Sample Information Assurance and security questions for Exit Exam preparation

By: - Berhanu M.

Area: Threats, risks, and vulnerabilities in information systems

1. Which of the following terms is defined as a potential danger that can exploit a vulnerability in an information system?
A) Risk
B) Threat
C) Vulnerability
D) Control

[1] Answer: B) Threat

2. What is the most significant difference between a threat and a vulnerability?
A) Threats are intentional and malicious, while vulnerabilities are accidental and unintentional.
B) Threats are accidental and unintentional, while vulnerabilities are intentional and malicious.
C) Threats are potential dangers to information systems, while vulnerabilities are weaknesses or security gaps.
D) Threats and vulnerabilities are synonymous terms with the same meaning.

[2] Answer: C) Threats are potential dangers to information systems, while vulnerabilities are weaknesses or security gaps.

3. Which of the following best describes a vulnerability in an information system?
A) A situation where a user forgets a password to their account.
B) An action taken by an attacker to steal sensitive information.
C) A weakness or security gap that can be exploited to compromise sensitive data.
D) A malicious program or code that can harm a system.

[3] Answer: C) A weakness or security gap that can be exploited to compromise sensitive data.

4. Which of the following best describes a risk in an information system?
A) The probability that a threat agent will exploit a vulnerability in a system.
B) The likelihood that a system will be attacked by a malicious actor.
C) The impact of a security breach on the organization.
D) The cost of implementing security controls to mitigate a security threat.

[4] Answer: C) The impact of a security breach on the organization.

5. Which of the following is not a common type of threat to information systems?
A) Human error
B) Malware attacks
C) Natural disasters
D) Commercial espionage

[5] Answer: C) Natural disasters

6. Which of the following is considered a technical vulnerability in an information system?
A) Insufficient policies or procedures
B) Weak passwords or lack of password policies
C) Lack of employee training and awareness
D) Social engineering attacks

[6] Answer: B) Weak passwords or lack of password policies

7. Which of the following is the best way to mitigate a vulnerability in an information system?
A) Removing the vulnerability altogether
B) Transferring the vulnerability to a third party
C) Reducing the likelihood of exploitation
D) Doing nothing and accepting the risk

[7] Answer: A) Removing the vulnerability altogether

8. What is the most significant difference between a threat agent and a vulnerability?
A) A threat agent is an attacker, while a vulnerability is a weakness or gap.
B) A threat agent is a security control, while a vulnerability is a security risk.
C) A threat agent is a security vulnerability, while a vulnerability is a security threat.
D) A threat agent and vulnerability are synonymous terms with the same meaning.

[8] Answer: A) A threat agent is an attacker, while a vulnerability is a weakness or gap.

9. Which of the following is not a common type of vulnerability in an information system?
A) Physical security vulnerabilities
B) Personnel security vulnerabilities
C) Hardware security vulnerabilities
D) Static security vulnerabilities

[9] Answer: D) Static security vulnerabilities

10. Which of the following is the best way to mitigate the risk of a security breach in an information system?
A) Implementing technical security controls
B) Providing employee training and awareness
C) Developing security policies and procedures
D) All of the above

[10] Answer: D) All of the above

Area-2 : Data Security Policies/Administration Security and Design secure systems

11. What is a data security policy?
A) A plan for securing physical infrastructure
B) A document outlining procedures and guidelines for protecting sensitive data
C) A set of regulations governing the transmission of information
D) A tool used to monitor user activity on a network

[11] Answer: B) A document outlining procedures and guidelines for protecting sensitive data

12. Which of the following is NOT an element of a data security policy?
A) Password policies
B) Access controls
C) Disaster recovery procedures
D) Marketing strategies

[12] Answer: D) Marketing strategies

13. What type of security is concerned with protecting an organization's physical assets?
A) Network security
B) Information security
C) Physical security
D) Operational security

[13] Answer: C) Physical security

14. Which of the following is NOT a common type of access control?
A) Mandatory access control (MAC)
B) Discretionary access control (DAC)
C) Role-based access control (RBAC)
D) Cryptographic access control (CAC)

[14] Answer: D) Cryptographic access control (CAC)

15. What is administration security?
A) A technical control that prevents unauthorized access to data
B) The management of people, processes, and technology used to administer a system
C) A physical control that limits access to a building or facility
D) A type of encryption used to protect communication between servers

[15] Answer: B) The management of people, processes, and technology used to administer a system

16. Which of the following is NOT a step in designing secure systems?
A) Identifying threats and risks
B) Selecting the most popular technology solutions
C) Defining security requirements
D) Evaluating and testing security controls

[16] Answer: B) Selecting the most popular technology solutions

17. What is the purpose of security testing in system design?
A) To identify vulnerabilities and assess the effectiveness of security controls
B) To ensure that the system meets all functional requirements
C) To improve system performance by optimizing resource utilization
D) To reduce maintenance costs and improve system uptime

[17] Answer: A) To identify vulnerabilities and assess the effectiveness of security controls

