DUMPSQUEEN

EC-Council Information Security Manager (E|ISM)

ECCouncil 512-50

Version Demo

Total Demo Questions: 20

Total Premium Questions: 404

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

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

Who in the organization determines access to information?

A. Legal department

B. Compliance officer

C. Data Owner

D. Information security officer

ANSWER: C

QUESTION NO: 2

Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

A. Security regulations

B. Asset classification

C. Information security policy

D. Data classification

ANSWER: C

QUESTION NO: 3

The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for

A. Confidentiality, Integrity and Availability

B. Assurance, Compliance and Availability

C. International Compliance

D. Integrity and Availability

ANSWER: A

QUESTION NO: 4

Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

A. National Institute of Standards and Technology (NIST) Special Publication 800-53

B. Payment Card Industry Digital Security Standard (PCI DSS)

C. International Organization for Standardization – ISO 27001/2

D. British Standard 7799 (BS7799)

ANSWER: C

Explanation:

Scenario2

QUESTION NO: 5

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

QUESTION NO: 6

Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.

B. Shadow applications.

C. Deception technology.

D. Vulnerability management.

ANSWER: B

QUESTION NO: 7

Which of the following is the BEST indicator of a successful project?

A. it is completed on time or early as compared to the baseline project plan

B. it meets most of the specifications as outlined in the approved project definition

C. it comes in at or below the expenditures planned for in the baseline budget

D. the deliverables are accepted by the key stakeholders

ANSWER: D

QUESTION NO: 8

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: 9

Which of the following is MOST important when dealing with an Information Security Steering committee:

A. Include a mix of members from different departments and staff levels.

B. Ensure that security policies and procedures have been vetted and approved.

C. Review all past audit and compliance reports.

D. Be briefed about new trends and products at each meeting by a vendor.

ANSWER: C

QUESTION NO: 10

The amount of risk an organization is willing to accept in pursuit of its mission is known as

A. Risk mitigation

B. Risk transfer

C. Risk tolerance

D. Risk acceptance

ANSWER: C

QUESTION NO: 11

Which of the following intellectual Property components is focused on maintaining brand recognition?

A. Trademark

B. Patent

C. Research Logs

D. Copyright

ANSWER: A

QUESTION NO: 12

Which business stakeholder is accountable for the integrity of a new information system?

A. CISO

B. Compliance Officer

C. Project manager

D. Board of directors

ANSWER: A

QUESTION NO: 13

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

A. Distance learning/Web seminars

B. Formal Class

C. One-One Training

D. Self –Study (noncomputerized)

ANSWER: D

QUESTION NO: 14

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 is unsure of the information provided and orders a vendor proof of concept to validate the system's scalability. This demonstrates which of the following?

A. An approach that allows for minimum budget impact if the solution is unsuitable

B. A methodology-based approach to ensure authentication mechanism functions

C. An approach providing minimum time impact to the implementation schedules

D. A risk-based approach to determine if the solution is suitable for investment

ANSWER: D

QUESTION NO: 15

Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

A. All vulnerabilities found on servers and desktops

B. Only critical and high vulnerabilities on servers and desktops

C. Only critical and high vulnerabilities that impact important production servers

D. All vulnerabilities that impact important production servers

ANSWER: C

QUESTION NO: 16

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: 17

During the last decade, what trend has caused the MOST serious issues in relation to physical security?

A. Data is more portable due to the increased use of smartphones and tablets

B. The move from centralized computing to decentralized computing

C. Camera systems have become more economical and expanded in their use

D. The internet of Things allows easy compromise of cloud-based systems

ANSWER: A

QUESTION NO: 18

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

A. Security administrators

B. Security mangers

C. Security technicians

D. Security analysts

ANSWER: B

QUESTION NO: 19

Dataflow diagrams are used by IT auditors to:

A. Order data hierarchically.

B. Highlight high-level data definitions.

C. Graphically summarize data paths and storage processes.

D. Portray step-by-step details of data generation.

ANSWER: C

QUESTION NO: 20

Payment Card Industry (PCI) compliance requirements are based on what criteria?

A. The types of cardholder data retained

B. The duration card holder data is retained

C. The size of the organization processing credit card data

D. The number of transactions performed per year by an organization

ANSWER: D