

BraindumpQuiz



- ✓ Online Tool, Convenient, easy to study.
- ✓ Instant Online Access
- ✓ Supports All Web Browsers
- ✓ Practice Online Anytime
- ✓ Test History and Performance Review
- ✓ Supports Windows / Mac / Android / iOS, etc.



- ✓ Installable Software Application
- ✓ Simulates Real Exam Environment
- ✓ Builds Exam Confidence
- ✓ Supports MS Operating System
- ✓ Two Modes For Practice
- ✓ Practice Offline Anytime



- ✓ Printable PDF Format
- ✓ Prepared by IT Experts
- ✓ Instant Access to Download
- ✓ Study Anywhere, Anytime
- ✓ 365 Days Free Updates
- ✓ Free PDF Demo Available



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.



Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

<http://www.braindumpquiz.com/>

Best exam materials provider - BraindumpQuiz! Choosing us, Benefit more!

Exam : **512-50**

Title : EC-Council Information
Security Manager (E |ISM)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

- A. perform an independent audit of the security controls.
- B. assign the responsibility to the information security team.
- C. assign the responsibility to the team responsible for the management of the controls.
- D. create operational reports on the effectiveness of the controls.

Answer: A

NO.2 The effectiveness of an audit is measured by?

- A. How the recommendations directly support the goals of the company
- B. How it exposes the risk tolerance of the company
- C. The number of security controls the company has in use
- D. The number of actionable items in the recommendations

Answer: A

NO.3 Which of the following is a primary method of applying consistent configurations to IT systems?

- A. Administration
- B. Audits
- C. Patching
- D. Templates

Answer: C

NO.4 Which of the following is a major benefit of applying risk levels?

- A. Risk appetite can increase within the organization once the levels are understood
- B. Risk management governance becomes easier since most risks remain low once mitigated
- C. Resources are not wasted on risks that are already managed to an acceptable level
- D. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology

Answer: C

NO.5 The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

- A. This represents a conflict of interest
- B. The IT team is not familiar in IT audit practices
- C. This represents a bad implementation of the Least Privilege principle
- D. The IT team is not certified to perform audits

Answer: A

NO.6 A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

- A. The software license expiration is probably out of synchronization with other software licenses
- B. The project was initiated without an effort to get support from impacted business units in the organization
- C. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects
- D. The software is out of date and does not provide for a scalable solution across the enterprise

Answer: B

NO.7 The general ledger setup function in an enterprise resource package allows for setting accounting periods.

Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

- A. The lack of policies and procedures for the proper segregation of duties.
- B. The need to change accounting periods on a regular basis.
- C. The need to create and modify the chart of accounts and its allocations.
- D. The requirement to post entries for a closed accounting period.

Answer: A

NO.8 While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

- A. Disaster recovery strategic plan
- B. Enterprise Risk Assessment
- C. Business continuity plan
- D. Application mapping document

Answer: A

NO.9 Human resource planning for security professionals in your organization is a:

- A. Training requirement that is on-going and always changing.
- B. Simple and easy task because the threats are getting easier to find and correct.
- C. Not needed because automation and anti-virus software has eliminated the threats.
- D. Training requirement that is met through once every year user training.

Answer: A

NO.10 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.

Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

- A. Involve internal audit
- B. Upper management support
- C. More frequent project milestone meetings
- D. More training of staff members

Answer: B

Explanation

Scenario10

NO.11 Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

- A. Decreased security awareness
- B. Reduction of budget
- C. Fines for regulatory non-compliance
- D. Improper use of information resources

Answer: C

NO.12 Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

- A. Understand the business goals of the organization
- B. Poses a strong technical background
- C. Understand all regulations affecting the organization
- D. Poses a strong auditing background

Answer: A

NO.13 Smith, the project manager for a larger multi-location firm, is leading a software project team that has 18 members, 5 of which are assigned to testing. Due to recent recommendations by an organizational quality audit team, the project manager is convinced to add a quality professional to lead to test team at additional cost to the project.

The project manager is aware of the importance of communication for the success of the project and takes the step of introducing additional communication channels, making it more complex, in order to assure quality levels of the project. What will be the first project management document that Smith should change in order to accommodate additional communication channels?

- A. Change control document
- B. Risk management plan
- C. WBS document
- D. Scope statement

Answer: C

NO.14 With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

- A. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
- B. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
- C. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program

D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

Answer: A

Reference: https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf (9)

NO.15 Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

- A.** Detective Controls
- B.** Preemptive Controls
- C.** Organizational Controls
- D.** Proactive Controls

Answer: C

NO.16 Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

- A.** Rigorous syslog reviews
- B.** Security Guards posted outside the Data Center
- C.** Intrusion Detection Systems (IDS)
- D.** Data Loss Prevention (DLP)

Answer: D

NO.17 Acceptable levels of information security risk tolerance in an organization should be determined by?

- A.** CEO and board of director
- B.** Corporate compliance committee
- C.** CISO with reference to the company goals
- D.** Corporate legal counsel

Answer: A

NO.18 Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

- A.** Least privileges
- B.** Rights collision

- C. Excessive privileges
- D. Privilege creep

Answer: C

NO.19 Which of the following is the MAIN security concern for public cloud computing?

- A. Unable to control physical access to the servers
- B. Unable to track log on activity
- C. Unable to run anti-virus scans
- D. Unable to patch systems as needed

Answer: A

NO.20 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. Annualized Rate of Occurrence (ARO)
- B. Single Loss Expectancy (SLE)
- C. Temporal Probability (TP)
- D. Exposure Factor (EF)

Answer: A