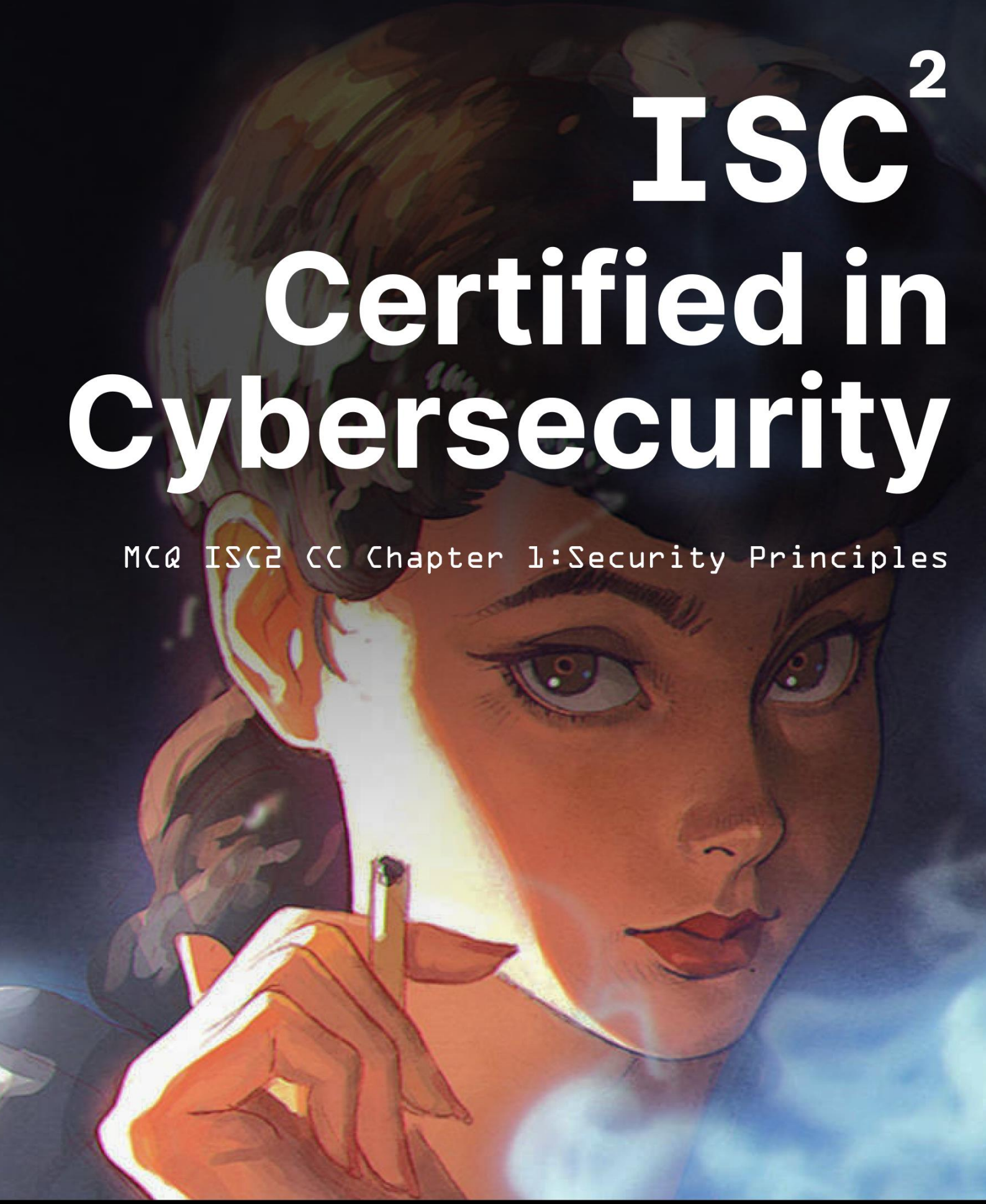

ISC² Certified in Cybersecurity

MCQ ISC2 CC Chapter 1:Security Principles

Based on documentation by WAN MUHAMMAD AZIM BIN WAN MOHD HAZAN AMRI

7/11/2022

Disclaimer

I used Claude.ai to make this MCQ practice exam by referencing Wan Azim's documentation of ISC2 CC. Claude.ai is used to extract information and create questions alongside their answers.

Huge thanks to Wan Azim for documenting the ISC2 Certified in Cybersecurity course!
For more write-ups or documentation check out my repo at:
https://github.com/MikhailAmzar/reports

Security Principles (50)

1. What are the three components of the CIA Triad?
A. Confidentiality, Integrity, Availability
B. Control, Implement, Audit
C. Cryptography, Identity, Authentication
D. Compliance, Investigation, Administration

2. Which of the following best describes the concept of integrity in information security?
A. Permitting authorized access to information
B. Ensuring systems and data are accessible when needed
C. Protecting information from improper disclosure
D. Maintaining completeness, accuracy, and consistency of data

3. What does PII stand for?
A. Private Internet Information
B. Personally Identifiable Information
C. Protected Internal Intelligence
D. Public Infrastructure Information

4. Which of the following is NOT considered a common method of authentication?
A. Something you know
B. Something you have
C. Something you are
D. Something you believe

5. What is the primary goal of non-repudiation?
A. To encrypt data during transmission
B. To ensure individuals cannot deny their actions
C. To prevent unauthorized access to systems
D. To maintain data integrity

6. What is the difference between single-factor authentication (SFA) and multi-factor authentication (MFA)?
A. SFA uses one factor, while MFA uses two or more factors
B. SFA is more secure than MFA
C. MFA is only used for low-security systems
D. There is no difference between the two

7. Which of the following best describes privacy in information security?
A. The right of an organization to collect data without restrictions
B. The right of an individual to control the distribution of information about themselves
C. The process of anonymizing all collected data
D. The ability to keep all information confidential

8. What does GDPR stand for?
A. Global Data Protection Regulation
B. General Data Privacy Rules
C. General Data Protection Regulation
D. Governance Data Policy Requirements

9. In the context of cybersecurity, what is an asset?
A. Only tangible items owned by an organization
B. Only intangible items owned by an organization
C. Anything of value owned by an organization
D. Exclusively the organization's financial resources

10. What is a vulnerability in information security?
A. A person or thing that exploits weaknesses
B. A gap or weakness in protection efforts
C. The level of risk an organization is willing to accept
D. The process of identifying threats

11. Which of the following is NOT typically considered a threat actor?
A. Insiders
B. Cybercriminals
C. Security professionals
D. Nation-states

12. What is the primary purpose of risk assessment?
A. To eliminate all risks
B. To identify, estimate, and prioritize risks
C. To implement security controls
D. To achieve regulatory compliance

13. Which of the following is NOT a common option for risk treatment?
A. Risk avoidance
B. Risk acceptance
C. Risk mitigation
D. Risk elimination

14. What does risk transference typically involve?
A. Ignoring the risk
B. Implementing controls to reduce the risk
C. Purchasing insurance
D. Ceasing the risky activity

15. What tool can be used to help prioritize risks based on likelihood and impact?
A. Risk elimination matrix
B. Risk acceptance chart
C. Risk mitigation table
D. Risk matrix

16. Which factor does NOT typically influence an organization's risk tolerance?
A. Geographic location
B. Industry regulations
C. Number of employees
D. Business objectives

17. What are physical controls in information security?
A. Policies and procedures
B. Firewalls and intrusion detection systems
C. Badge readers and security guards
D. Encryptions and access control lists

18. Which of the following is an example of a technical control?
A. Security policy
B. Security awareness training
C. Access control system
D. Physical barriers

19. What is the primary purpose of administrative controls?
A. To prevent unauthorized physical access
B. To manage the behaviour of personnel
C. To detect network intrusions
D. To encrypt sensitive data

20. Which of the following best describes governance in an organization?
A. The process of how an organization is managed
B. The technical implementation of security controls
C. The physical security measures in place
D. The process of responding to security incidents

21. What is the relationship between laws, regulations, standards, and policies?
A. They are all the same thing
B. Laws inform regulations, which guide standards, which shape policies
C. Policies dictate laws, which create regulations and standards
D. Standards create laws, which inform policies and regulations

22. Which U.S. law governs the use of protected health information (PHI)?
A. GDPR
B. HIPAA
C. SOX
D. PCI-DSS

23. What does NIST stand for?
A. National Information Security Team
B. National Institute of Standards and Technology
C. National Infrastructure and Security Taskforce
D. Network and Information Systems Tribunal

24. What is the primary difference between policies and procedures?
A. Policies are high-level guidelines, while procedures are detailed steps
B. Procedures are high-level guidelines, while policies are detailed steps
C. Policies are only for executives, while procedures are for regular employees
D. There is no difference between policies and procedures

25. According to the $(ISC)^2$ Code of Ethics, information security professionals have a duty to protect:
A. Only their employer
B. Only their clients
C. Society, the common good, and the infrastructure
D. Only themselves and their colleagues

26. What does adequate security mean?
A. Implementing all possible security controls
B. Security commensurate with the risk and magnitude of potential harm
C. Following a specific set of best practices
D. Achieving 100% protection against all threats

27. What is the purpose of a security baseline?
A. To define the highest level of security possible
B. To document the lowest level of security configuration allowed
C. To list all known vulnerabilities
D. To identify all assets in an organization

