

# Question Bank/Mock Exam Questions

1. True or False: Data integrity can be affected by virus infections and data communications errors.
2. What is the name of the process that is used to establish whether or not a user's identity is legitimate?
  - A. Availability
  - B. Accountability
  - C. Authorization
  - D. Authentication
3. Which of the following terms can be used to describe trade secrets, copyrights, trademarks, and patents?
  - A. Quality of service
  - B. Availability
  - C. Intellectual property
  - D. Competitive intelligence
4. A person who has authorization from an organization to test its information systems and network defence is known as which of the following?
  - A. script kiddie
  - B. penetration tester
  - C. professional hacker
  - D. packet monkey
5. What type of malware actually evolves, changing its size and other external file characteristics to elude detection by antivirus programs?
  - A. Trojan horse
  - B. trap door
  - C. polymorphic threat
  - D. macro virus
6. Which is NOT one of the core principles in traditional management theory?
  - A. Staffing
  - B. Leading
  - C. Directing
  - D. Controlling
7. What is the name for an intermediate point in a planning process, at which progress towards a goal can be measured?
  - A. Break point
  - B. Stop point
  - C. Objective

- D. Directive
- 8. Which management function is dedicated to the structuring of resources to support the accomplishment of objectives?
  - A. Organizing
  - B. Controlling
  - C. Planning
  - D. Leading
- 9. In which of the following policies would you find sets of rules that define acceptable behaviour within a specific organizational resource, such as Internet usage?
  - A. System-Specific Policies
  - B. Issue-Specific Security Policies
  - C. Enterprise Information Security Policy
  - D. Security Awareness Policy
- 10. The study of choices that have been made by individuals in the past is known as which of the following?
  - A. Normative Ethics
  - B. Applied Ethics
  - C. Meta-Ethics
  - D. Descriptive Ethics
- 11. Which of the following is a collection of statutes that regulates the interception of wire, electronic, and oral communications?
  - A. Federal Privacy Act
  - B. Copyright Act
  - C. Security and Freedom Through Encryption Act
  - D. Electronic Communications Privacy Act (ECPA)
- 12. All but which of the following is one of the five fundamental privacy principles of HIPAA?
  - A. Public control of medical information
  - B. Boundaries on the use of medical information
  - C. Balance of public responsibility for the use of medical information
  - D. Security of health information
- 13. Which of the six PCI DSS standard areas includes the requirement of using maintained and updated malware and anti-virus protection?
  - A. Cardholder Data Protection
  - B. Vulnerability Management Program Maintenance
  - C. Strong Access Control Measure Implementation
  - D. Network Monitoring and Testing
- 14. True or False: Liability can be applied to conduct even when no law or contract has been breached.

15. A court's right to hear a case if an act was committed in its territory or involving its citizenry is known as which of the following?
- A. restitution
  - B. jurisdiction
  - C. diligence
  - D. due care
16. What act increased the Secret Service's role in investigating fraud and related activity in connection with computers?
- A. PATRIOT Act
  - B. Digital Millennium Copyright Act
  - C. Computer Fraud and Abuse Act
  - D. Sarbanes-Oxley Act
17. Which of the following is the most complex part of the digital forensics investigation process?
- A. Identify relevant items
  - B. Acquire the evidence
  - C. Authenticate the recovered evidence
  - D. Analyze the data
18. Which of the following is used to declare the intended areas of operation for a business?
- A. Values statement
  - B. Vision statement
  - C. Objectives statement
  - D. Mission Statement
19. True or False: Organizational planning should make use of a bottom-up process in which the employees choose the initiatives the organization should pursue.
20. A multi-layered approach to strategic planning encompasses two key objectives: general strategy and which of the following?
- A. overall strategic planning
  - B. Archived profiling
  - C. Organizational profiling
  - D. InfoSec planning
21. Which of the following best describes a stakeholder?
- A. An individual or group that owns financial stock in an organization
  - B. A competing organization
  - C. An individual who buys an organization's products
  - D. An individual or group who has a vested interest
22. Which of the following is used to establish a formal set of organizational principles and qualities for an organization?
- A. Values statement
  - B. Vision statement

