KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **712-50**

Title : EC-Council Certified CISO (CCISO)

Version : DEMO

1.An auditor is reviewing the security classifications for a group of assets and finds that many of the assets are not correctly classified.
What should the auditor's NEXT step be?
A. Immediately notify the board of directors of the organization as to the finding
B. Correct the classifications immediately based on the auditor's knowledge of the proper classification
C. Document the missing classifications
D. Identify the owner of the asset and induce the owner to apply a proper classification
Answer: D
Explanation:
Proper Asset Classification Responsibility:
Asset classification is the responsibility of the asset owner, as they have the best understanding of the asset's value and sensitivity.
The auditor's role is to identify gaps and guide the process, not to directly reclassify assets.
Why Not Other Options:
A: Immediate board notification is premature without thorough documentation and recommendations.
B: The auditor does not have the authority or detailed knowledge to classify assets.
C: Documenting the issue is part of the process but does not resolve the problem.
References:
EC-Council CISO Material: Asset Management and Classification Best Practices.

2.What cloud computing environment allows access and use by several organizations for information sharing?
A. Community cloud
B. Public cloud
C. Private cloud
D. Hybrid cloud
Answer: A
Explanation:
Comprehensive and Detailed Explanation (250–350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:
The EC-Council CCISO Body of Knowledge, aligned with NIST cloud definitions, identifies a community cloud as the cloud deployment model designed to be shared by several organizations with common interests, mission requirements, or compliance needs.
CCISO documentation explains that community clouds are commonly used by organizations within the same industry, regulatory environment, or operational mission—such as government agencies, healthcare providers, or financial institutions. These environments allow participating organizations to share infrastructure while maintaining mutually agreed security controls, governance structures, and compliance requirements.
A public cloud is available to the general public and does not imply shared governance or restricted membership. A private cloud is dedicated to a single organization, while a hybrid cloud combines two or more cloud types but does not inherently enable multi-organization information sharing under common governance.
CCISO materials emphasize that community clouds strike a balance between cost efficiency and control, making them ideal for collaborative environments requiring shared access with controlled risk.

Thus, community cloud is the correct answer.

3.What does the information security program primarily protect?
A. All organizational assets as identified by the Chief Information Officer
B. Audit schedules, reports, and remediations
C. Critical data, systems, and processes
D. Intellectual property and trademarks used by the business
Answer: C
Explanation:
Comprehensive and Detailed Explanation (250–350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:
The EC-Council CCISO Body of Knowledge defines the primary objective of an information security program as the protection of critical data, systems, and business processes that support organizational objectives.
CCISO guidance emphasizes that information security is a risk-based discipline, meaning not all assets are protected equally. Instead, resources are prioritized toward assets that are essential to mission execution, revenue generation, regulatory compliance, and operational resilience.
While intellectual property, trademarks, and other assets may be included, CCISO materials clarify that these are protected only insofar as they are critical to business operations. Similarly, audit artifacts and CIO-identified assets are not the primary focus of the security program itself.
The CCISO framework highlights the CIA triad—confidentiality, integrity, and availability—as applied to critical information and systems, ensuring continuity and trust in business operations.
Therefore, the correct answer is critical data, systems, and processes.

4.An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO). The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?
A. ISO 22318 Supply Chain Continuity
B. ISO 27031 BCM Readiness
C. ISO 22301 BCM Requirements
D. ISO 22317 BIA
Answer: C
Explanation:
ISO 22301 provides a comprehensive standard for Business Continuity Management (BCM) requirements, covering the complete BCM lifecycle, including planning, implementing, operating, monitoring, and improving BCM systems. While ISO 22318 (A) focuses on supply chain continuity and ISO 27031 (B) addresses ICT readiness, ISO 22301 offers a broader approach. ISO 22317 (D) pertains specifically to Business Impact Analysis (BIA).
Reference: https://www.smartsheet.com/content/iso-22301-business-continuity-guide

5.Involvement of senior management is MOST important in the development of:
A. IT security implementation plans.
B. Standards and guidelines.
C. IT security policies.

D. IT security procedures.

Answer: C

Explanation:

The involvement of senior management is most important in the development of IT security policies because policies set the strategic direction and priorities for the organization. These policies ensure alignment between security measures and business objectives, which require input and approval from senior leadership.

Role of IT Security Policies:

Policies define the organization's security goals, objectives, and responsibilities.

They require senior management's endorsement to ensure they are enforceable and aligned with business priorities.

Significance of Senior Management Involvement:

Provides authority and resources to implement the policies. Ensures buy-in across departments for consistent adherence. Comparison with Other Options:

Implementation Plans, Standards, Guidelines, and Procedures: These are tactical and operational layers derived from the overarching policies.

Governance and Risk Management: Emphasizes that policies reflect the organization’s commitment to security and require executive input.

Strategic Leadership: Senior management’s role in driving security policy development is critical for organizational success.