ExamEnroll
EXAM SUCCESS SIMPLIFIED

Isaca

CISM

Certified Information Security Manager

Exam Version: 60.1

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Thank you for Downloading CISM exam PDF Demo

You can also try our CISM practice exam software

Visit link below:

https://examsenroll.com/exam/cism

Question 1. (Single Select)

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. (Single Select)

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 3. (Single Select)

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. Reference = 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 4. (Single Select)

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 5. (Single Select)

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.

For More Information - Visit link below:

https://examsenroll.com/exam/cism

Thanks for using our Product!

Pass Your Certification With ExamsEnroll Guarantee

For $20 discount, use coupon code:

MINUS20

Sales: sales@examsenroll.com

Support: support@examsenroll.com