- C. Mission statement
- D. Morals statement

23. True or False: InfoSec objectives must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach.
24. According to the IDEAL framework, which functional role should be responsible for communicating policies to employees and coordinate training?
- A. Chief Executive Officer
  - B. Chief Risk Officer
  - C. Mid-Level Manager
  - D. Enterprise Staff
25. Which of the following governance processes, as outlined in ISO 27014:2013, involves the review and assessment of organizational information security performance toward goals and objectives by the governing body?
- A. Monitor
  - B. Direct
  - C. Communicate
  - D. Assure
26. Why is the bottom-up approach less effective than the top-down approach?
- A. Lack of technical support
  - B. Lack of management support
  - C. Lack of stakeholder support
  - D. Lack of stockholder support
27. Which type of security policy sets the strategic direction, scope, and tone for an organization's security efforts?
- A. System-specific security policy
  - B. Issue-specific security policy
  - C. Enterprise information security policy
  - D. Strategic planning security policy
28. True or False: Most modern server operating systems translate ACLs into configuration sets that administrators can use to control access to their systems.
- A. Answer: True
29. Which of the following is NOT a typical permission available for use in ACLs?
- A. Read
  - B. Write
  - C. Delete
  - D. Expunge
30. Which of the following is NOT a specific characteristic of ISSP?

- A. It addresses specific technology-based resources
  - B. It requires frequent updates
  - C. It addresses hardware implementation issues
  - D. It contains an issue statement
31. Which of the following is NOT an InfoSec policy recommended in NIST's Special Publication 800-14 document?
- A. Enterprise information security policy (EISP)
  - B. Issue-specific security policies (ISSP)
  - C. System-specific security policies (SysSP)
  - D. Task-specific security policies (TSSP)
32. What is used to regulate the who, what, when, where, and how aspects of access to a system or resource?
- A. Configuration rules
  - B. Access control lists
  - C. Rule-based policies
  - D. Security policies
33. True or False: A policy administrator is the combination of a system administrator and a CIO.
34. In which SecSDLC phase should the policy development committee determine the fundamental philosophy of the organization when it comes to policy?
- A. Implementation phase
  - B. Design phase
  - C. Investigation phase
  - D. Analysis phase
35. What is the name of the agreement screen that prompts for user acceptance of fair and responsible use terms for a particular software package?
- A. End-user license agreement
  - B. End-user fair-use policy
  - C. End-user terms of use agreement
  - D. End-user distribution policy
36. All but which of the following occurs during the investigation phase of policy development?
- A. Attaining support from senior management
  - B. Providing clear articulation of goals
  - C. Performing a risk assessment
  - D. Creating a detailed outline of a policy's scope
37. Which of the following information security roles best describe a type of specialized security administrator, and is typically responsible for analyzing and designing security solutions in a specific domain.
- A. Security manager
  - B. Chief security officer

- C. Security analyst
  - D. Chief information security officer
38. True or False: A CISO never reports to the CIO, and must always go through management hierarchies.
39. Which security role is typically an entry-level position responsible for monitoring some aspect of the organization's security posture?
- A. Security technicians
  - B. Security administrators
  - C. Analysts
  - D. Watchstanders
40. Which certification is considered to be one of the most prestigious certifications for security managers and CISOs?
- A. CISA
  - B. CISSP
  - C. CND
  - D. CompTIA Security+
41. An organization is considered to be medium-sized when it has approximately how many devices?
- A. Less than 100
  - B. More than 1000
  - C. More than 100, less than 1000
  - D. More than 2000
42. True or False: It is the CISO's responsibility to ensure that InfoSec functions are performed within an organization.
43. All but which of the following is certification training recommended for a student focusing on managerial information security?
- A. Certified Information Systems Security Professional
  - B. Security+
  - C. Certified Information Security Manager
  - D. Global Information Security Officer
44. Which of the following is NOT a major benefit of SETA programs?
- A. They enable the organization to hold employees accountable
  - B. They can inform members of the organization about where to report policy violations
  - C. They can improve employee behavior
  - D. They can improve configuration rule security
45. Which of the following represents a sequence of activities or events that take the majority of time to complete on a PERT or CPM diagram?
- A. Critical order
  - B. Absolute path

