

DUMPS ARENA

EC-Council Information Security Manager (E|ISM)

EC Council 512-50

Version Demo

Total Demo Questions: 20

Total Premium Questions: 404

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Governance, Risk, Compliance	98
Topic 2, Information Security Controls and Audit Management	76
Topic 3, Security Program Management and Operations	69
Topic 4, Information Security Core Competencies	31
Topic 5, Strategic Planning, Finance, Procurement, and Third-Party Management	130
Total	404

QUESTION NO: 1

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

- A. Enforce the existing security standards and do not allow the deployment of the new technology.
- B. Amend the standard to permit the deployment.
- C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
- D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

ANSWER: C**QUESTION NO: 2**

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

- A. The Net Present Value (NPV) of the project is positive
- B. The NPV of the project is negative
- C. The Return on Investment (ROI) is larger than 10 months
- D. The ROI is lower than 10 months

ANSWER: B**QUESTION NO: 3**

To have accurate and effective information security policies how often should the CISO review the organization policies?

- A. Every 6 months
- B. Quarterly
- C. Before an audit
- D. At least once a year

ANSWER: D

QUESTION NO: 4

Information security policies should be reviewed:

- A. by stakeholders at least annually
- B. by the CISO when new systems are brought online
- C. by the Incident Response team after an audit
- D. by internal audit semiannually

ANSWER: A**QUESTION NO: 5**

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

- A. Subscribe to vendor mailing list to get notification of system vulnerabilities
- B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
- C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
- D. Conduct security testing, vulnerability scanning, and penetration testing

ANSWER: D**QUESTION NO: 6**

Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.

When adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

- A. Annually
- B. Semi-annually
- C. Quarterly
- D. Never

ANSWER: D**QUESTION NO: 7**

File Integrity Monitoring (FIM) is considered a

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

ANSWER: C

QUESTION NO: 8

Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?

- A. Configure logging on each access point
- B. Install a firewall software on each wireless access point.
- C. Provide IP and MAC address
- D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.

ANSWER: C

QUESTION NO: 9

A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes. Which of the following represents the MOST LIKELY cause of this situation?

- A. Poor audit support for the security program
- B. A lack of executive presence within the security program
- C. Poor alignment of the security program to business needs
- D. This is normal since business units typically resist security requirements

ANSWER: C

QUESTION NO: 10

When should IT security project management be outsourced?

- A. When organizational resources are limited
- B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
- C. On new, enterprise-wide security initiatives

D. On projects not forecasted in the yearly budget

ANSWER: B

QUESTION NO: 11

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

- 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

QUESTION NO: 12

Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

- A. Need to comply with breach disclosure laws
- B. Need to transfer the risk associated with hosting PII data
- C. Need to better understand the risk associated with using PII data
- D. Fiduciary responsibility to safeguard credit card information

ANSWER: C

QUESTION NO: 13

Which of the following activities must be completed BEFORE you can calculate risk?

- A. Determining the likelihood that vulnerable systems will be attacked by specific threats
- B. Calculating the risks to which assets are exposed in their current setting
- C. Assigning a value to each information asset
- D. Assessing the relative risk facing the organization's information assets

ANSWER: C

QUESTION NO: 14

The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

- A. The asset is more expensive than the remediation
- B. The audit finding is incorrect
- C. The asset being protected is less valuable than the remediation costs
- D. The remediation costs are irrelevant; it must be implemented regardless of cost.

ANSWER: C**QUESTION NO: 15**

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**QUESTION NO: 16**

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. A security training program for developers
- C. A risk management process
- D. A audit management process

ANSWER: B

QUESTION NO: 17

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

- A. Susceptibility to attack, mitigation response time, and cost
- B. Attack vectors, controls cost, and investigation staffing needs
- C. Vulnerability exploitation, attack recovery, and mean time to repair
- D. Susceptibility to attack, expected duration of attack, and mitigation availability

ANSWER: A**QUESTION NO: 18**

The PRIMARY objective for information security program development should be:

- A. Reducing the impact of the risk to the business.
- B. Establishing strategic alignment with business continuity requirements
- C. Establishing incident response programs.
- D. Identifying and implementing the best security solutions.

ANSWER: A**QUESTION NO: 19**

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a need to develop a more unified incident response capability.
- B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
- C. When there is a variety of technologies deployed in the infrastructure.
- D. When it results in an overall lower cost of operating the security program.

ANSWER: B**QUESTION NO: 20**

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