

EC-Council

Exam Questions 712-50

EC-Council Certified CISO (CCISO)



NEW QUESTION 1

- (Exam Topic 6)

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:

Reference: <https://www.smartsheet.com/content/iso-22301-business-continuity-guide>

NEW QUESTION 2

- (Exam Topic 6)

Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye.

However, authorization failures can occur with individuals who have?

- A. Glaucoma or cataracts
- B. Two different colored eyes (heterochromia iridium)
- C. Contact lens
- D. Malaria

Answer: A

NEW QUESTION 3

- (Exam Topic 6)

A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data backup and restoral?

- A. Recovery Point Objective (RPO)
- B. Mean Time to Delivery (MTD)
- C. Recovery Time Objective (RTO)
- D. Maximum Tolerable Downtime (MTD)

Answer: C

Explanation:

Reference:

<https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%2>

NEW QUESTION 4

- (Exam Topic 6)

What is a Statement of Objectives (SOA)?

- A. A section of a contract that defines tasks to be performed under said contract
- B. An outline of what the military will do during war
- C. A document that outlines specific desired outcomes as part of a request for proposal
- D. Business guidance provided by the CEO

Answer: A

NEW QUESTION 5

- (Exam Topic 6)

Who is responsible for verifying that audit directives are implemented?

- A. IT Management
- B. Internal Audit
- C. IT Security
- D. BOD Audit Committee

Answer: B

Explanation:

Reference: <https://www.eccouncil.org/information-security-management/>

NEW QUESTION 6

- (Exam Topic 2)

Creating a secondary authentication process for network access would be an example of?

- A. Nonlinearities in physical security performance metrics

- B. Defense in depth cost enumerated costs
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Answer: A

NEW QUESTION 7

- (Exam Topic 2)

A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

- A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
- B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
- C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
- D. If the findings do not impact regulatory compliance, review current security controls.

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

When choosing a risk mitigation method what is the MOST important factor?

- A. Approval from the board of directors
- B. Cost of the mitigation is less than the risk
- C. Metrics of mitigation method success
- D. Mitigation method complies with PCI regulations

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

When dealing with a risk management process, asset classification is important because it will impact the overall:

- A. Threat identification
- B. Risk monitoring
- C. Risk treatment
- D. Risk tolerance

Answer: C

NEW QUESTION 10

- (Exam Topic 5)

Which of the following best describes the sensors designed to project and detect a light beam across an area?

- A. Smoke
- B. Thermal
- C. Air-aspirating
- D. Photo electric

Answer: D

Explanation:

Reference: https://en.wikipedia.org/wiki/Photoelectric_sensor

NEW QUESTION 11

- (Exam Topic 5)

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.

The CISO discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?

- A. Create new use cases for operational use of the solution
- B. Determine if sufficient mitigating controls can be applied
- C. Decide to accept the risk on behalf of the impacted business units
- D. Report the deficiency to the audit team and create process exceptions

Answer: B

NEW QUESTION 12

- (Exam Topic 5)

Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

- A. Network based security preventative controls
- B. Software segmentation controls
- C. Network based security detective controls
- D. User segmentation controls

Answer: A

NEW QUESTION 13

- (Exam Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. What type of control is being implemented by supervisors and data owners?

- A. Management
- B. Operational
- C. Technical
- D. Administrative

Answer: B

NEW QUESTION 14

- (Exam Topic 5)

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. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning. Which of the following is the MOST logical next step?

- A. Validate the effectiveness of current controls
- B. Create detailed remediation funding and staffing plans
- C. Report the audit findings and remediation status to business stake holders
- D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 15

- (Exam Topic 5)

When analyzing and forecasting an operating expense budget what are not included?

- A. Software and hardware license fees
- B. Utilities and power costs
- C. Network connectivity costs
- D. New datacenter to operate from

Answer: D

NEW QUESTION 16

- (Exam Topic 5)

The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

- A. Security certification
- B. Security system analysis
- C. Security accreditation
- D. Alignment with business practices and goals.

Answer: C

NEW QUESTION 17

- (Exam Topic 5)

During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

- A. The budget is in a temporary state of imbalance
- B. The budget is operating at a deficit
- C. She can realign the budget through moderate capital expense (CAPEX) allocation
- D. She has a surplus of operational expenses (OPEX)

Answer: A

NEW QUESTION 18

- (Exam Topic 5)

A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

- A. Poorly configured firewalls
- B. Malware
- C. Advanced Persistent Threat (APT)
- D. An insider

Answer: D

NEW QUESTION 19

- (Exam Topic 5)

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives. How can you reduce the administrative burden of distributing symmetric keys for your employer?

- A. Use asymmetric encryption for the automated distribution of the symmetric key
- B. Use a self-generated key on both ends to eliminate the need for distribution
- C. Use certificate authority to distribute private keys
- D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: A

NEW QUESTION 20

- (Exam Topic 5)

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?

- A. Peers
- B. End Users
- C. Executive Management
- D. All of the above

Answer: D

NEW QUESTION 21

- (Exam Topic 5)

Where does bottom-up financial planning primarily gain information for creating budgets?

- A. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages
- B. By reviewing last year's program-level costs and adding a percentage of expected additional portfolio costs
- C. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle
- D. By adding all planned operational expenses per quarter then summarizing them in a budget request

Answer: D

NEW QUESTION 22

- (Exam Topic 5)

Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. Once supervisors and data owners have approved requests, information system administrators will implement

- A. Technical control(s)
- B. Management control(s)
- C. Policy control(s)
- D. Operational control(s)

Answer: A

NEW QUESTION 23

- (Exam Topic 5)

A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?

- A. Service
- B. Program
- C. Portfolio
- D. Cost center

Answer: B

NEW QUESTION 24

- (Exam Topic 5)

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

Answer: D

NEW QUESTION 25

- (Exam Topic 5)

Which of the following would negatively impact a log analysis of a multinational organization?

- A. Centralized log management
- B. Encrypted log files in transit
- C. Each node set to local time
- D. Log aggregation agent each node

Answer: D

NEW QUESTION 26

- (Exam Topic 3)

The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?

- A. Provide developer security training
- B. Deploy Intrusion Detection Systems
- C. Provide security testing tools
- D. Implement Compensating Controls

Answer: D

NEW QUESTION 27

- (Exam Topic 3)

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

- A. Failed to identify all stakeholders and their needs
- B. Deployed the encryption solution in an inadequate manner
- C. Used 1024 bit encryption when 256 bit would have sufficed
- D. Used hardware encryption instead of software encryption

Answer: A

NEW QUESTION 28

- (Exam Topic 3)

The ultimate goal of an IT security projects is:

- A. Increase stock value
- B. Complete security
- C. Support business requirements
- D. Implement information security policies

Answer: C

NEW QUESTION 29

- (Exam Topic 3)

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

- A. Alignment with the business
- B. Effective use of existing technologies
- C. Leveraging existing implementations
- D. Proper budget management

Answer: A

NEW QUESTION 30

- (Exam Topic 2)

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

- A. Servers, routers, switches, modem
- B. Firewall, exchange, web server, intrusion detection system (IDS)
- C. Firewall, anti-virus console, IDS, syslog
- D. IDS, syslog, router, switches

Answer: C

NEW QUESTION 31

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

712-50 Practice Exam Features:

- * 712-50 Questions and Answers Updated Frequently
- * 712-50 Practice Questions Verified by Expert Senior Certified Staff
- * 712-50 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 712-50 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 712-50 Practice Test Here](#)