ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Eccouncil

Code: 712-50

Exam: EC-Council Certified CISO (CCISO)

https://www.examsnest.com/exam/712-50/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 10.1

Topic 1, Governance (Policy, Legal & Compliance)

Question: 1

Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information

B. Bodily Information

C. Territorial Information

D. Communications Information

Answer: A

Explanation:

Definition of Confidential/Protected Information: Confidential or protected information encompasses any data that must be safeguarded from unauthorized access or disclosure to ensure its confidentiality, integrity, and availability. This category includes sensitive personal, financial, medical, and proprietary information.

Examples of Confidential/Protected Information:

Credit Card Information: Financial data that requires compliance with PCI-DSS standards for secure handling and processing.

Medical Data: Protected under regulations such as HIPAA in the U.S., ensuring privacy and security of patient health information.

Government Records: Often classified or protected under laws and regulations to maintain national security and ensure the privacy of sensitive governmental operations.

Key Reference:

The EC-Council Certified CISO (CCISO) framework specifically identifies the handling and protection of such data as a core responsibility under the domain of Information Security Management.

Per EC-Council CCISO material, such data forms the backbone of risk assessment and compliance mandates in most regulatory frameworks.

Connection to Cybersecurity Best Practices: As per the CCISO guidelines, proper classification and protection of this type of information are paramount. This involves:

Establishing security policies.

Implementing technical controls such as encryption and access control.

Training employees to recognize and handle sensitive data appropriately.

Question: 2

The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope

B. Getting authority to operate the system from executive management

C. Changing the default passwords

D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

Explanation:

Understanding the Authorization Process
The system authorization process is a structured methodology ensuring that a system operates securely within an acceptable risk framework. According to EC-Council Certified CISO standards, this process follows a lifecycle approach which culminates in obtaining formal approval from senior management.

Steps in the Authorization Process
a. Risk Assessment: Evaluate threats, vulnerabilities, and potential impacts.
b. Implementation of Security Controls: Deploy safeguards to mitigate identified risks.
c. Testing and Validation: Conduct tests such as vulnerability assessments to ensure controls are functioning correctly.
d. Documentation: Record compliance with security controls and assessments.
e. Final System Review: This includes activities like scanning the system and ensuring all identified high and medium vulnerabilities are addressed.

Final Step: Authority to Operate

After the above steps are completed, the system owner or project leader submits the authorization package to executive management. The final decision lies with senior-level stakeholders who evaluate if the system meets all organizational security requirements and residual risk is acceptable. Upon approval, they provide formal authorization to operate (ATO).

Why Option B is Correct

This aligns with EC-Council's emphasis on governance and senior management oversight in risk management frameworks. The ultimate authority for the operation of any system lies with the top executives who are accountable for the organization's security posture.

Reference

This procedure is documented in various EC-Council CISO materials, ensuring it is consistent with best practices for managing organizational cybersecurity frameworks.

Question: 3

The single most important consideration to make when developing your security program, policies, and processes is:

A. Budgeting for unforeseen data compromises

B. Streamlining for efficiency

C. Alignment with the business

D. Establishing your authority as the Security Executive

Answer: C

Explanation:

Importance of Alignment with Business Objectives:

According to the EC-Council CCISO framework, aligning the security program with business objectives ensures that security measures support the organization's strategic goals.

This alignment is critical to gaining executive buy-in and justifying the investment in security measures.

Business-Driven Security Approach:

The CCISO program emphasizes that a security strategy disconnected from business goals can lead to inefficiencies, reduced support from leadership, and inadequate protection.

Security should not be a standalone function but integrated into business processes to maximize its

effectiveness.

Supporting Reference:

EC-Council training material highlights alignment with business objectives as the cornerstone of governance, risk management, and compliance (GRC) practices. This approach ensures that security enhances business resilience while minimizing risk.

Question: 4

An organization's Information Security Policy is of MOST importance because

A. it communicates management's commitment to protecting information resources

B. it is formally acknowledged by all employees and vendors

C. it defines a process to meet compliance requirements

D. it establishes a framework to protect confidential information

Answer: A

Explanation:

Purpose of an Information Security Policy:

The policy serves as a foundational document that articulates the organization's commitment to safeguarding its information assets.

It demonstrates management's intent and direction toward implementing robust security measures.

Management Commitment:

As per EC-Council CCISO, management's visible commitment to security is essential for creating a culture of compliance and accountability across the organization.

Policies provide a basis for decision-making, risk management, and incident response.

Supporting Reference:

The CCISO program outlines that a well-documented and communicated information security policy ensures clarity in roles and responsibilities, fostering alignment among all stakeholders, including employees and vendors.

Question: 5

Developing effective security controls is a balance between:

A. Risk Management and Operations

B. Corporate Culture and Job Expectations

C. Operations and Regulations

D. Technology and Vendor Management

Answer: A

Explanation:

Balancing Risk and Operations:

Effective security controls must mitigate risks without hindering operational efficiency. This balance is a recurring theme in the EC-Council CCISO material, which emphasizes integrating security into business workflows.

Overly restrictive controls can impede productivity, while overly lenient controls may expose the organization to unacceptable risks.

Principles of Risk Management:

Identify, evaluate, and prioritize risks while considering operational realities. The controls must be practical and aligned with the organization's risk appetite.

Supporting Reference:

The CCISO framework highlights that security leaders should aim to develop controls that enable business operations while providing adequate safeguards against threats. This ensures that security becomes an enabler, not a hindrance, to business goals.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Eccouncil

Code: 712-50

Exam: EC-Council Certified CISO (CCISO)

https://www.examsnest.com/exam/712-50/

Use Coupon “**SAVE15**” for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation