrupted during transmission, using methods such as checksums, hashes, or digital signatures3. Some examples of secure transmission protocols are:
Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used protocols for securing web, email, and other application layer communications over the Internet. SSL and TLS use symmetric encryption, asymmetric encryption, and digital certificates to establish secure sessions between clients and servers, and to encrypt and authenticate the data exchanged.
Internet Protocol Security (IPsec), which is a protocol and algorithm suite that secures data transferred over public networks like the Internet. IPsec operates at the network layer and provides end-to-end security for IP packets. IPsec uses two main protocols: Authentication Header (AH), which provides data integrity and authentication, and Encapsulating Security Payload (ESP), which provides data confidentiality, integrity, and authentication. IPsec also uses two modes: transport mode, which protects the payload of IP packets, and tunnel mode, which protects the entire IP packet.
Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over insecure networks. SSH uses encryption, authentication, and integrity to protect the data transmitted between a client and a server. SSH also supports port forwarding, which allows secure tunneling of other network services through SSH connections.
Reference = 1: 6 Network Security Protocols You Should Know | Cato Networks 2: Eavesdropping Attacks - an overview | ScienceDirect Topics 3: Network Security Protocols - an overview | ScienceDirect Topics : SSL/TLS (Secure Sockets Layer/Transport Layer Security) - Definition : IPsec -