



712-50^{Q&As}

EC-Council Certified CISO (CCISO)

Pass EC-COUNCIL 712-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/712-50.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer, you see there is no badge reader.

What should you do?

- A. Post a guard at the door to maintain physical security
- B. Close and chain the door shut and send a company-wide memo banning the practice
- C. A physical risk assessment on the facility
- D. Nothing, this falls outside your area of influence

Correct Answer: C

QUESTION 2

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

- A. Temporal Probability (TP)
- B. Annualized Rate of Occurrence (ARO)
- C. Single Loss Expectancy (SLE)
- D. Exposure Factor (EF)

Correct Answer: B

QUESTION 3

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.

Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?

- A. NIST and Privacy Regulations
- B. NIST and Data Breach Notification Laws
- C. ISO 27000 and Payment Card Industry Data Security Standards
- D. ISO 27000 and Human resources best practices

Correct Answer: C



QUESTION 4

Which of the following statements about Encapsulating Security Payload (ESP) is true?

- A. It is an IPSec protocol
- B. It is a text-based communication protocol
- C. It uses UDP port 22
- D. It uses TCP port 22 as the default port and operates at the application layer

Correct Answer: A

QUESTION 5

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget. Using the best business practices for project management, you determine that the project correctly aligns with the organization goals.

What should be verified next?

- A. Scope
- B. Constraints
- C. Resources
- D. Budget

Correct Answer: A

QUESTION 6

Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings, you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.

To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

- A. Business continuity plan
- B. Security roadmap
- C. Business impact analysis
- D. Annual report to shareholders

Correct Answer: C



QUESTION 7

Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus.

Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

- A. Eradication
- B. Containment
- C. Recovery
- D. Identification

Correct Answer: A

QUESTION 8

An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?

- A. The DLP Solution was not integrated with mobile device anti-malware
- B. Data classification was not properly performed on the assets
- C. The sensitive data was not encrypted while at rest
- D. A risk assessment was not performed after purchasing the DLP solution

Correct Answer: B

QUESTION 9

Which type of scan is used on the eye to measure the layer of blood vessels?

- A. Facial recognition scan
- B. Iris scan
- C. Signature kinetics scan
- D. Retinal scan

Correct Answer: D



QUESTION 10

When selecting a security solution with reoccurring maintenance costs after the first year

- A. Implement the solution and ask for the increased operating cost budget when it is time
- B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
- C. Defer selection until the market improves and cash flow is positive
- D. The CISO should cut other essential programs to ensure the new solution's continued use

Correct Answer: B

QUESTION 11

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units.

Which of the following standards and guidelines can BEST address this organization's need?

- A. International Organization for Standardizations 22301 (ISO-22301)
- B. Information Technology Infrastructure Library (ITIL)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations 27005 (ISO-27005)

Correct Answer: A

QUESTION 12

Which of the following can the company implement in order to avoid this type of security issue in the future?

- A. Network based intrusion detection systems
- B. An audit management process
- C. A security training program for developers
- D. A risk management process

Correct Answer: C

QUESTION 13

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

Correct Answer: C

QUESTION 14

You have been hired as the Information System Security Officer (ISSO) for a US federal government agency. Your role is to ensure the security posture of the system is maintained. One of your tasks is to develop and maintain the system security plan (SSP) and supporting documentation.

Which of the following is NOT documented in the SSP?

- A. The controls in place to secure the system
- B. Name of the connected system
- C. The results of a third-party audits and recommendations
- D. Type of information used in the system

Correct Answer: D

QUESTION 15

What are the common data hiding techniques used by criminals?

- A. Unallocated space and masking
- B. Website defacement and log manipulation
- C. Disabled Logging and admin elevation
- D. Encryption, Steganography, and Changing Metadata/Timestamps

Correct Answer: D

Reference: <https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/>