- C. Slack time
  - D. Critical path
46. Which of the following is considered one of the least frequently implemented but most effective security methods?
- A. Security Education
  - B. Security Certifications
  - C. Security Training
  - D. Security Awareness
47. True or False: Only the InfoSec and IT communities have a role to play in the management of risks to information assets.
48. The evaluation and reaction to risk to the entire organization is known as which of the following?
- A. RM framework
  - B. RM process
  - C. Enterprise Risk Management (ERM)
  - D. risk management policy
49. Which of the following is the first stage of the RM framework?
- A. Framework design
  - B. Framework monitoring and review
  - C. Continuous improvement
  - D. Executive governance and support
50. What name is given to the relative executives who work together with the support of the CISO in developing and enabling the RM framework and its resulting process?
- A. governance group
  - B. RM framework team
  - C. risk management policy developers
  - D. risk tolerance team
51. Which of the following framework implementation methods is considered the boldest method?
- A. desk check
  - B. pilot test
  - C. phased approach
  - D. direct cutover
52. An evaluation of the threats to information assets?
- A. threat assessment
  - B. risk analysis
  - C. data classification scheme
  - D. risk identification
53. In some corporate models, information assets can be categorized into which of the following groups?
- A. People, planning, technology

- B. Planning, performing, tasking
- C. Preparedness, planning, and technology
- D. People, process, and technology

54. Which term below defines the identification and assessment of risks for each vulnerability identified by an organization?

- A. Risk determination
- B. Risk analysis
- C. Risk identification
- D. Risk management

55. The overall rating, or numerical value, of the probability that a specific vulnerability will be exploited is known as which of the following?

- A. risk
- B. risk determination
- C. likelihood
- D. qualitative assessment

56. Which of the following terms best describes the state of having limited or imperfect knowledge of a situation, making it less likely the organization can successfully anticipate future events or outcomes?

- A. uncertainty
- B. risk determination
- C. likelihood
- D. risk appetite

57. Which risk treatment strategy focuses on planning and preparation to reduce the damage caused by a realized incident or disaster?

- A. Mitigation
- B. Termination
- C. Transference
- D. Acceptance

58. True or False: An example of using the transference risk treatment strategy would be to outsource the security of an asset to another organization.

59. Which of the following is NOT one of the three types of plans included in a mitigation risk treatment strategy?

- A. Incident response (IR) plan
- B. Disaster recovery (DR) plan
- C. Business continuity (BC) plan
- D. Risk control plan (RC)

60. When is the acceptance risk treatment strategy NOT an acceptable approach?

- A. The cost of protecting an asset is more than the asset is worth
- B. The asset consists of employee and / or customer information
- C. The asset is considered expendable
- D. The asset has relatively little risk

61. Which risk treatment strategy approach can also be referred to as an avoidance strategy?
- A. Termination
  - B. Acceptance
  - C. Defence
  - D. Transferral
62. Which of the following can be calculated using the values from an ARO multiplied by the values from an SLE?
- A. cost benefit analysis
  - B. asset valuation
  - C. annualized loss expectancy
  - D. operational feasibility
63. True or False: Asset valuation is the process of assigning financial value or worth to each information asset.
64. Operational feasibility, which refers to user acceptance and support, as well as management acceptance and support, is also known as which of the following?
- A. organizational feasibility
  - B. behavioural feasibility
  - C. technical feasibility
  - D. political feasibility
65. Which risk management technique relies on a group evaluating, rating, and ranking assets?
- A. Delphi technique
  - B. OCTAVE methods
  - C. Microsoft's technique
  - D. FAIR
66. Taking a look at the paths taken by other organization in order to create a blueprint is known as which of the following?
- A. framework
  - B. benchmarking
  - C. comparison model
  - D. architecture
67. Which of the following is NOT one of the five principles provided by COBIT 5?
- A. Meeting Stakeholder Needs
  - B. Covering the Enterprise End-to-End
  - C. Applying a Single, Integrated Framework
  - D. Reliability of Financial Reporting