18. Which of the following is NOT an example of a security control?
A) Firewalls
B) Intrusion Detection Systems (IDS)
C) Password policies
D) Social media marketing strategies

[18] Answer: D) Social media marketing strategies

19. What is the best practice for managing passwords?
A) Using complex passwords that are difficult to remember
B) Sharing passwords with trusted colleagues to save time
C) Changing passwords every month
D) Using a combination of length, complexity, and uniqueness for passwords

[19] Answer: D) Using a combination of length, complexity, and uniqueness for passwords

20. What is the purpose of encryption in information security?
A) To protect data from unauthorized access and modifications
B) To limit access to a building or facility
C) To monitor user activity on a network
D) To reduce the risk of data loss or corruption

[20] Answer: A) To protect data from unauthorized access and modifications

21. What is the term for the process of identifying and prioritizing risks to information assets?
A) Risk assessment
B) Vulnerability analysis
C) Penetration testing
D) Incident response

[21] Answer: A) Risk assessment

22. What is two-factor authentication?
A) A security process that uses a password and a security question to verify user identities
B) A security process that uses a fingerprint scan and a retina scan to verify user identities
C) A security process that requires users to provide two forms of identification to access a system
D) A security process that uses two different devices or methods to verify a user's identity, such as a password and a security token

[22] Answer: D) A security process that uses two different devices or methods to verify a user's identity, such as a password and a security token

23. What is the function of a firewall in network security?
A) To encrypt data transmissions between servers
B) To detect and prevent unauthorized access to a network
C) To authenticate user identities
D) To monitor user activity on a network

[23] Answer: B) To detect and prevent unauthorized access to a network

24. What is the process of removing data from a storage device so that it cannot be recovered?
A) Data encryption
B) Data destruction
C) Data backup
D) Data retention

[24] Answer: B) Data destruction

25. What is the term for a person who identifies and exploits vulnerabilities in computer systems for unauthorized access or malicious purposes?
A) Hacker
B) Whistleblower
C) Security analyst
D) Network administrator

[25] Answer: A) Hacker

Area-3 Information Systems Security concepts

26. What is the primary goal of information security?
A) To protect against all possible threats and risks to information and information systems
B) To ensure that all information is classified and labeled correctly
C) To prevent unauthorized access, use, disclosure, modification, or destruction of information
D) To encrypt all information to prevent interception and decryption by unauthorized individuals

[26] Answer: C) To prevent unauthorized access, use, disclosure, modification, or destruction of information

27. What is the term for a program that is designed to cause harm to a computer system?
A) Virus
B) Trojan
C) Worm
D) Malware

[27] Answer: D) Malware

28. What is the least privilege principle in information security?
A) Granting users access to all resources by default
B) Limiting user access to only the resources needed to perform their job functions
C) Allowing users to access any resource upon request
D) Granting users access to resources based on their seniority within the organization

[28] Answer: B) Limiting user access to only the resources needed to perform their job functions

29. Which of the following is an example of a physical security control?
A) Firewalls
B) Intrusion Detection Systems (IDS)
C) Biometric authentication
D) Encryption

[29] Answer: C) Biometric authentication

30. Which of the following is a best practice for password security?

A) Using the same password for multiple accounts
B) Sharing passwords with coworkers or friends
C) Changing passwords regularly
D) Using short and simple passwords

[30] Answer: C) Changing passwords regularly

31. In information security, what is the CIA triad?
A) Confidentiality, Integrity, Availability
B) Control, Identification, Authorization
C) Compliance, Implementation, Assessment
D) Cybersecurity, Infrastructure, Access control

[31] Answer: A) Confidentiality, Integrity, Availability

32. What is multi-factor authentication?
A) A security process that uses multiple passwords to verify a user's identity
B) A security process that uses a password and a fingerprint scan to verify a user's identity
C) A security process that requires users to provide multiple forms of identification to access a system
D) A security process that uses strong encryption to protect sensitive data

[32] Answer: C) A security process that requires users to provide multiple forms of identification to access a system

33. What is the difference between a vulnerability and an exploit?
A) A vulnerability is a potential weakness in a system, while an exploit is a way to take advantage of that weakness.
B) A vulnerability is a type of malware, while an exploit is a type of attack.
C) A vulnerability is a software bug, while an exploit is a hardware defect.
D) A vulnerability is an intentional weakness introduced by a developer, while an exploit is a way to leverage that weakness for gain.

[33] Answer: A) A vulnerability is a potential weakness in a system, while an exploit is a way to take advantage of that weakness.

34. What is the process of converting plaintext into ciphertext?
A) Decryption
B) Authentication
C) Authorization
D) Encryption

[34] Answer: D) Encryption

35. Which of the following is an example of a social engineering attack?
A) A phishing email that tricks a user into divulging their login credentials
B) A distributed denial of service (DDoS) attack that overwhelms a server with traffic
C) A buffer overflow attack that crashes a system by exploiting a software vulnerability
D) A man-in-the-middle attack that intercepts and alters data transmissions between two parties

[35] Answer: A) A phishing email that tricks a user into divulging their login credentials