Eccouncil 712-50 CCISO Practice Questions

Shared by Fry on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Management]

What is the name of a formal statement that defines the strategy, approach, or expectations related to specific concerns within an organization:

Options:

A- Policy
B- standard
C- Procedure
D- Guideline

Answer:

A

Question 2

Question Type: MultipleChoice

As the CISO, you have been tasked with the execution of the company's key management program. You

MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key

control will ensure no single individual can constitute or re-constitute a key?

Options:

A- Dual Control
B- Separation of Duties
C- Split Knowledge
D- Least Privilege

Answer:

C

Explanation:

Split knowledge ensures that no single individual can independently generate or reconstruct an encryption key. This principle divides knowledge of the key among multiple individuals, requiring their collaboration for key generation or usage. While dual control involves multiple individuals acting together, split knowledge specifically ensures that individual actions alone cannot compromise key integrity. Separation of duties and least privilege focus on broader security principles rather than encryption-specific safeguards.

Question 3

Question Type: MultipleChoice

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the ''real workers.''

Which group of people should be consulted when developing your security program?

Options:

A- Peers
B- End Users
C- Executive Management
D- How vulnerabilities can potentially be exploited in systems that impact the organization

Answer:

D

Explanation:

Why Engage All Groups?

Developing an effective security program requires input from multiple stakeholders:

Peers: Help ensure the program aligns with departmental objectives and industry best practices.

End Users: Provide insights into operational challenges and ensure the program is practical without being overly restrictive.

Executive Management: Their support is critical for securing funding, enforcing policies, and

aligning security initiatives with organizational goals.

Corporate Culture Challenges

Overcoming the perception of security as a hindrance requires collaboration and demonstrating how security can enhance productivity and protect the organization's interests.

EC-Council Reference

Emphasizes the importance of involving all stakeholders to ensure buy-in and alignment with organizational objectives.

Question 4

Question Type: MultipleChoice

Which of the following is an accurate description of a balance sheet?

Options:

A- The percentage of earnings that are retained by the organization for reinvestment in the business
B- The details of expenses and revenue over a long period of time
C- A summarized statement of all assets and liabilities at a specific point in time
D- A review of regulations and requirements impacting the business from a financial perspective

Answer:

C

Explanation:

Balance Sheet Overview:

Provides a snapshot of an organization's financial position at a specific point in time.

Includes assets (what the company owns), liabilities (what it owes), and equity (owner's claims).

Purpose:

Used to evaluate financial health and guide strategic decisions.

Key sections:

Assets: Cash, accounts receivable, inventory, etc.

Liabilities: Loans, accounts payable, etc.

Equity: Shareholder investments and retained earnings.

Why Not Other Options:

A: Describes retained earnings, not a balance sheet.

B: Refers to an income statement, not a balance sheet.

D: Describes regulatory compliance, unrelated to financial reporting.

EC-Council CISO Handbook: Financial Management for Security Programs

Question 5

Question Type: MultipleChoice

As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.

Which is the BEST type of risk that defines this event?

Options:

A- Compliance Risk
B- Reputation Risk
C- Operational Risk
D- Strategic Risk

Answer:

B

Explanation:

Reputation Risk Defined:

Reputation risk refers to potential harm to an organization's brand or public image, which can result from negative events, including vendor issues.

Relevance to Scenario:

If a vendor engaged with high-profile clients suffers bad publicity, it could reflect poorly on your organization, jeopardizing its reputation.

Why Not Other Options:

A: Compliance risk relates to failing to meet regulatory requirements, which is not the primary concern here.

C: Operational risk refers to process failures or disruptions, unrelated to brand perception.

D: Strategic risk involves long-term business decisions, not immediate reputation impacts.

EC-Council CISO Handbook: Risk Management and Vendor Risk Assessment.

Question 6

Question Type: MultipleChoice

What standard would you use to help determine key performance indicators?

Options:

A- ITIL
B- FIPS140-2
C- NI5TSP800-53
D- NISTSP800-5S

Answer:

D

Question 7

Question Type: MultipleChoice

Which technology can provide a computing environment without requiring a dedicated hardware backend?

Options:

A- Mainframe server
B- Virtual Desktop
C- Thin client
D- Virtual Local Area Network

Answer:

B

Explanation:

A Virtual Desktop provides a computing environment without requiring dedicated hardware on the backend. This technology uses virtualization to host desktop environments on a centralized server, enabling users to access their desktop remotely. Unlike mainframe servers (A) or thin clients (C), virtual desktops provide flexibility, scalability, and reduced dependency on physical hardware. VLANs (D) are for network segmentation and do not provide a computing environment.

Question 8

Question Type: MultipleChoice

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and

uses the special card in order to access the restricted area of the target company. Just as the employee opens

the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so

that he can enter. What is the best way to undermine the social engineering activity of tailgating?

Options:

A- Post a sign that states, ''no tailgating'' next to the special card reader adjacent to the secure door
B- Issue special cards to access secure doors at the company and provide a one-time only brief description of
use of the special card

C- Educate and enforce physical security policies of the company to all the employees on a regular basis
D- Setup a mock video camera next to the special card reader adjacent to the secure door

Answer:

C

Question 9

Question Type: MultipleChoice

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?

Options:

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.

EC-Council CISO Material: Asset Management and Classification Best Practices.

P2P exams