68. What term is used to describe the act of retrieving potentially compromising information from recycle bins or trash areas?
- A. cleaning trash
  - B. dumpster diving
  - C. mantrap
  - D. shoulder surfing
69. True or False: In lattice-based access control, users are assigned a matrix of authorizations for particular areas of access.
70. When using the U.S. military classification scheme, which classification indicates that disclosure of contained information could cause minor or moderate damage to national security?
- A. Confidential data
  - B. Need-to-know
  - C. Top secret data
  - D. For official use only
71. The use of specialized classification schemes is known as which of the following?
- A. Clarification
  - B. Obfuscation
  - C. Compartmentalization
  - D. Fortification
72. In the Clark-Wilson integrity model, what is known as a procedure that only allows changes to a constrained data item?
- A. integrity verification procedure
  - B. target of evaluation procedure
  - C. system evaluation procedure
  - D. transformation procedure
73. Which of the following is NOT one of the primitive protection rights in the Graham-Denning Access Control Model?
- A. Create object
  - B. Grant object
  - C. Read access
  - D. Transfer access
74. True or False: Organizations that provide complete job descriptions when advertising open positions should include the elements of the job description that describe access privileges.
75. Which type of security (background) check might be required by someone applying for jobs in law enforcement or high-security positions?
- A. identity checks
  - B. credit history
  - C. polygraph test
  - D. reference check

76. Which personnel security practice is used to ensure that no one employee is performing actions that cannot be knowledgeably reviewed by another employee?
- A. mandatory vacation policy
  - B. two-person control
  - C. separation of duties
  - D. task rotation
77. All but which of the following is one of the four factors critical to success of an InfoSec program, as listed by SP 800-55 Rev. 1?
- A. Actions-oriented measurement analysis
  - B. Strong upper-level management support
  - C. Practical InfoSec policies and procedures
  - D. Quantifiable performance measurements
78. Which phase of the performance measurement development process identifies relevant stakeholders and their interests in InfoSec measurement?
- A. Phase 1
  - B. Phase 2
  - C. Phase 4
  - D. Phase 7
79. Measurements that examine the performance of an individual control or group of controls within the InfoSec program are known as which of the following?
- A. micro-focus measurements
  - B. baseline measurements
  - C. macro-focus measurements
  - D. benchmark measurements
80. True or False: Performance targets are often a hindrance to effective security.
81. True or False: An organization that works within an industry regulated by laws and standards is required to meet regulatory or industry guidelines in security practices.
82. What term below is used to describe security efforts that are considered among the best in an industry?
- A. Standard of due care
  - B. Standard of due diligence
  - C. Recommended business practices
  - D. Best security practices
83. Which of the following contains the contact information of individuals that need to be notified in the event of an actual incident?
- A. incident response policy
  - B. business process
  - C. alert roster
  - D. after-action review

84. True or False: Detecting a modification of system logs is an indicator that an actual incident has taken place.
85. Which of the following is NOT a major component of contingency planning?
- A. Incident response plan
  - B. Disaster relief plan
  - C. Disaster recovery plan
  - D. Business continuity plan
86. True or False: Slow-onset disasters occur over time and gradually degrade an organization's ability to withstand their effects.
87. Which type of offsite backup service provides backups for transactional data only, typically in real time?
- A. Electronic vaulting
  - B. Traditional data backups
  - C. Database shadowing
  - D. Remote journaling
88. There are several strategies that can be used to test contingency plans. Which of the following is the simplest kind of validation and involves distributing copies of the appropriate plans to all individuals who will be assigned roles during an actual incident?
- A. full-interruption testing
  - B. simulation
  - C. structured walk-through
  - D. desk check
89. A snapshot of a particular version of software assembled or linked from its component modules is known as which of the following?
- A. auditing
  - B. minor release
  - C. build
  - D. software library
90. True or False: Agencies should monitor the status of their programs to ensure that ongoing information security activities are providing appropriate support to the agency's mission.
91. Which phase of the security services life cycle (SSLC) involves determining the need?
- A. Initiation Phase
  - B. Assessment Phase

