Vendor: EC-Council

Exam Code: 712-50

Exam Name: EC-Council Certified CISO (CCISO)

Version: DEMO

QUESTION 1
When managing a project, the MOST important activity in managing the expectations of stakeholders is:

A. To force stakeholders to commit ample resources to support the project
B. To facilitate proper communication regarding outcomes
C. To assure stakeholders commit to the project start and end dates in writing
D. To finalize detailed scope of the project at project initiation

Answer: B
Explanation:
Managing Stakeholder Expectations:
Effective communication ensures stakeholders are informed about project goals, progress, and potential risks.

Clear and consistent communication builds trust and alignment with stakeholders' expectations.

QUESTION 2
Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

A. Incident response plan
B. Business Continuity plan
C. Disaster recovery plan
D. Damage control plan

Answer: C
Explanation:
Disaster Recovery Plan (DRP):
A DRP provides detailed, step-by-step procedures for restoring systems and operations after a disaster, such as a major earthquake. The focus is on IT systems and critical infrastructure.

QUESTION 3
A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

A. Inability to export the private certificate/key
B. It can double as physical identification at the DMV
C. It has the user's photograph to help ID them
D. It can be used as a secure flash drive

Answer: A
Explanation:
Key Cybersecurity Feature of a PIV Card:
The PIV card securely stores a private key that cannot be exported, ensuring it is only used within the card itself.

This prevents unauthorized access or duplication of sensitive cryptographic credentials.

QUESTION 4
Which of the following is the MOST important action of an Information Security Steering Committee?

A. Be briefed about new trends and products by a vendor
B. Ensure the committee includes members from different departments and employee levels
C. Ensure that security policies and procedures have been approved by the Board of Directors
D. Review of current audit and compliance reports

Answer: C
Explanation:
The EC-Council CCISO Body of Knowledge identifies ensuring board approval of security policies and procedures as the most important responsibility of an Information Security Steering Committee. CCISO guidance emphasizes that this committee serves as a governance bridge between executive leadership, the board, and operational security functions.

Board approval provides authority, accountability, and enforceability to security policies. Without this approval, policies lack governance backing and are often ignored or inconsistently applied. While diversity of membership and audit reviews are important, they are supporting functions.

CCISO materials stress that the steering committee ensures security aligns with business objectives and risk tolerance through formal board endorsement. Therefore, option C is correct.

QUESTION 5
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget. Using the best business practices for project management you determine that the project correctly aligns with the company goals and the scope of the project is correct. What is the NEXT step?

A. Review time schedules
B. Verify budget
C. Verify resources
D. Verify constraints

Answer: C
Explanation:
After verifying the scope of the project, the next logical step is to verify resources. Ensuring that adequate resources are available and appropriately allocated is critical for addressing delays and budget overruns.

Resource Verification:
Ensures sufficient personnel, budget, and tools are allocated.

Identifies bottlenecks caused by resource shortages or misallocation.

Importance After Scope:
Once the scope is validated, resource availability is a primary factor in meeting schedules and budgets.

QUESTION 6
SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. After determining the audit findings are accurate, which of the following is the MOST logical next activity?

A. Begin initial gap remediation analyses
B. Review the security organization's charter
C. Validate gaps with the Information Technology team
D. Create a briefing of the findings for executive management

Answer: A
Explanation:
Logical Next Activity After Validating Findings
Once gaps are validated, the logical next step is to perform remediation analyses to prioritize actions based on the severity of the gaps and available resources.

This step lays the groundwork for creating detailed remediation plans.

QUESTION 7
A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

A. Change management
B. Business continuity planning
C. Security Incident Response
D. Thought leadership

Answer: C
Explanation:
Convening key stakeholders to address a severe security threat is a classic example of a security incident response. It involves analyzing the threat, determining modifications to security controls, and mitigating the risk to the organization.

QUESTION 8
What type of test is performed by an auditor when a sample of programs is selected to determine if software source and object versions are the same?

A. A sample test of program library features
B. A sample test of programming object reuse controls
C. A compliance test of program compiler operations
D. A compliance test of program library controls

Answer: D
Explanation:
According to EC-Council CCISO documentation, verifying that source code and compiled object code match is part of a compliance test of program library controls.