28. What is a bot in the context of information security?
A. A helpful automated program
B. A physical robot used for security
C. Malicious code acting like a remote-controlled "robot" for an attacker
D. A type of authentication token

29. What does the term "criticality" refer to in information security?
A. The negative attitude of employees towards security
B. The degree to which an organization depends on information or systems
C. The number of vulnerabilities in a system
D. The complexity of the IT infrastructure

30. What is the primary goal of encryption?
A. To make data unreadable to unauthorized parties
B. To reduce the size of data for efficient storage
C. To increase the speed of data transmission
D. To create multiple copies of data for redundancy

31. What are the three factors commonly used for authentication?
A. Who you are, what you do, where you are
B. Something you know, something you have, something you are
C. Username, password, PIN
D. Biometrics, smart cards, security questions

32. Which of the following best describes non-repudiation?
A. The ability to deny sending a message
B. The inability to deny taking an action
C. The process of deleting audit trails
D. The method of using fake identities online

33. What is the primary difference between qualitative and quantitative risk analysis?
A. Qualitative uses descriptors like high/medium/low, while quantitative uses numerical values
B. Qualitative is more accurate than quantitative
C. Quantitative is always preferred over qualitative
D. There is no significant difference between the two

34. What does IETF stand for?
A. International Encryption Task Force
B. Internet Engineering Task Force
C. Information Evaluation and Testing Facility
D. Integrated Emergency Task Force

35. Which of the following is NOT a step in the risk management process?
A. Risk identification
B. Risk assessment
C. Risk treatment
D. Risk perpetuation

36. What is the purpose of the $(ISC)^2$ Code of Ethics Preamble?
A. To list all possible ethical violations
B. To state the purpose and intent of the Code of Ethics
C. To provide a detailed guide for ethical decision making
D. To outline punishment for ethical breaches

37. What does "authorization" refer to in information security?
A. The process of verifying a user's identity
B. The right or permission granted to access a system resource
C. The process of encrypting data transmissions
D. The method of creating strong passwords

38. Which statement best describes the difference between a threat and a vulnerability?
A. A threat exploits a vulnerability; a vulnerability is a weakness that can be exploited
B. A threat is internal; a vulnerability is always external
C. A vulnerability is a person; a threat is a software bug
D. There is no difference; the terms are interchangeable

39. What is a key characteristic of technical controls?
A. They are primarily implemented through the information system itself
B. They never require human intervention
C. They are always physical in nature
D. They are only used in high-security environments

40. According to the CIA triad, what does availability mean?
A. Information is accessible only to authorized parties
B. Information is accurate and consistent
C. Systems and data are accessible when needed by authorized users
D. All systems are operational 24/7 without any downtime

41. What is the main goal of privacy legislation?
A. To prohibit companies from collecting any personal data
B. To control the collection, use, and distribution of personal information
C. To make all personal information publicly available
D. To increase government surveillance capabilities

42. Which factor does NOT typically contribute to the likelihood of a risk occurring?
A. Threat capability
B. Nature of the vulnerability
C. Existing controls
D. The CEO's personality

43. What is risk appetite?
A. The level of risk an entity is willing to assume to achieve a desired result
B. The total number of risks an organization faces
C. The process of identifying new risks
D. The speed at which new risks emerge

44. Which of the following is an example of an administrative control?
A. Firewall
B. Security policy
C. Mantrap
D. Encryption

45. What is the primary purpose of separation of duties?
A. To ensure that no single person can abuse their powers
B. To create more job positions in an organization
C. To reduce the efficiency of business processes
D. To increase the workload of employees

46. What does defense in depth refer to?
A. Using only the most expensive security solutions
B. Implementing multiple layers of security controls
C. Protecting only the most critical assets
D. Employing armed guards at all entry points

47. Which statement best describes the purpose of security awareness training?
A. To make employees fearful of security threats
B. To reduce the workload of the IT security team
C. To help employees recognize and respond to security threats
D. To teach all employees to become security experts

48. What is social engineering?
A. The process of designing secure social media platforms
B. A method of manipulating people into divulging confidential information
C. The practice of building secure physical infrastructure
D. A technique for developing secure social networks within an organization

49. What is the primary goal of business continuity planning?
A. To ensure that critical business functions can continue during and after a disaster
B. To maximize profits during normal operations
C. To reduce day-to-day operational costs
D. To improve employee satisfaction

50. Which of the following best describes the principle of least privilege?
A. Users should be given minimum levels of access needed to perform their jobs
B. All users should have equal access to all resources
C. Administrators should have access to all systems at all times
D. Employees should not be privileged with any access to IT systems