- C. Operations Phase
- D. Implementation Phase

92. In which CM control does the organization analyze changes to the information system to determine potential security impacts prior to change implementation?
- A. Baseline Configuration
  - B. Security Impact Analysis
  - C. Access Restrictions for Change
  - D. Configuration Management Policy and Procedures
93. Which of the following is NOT a domain in the recommended maintenance model?
- A. Readiness and review
  - B. Internal monitoring
  - C. Vulnerability assessment and remediation
  - D. Configuration management
94. Which of the following terms best describe a procedure that compares the current state of a network-segment against a known previous state of the same network segment?
- A. difference analysis
  - B. external monitoring
  - C. internal monitoring
  - D. intrusion detection
95. Which component of the maintenance model focuses on identifying and planning ongoing information security activities and identifying risks?
- A. Electronic vaulting
  - B. Traditional data backups
  - C. Database shadowing
  - D. Remote journaling
96. True or False: An intranet vulnerability assessment is designed to find and document selected vulnerabilities that are likely to be present on the organization's public network.
97. The use of mobile scanning techniques to identify open wireless access points is known as which of the following?
- A. wireless vulnerability testing
  - B. war driving
  - C. intrusion detection
  - D. penetration testing
98. Which of the following uses a challenge response mechanism in which a server challenges a user with a number, which a user must then enter into a device to calculate the response number?
- A. virtual password
  - B. synchronous token
  - C. smart card

D. asynchronous token

99. True or False: A password is typically longer than a passphrase.

100. What is the name for a network segment that exists as an intermediate area between a trusted network and an untrusted network?

- A. Proxied network zone (PNZ)
- B. Sanitization zone (SZ)
- C. Demilitarized zone (DMZ)
- D. Internal-External zone (IEZ)

101. Which of the following terms best describe a firewall type that can react to network traffic and create or modify configuration rules to adapt?

- A. application layer firewall
- B. dynamic packet filtering firewall
- C. proxy firewall
- D. content filter

102. What term is described as the rate at which fraudulent users or nonusers are allowed access to systems as a result of failure within a biometric device?

- A. False accept rate
- B. False reject rate
- C. Crossover error rate
- D. False negative rate

103. Which encryption technique is the successor to 3DES, and has a key length of 128, 192, or 256 bits?

- A. Data Encryption Standard (DES)
- B. Advanced Encryption Standard (AES)
- C. Kerberos
- D. IP Security (IPsec)

104. After plaintext messages have been encrypted, the encrypted text is known as which of the following?

- A. algorithm
- B. decipher
- C. cleartext
- D. ciphertext

105. True or False: Private key encryption is also known as asymmetric encryption.

106. Wireshark is an example of what type of utility?

- A. Port scanner
- B. Content filter
- C. Packet sniffer
- D. Vulnerability scanner

**Definition-Based Questions (5 Marks Each):** approximately 60 to 80 words

1. Define "Compliance" within the realm of data security and elucidate its critical importance for organizations.
2. Elaborate on the role of "Cryptography" in safeguarding data security and elucidate how it serves as a protective measure for sensitive information.
3. Explain the concept of "Physical Security" and offer an illustrative example of a physical security measure.
4. Define "Intrusion Detection Systems (IDS)" and provide a brief description of how these systems assist organizations in maintaining data security.
5. Define the strategic role of "Governance and Strategic Planning for Security" in the management of information security.
- 6.

Explore the relationship between "Risk Management: Identifying and Assessing Risk" and the development of a comprehensive security program. (5 marks)

**Long Essay Questions (15 Marks Each):** approximately 250 to 300 words

1. Compose a comprehensive essay on the "Security Mechanisms" employed in safeguarding data. Examine a range of mechanisms, such as access controls, firewalls, and intrusion detection systems, and analyze how these are incorporated into the overarching security strategy of an organization.

2. Assess the significance of "Risk Management" in the realm of data security. Outline the procedures involved in identifying and evaluating risks, and delve into effective strategies for controlling and mitigating these risks.

3. Explore the importance of "Governance" and its impact on strategic planning for security. Provide examples of how effective governance can influence an organization's ability to manage data security.

4. Compare and contrast different "Security Management Models and Practices." Discuss the advantages and disadvantages of each model and provide recommendations for selecting the most suitable one for an organization.

5. Discuss the challenges and considerations involved in "Planning for Contingencies" in data security. Explain the importance of having a robust contingency plan and how it can mitigate potential security breaches.

The END