Program library controls ensure that only authorized, approved, and properly compiled code is promoted to production. Auditors test these controls to confirm integrity, version control, and change management effectiveness.

Compiler operations (Option C) relate to build processes, not library integrity. Options A and B do not address compliance verification. Therefore, Option D is correct.

QUESTION 9
What is the MOST critical output of the incident response process?

A. A complete document of all involved team members and the support they provided
B. Recovery of all data from affected systems
C. Lessons learned from the incident, so they can be incorporated into the incident response processes
D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C
Explanation:
The most critical output of the incident response process is the lessons learned. These lessons help refine incident response plans, prevent recurrence, and improve organizational resilience. While documenting team activities, recovering data, and detailing evidence processes (A, B, D) are important, they do not provide the proactive improvement that lessons learned offer for future incident handling.

QUESTION 10
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

A. Single loss expectancy multiplied by the annual rate of occurrence
B. Total loss expectancy multiplied by the total loss frequency
C. Value of the asset multiplied by the loss expectancy
D. Replacement cost multiplied by the single loss expectancy

Answer: A
Explanation:
Calculation of Annual Loss Expectancy (ALE):
ALE = Single Loss Expectancy (SLE) x Annual Rate of Occurrence (ARO)

SLE: The monetary loss from a single event.

ARO: The estimated frequency of the event occurring annually.

Why This Formula is Correct:
This method accurately predicts potential yearly losses from specific risks, helping organizations prioritize mitigation strategies.

QUESTION 11
Which of the following is MOST useful when developing a business case for security initiatives?

A. Budget forecasts
B. Request for proposals
C. Cost/benefit analysis
D. Vendor management

Answer: C
Explanation:
Cost/benefit analysis evaluates the financial and operational advantages of a security initiative against its costs, helping build a strong business case.

Foundation for Business Cases:

Provides clarity on the financial return, operational improvements, and risk reductions offered by the initiative.

Key Elements:
Quantitative: Monetary costs and potential savings from risk mitigation.

Qualitative: Non-financial benefits like improved reputation or compliance.

Decision Support:
Enables stakeholders to understand the trade-offs, ROI, and overall value, making it a cornerstone for justifying investments.

Additional Factors:
Budget forecasts, vendor proposals, and management considerations complement but do not replace a cost/benefit analysis.

Strategic Justification: Outlines the importance of cost/benefit analysis in presenting security initiatives to decision-makers.

Resource Allocation: Helps prioritize projects with maximum return and risk reduction.

QUESTION 12
Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

A. Alignment with business goals
B. ISO27000 accreditation
C. PCI attestation of compliance
D. Financial statements

Answer: B
Explanation:
ISO27000 Accreditation
ISO 27000 standards provide a framework for assessing and certifying an organization's information security management systems (ISMS).

An independent body evaluates the organization's compliance with ISO standards, ensuring robust security controls.

QUESTION 13
Which of the following is MOST likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

Answer: C
Explanation:
Understanding Discretionary Elements:
Guidelines provide recommendations rather than mandatory actions. They are flexible and can be adapted based on specific circumstances.

Unlike policies, procedures, or standards, guidelines are not enforceable but are intended to support compliance with best practices.

QUESTION 14
Which of the following is the MOST critical aspect of a security policy?

A. Clearly defined processes to meet compliance requirements
B. Formal acknowledgement by most employees and vendors
C. An established guideline to protect confidential information
D. Communication of management's commitment to security

Answer: D
Explanation:
CCISO documentation stresses that the most critical aspect of a security policy is visible communication of management's commitment. Leadership endorsement establishes authority, accountability, and enforceability.

Processes, acknowledgements, and guidelines are important, but without leadership commitment, policies are ignored. CCISO materials consistently identify leadership commitment as the foundation of policy effectiveness.

QUESTION 15
What is the next step after defining the conditions under which standard security controls must be applied?

A. Perform an asset inventory and apply classifications
B. Analyze future security control plans
C. Adopt a culture of risk awareness
D. Create risk mitigation plans

Answer: D
Explanation:
CCISO documentation explains that once conditions for applying controls are defined, the next step is to create risk mitigation plans. This translates control requirements into actionable remediation activities, timelines, and ownership.

Asset inventory and awareness are foundational steps that typically precede control definition. Therefore, risk mitigation planning follows control applicability.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**