ISC^2

Certified in Cybersecurity

MCQ ISC2 CC Chapter 3:Access Control Concepts

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

Access Control Concepts

Here is a 50-question exam covering the main topics from Chapter 3: Access Control Concepts

1. What is the primary purpose of a security control?
A. To increase system performance
B. To preserve the CIA Triad
C. To reduce operational costs
D. To simplify user interfaces

2. Access control primarily involves:
A. Limiting what objects can be available to what subjects according to what rules
B. Increasing the speed of data transmission
C. Enhancing user experience
D. Automating all security processes

3. Which of the following is an example of a subject in access control?
A. A building
B. A user
C. A printer
D. A database

4. An object in access control is characterized as:
A. Active
B. Passive
C. Both active and passive
D. Neither active nor passive

5. What is the primary function of an access rule?
A. To initiate system backups
B. To allow or deny access to an object
C. To increase network bandwidth
D. To design user interfaces

6. Defence in depth describes:
A. A single, strong security measure
B. An information security strategy integrating multiple layers
C. A physical barrier around the data center
D. A type of firewall configuration

7. What is the Principle of Least Privilege?
A. Granting users all possible permissions
B. Permitting only minimum access necessary for users to fulfill their function
C. Allowing unrestricted access to all resources
D. Providing the same level of access to all users

8. What is an example of the Principle of Least Privilege in healthcare?
A. All staff have access to all patient records
B. Doctors have access only to data related to their own patients
C. Receptionists have full access to medical data
D. Nurses can modify any patient's prescription

9. What is Privileged Access Management?
A. Giving all users administrative rights
B. Removing all access restrictions
C. Managing access rights of users with elevated privileges
D. Ignoring user roles in access control

10. Which of the following is a typical measure for moderating risks from privileged accounts?
A. Less extensive logging
B. More stringent access control
C. Minimal background checks
D. Reduced auditing

11. What is segregation of duties based on?
A. The practice that one person should control an entire high-risk transaction
B. The security practice that no one person should control an entire high-risk transaction from start to finish
C. Assigning all duties to a single individual
D. Avoiding the distribution of responsibilities

12. What is an example of segregation of duties?
A. One person submits and approves all invoices
B. The same employee submits an invoice, approves it, and processes the payment
C. An employee submits an invoice, but a manager must approve it before payment
D. All employees have the authority to approve any invoice

13. What is the two-person rule?
A. A security strategy requiring a minimum of two people in an area together
B. A rule allowing individuals to work alone in high-security areas
C. A policy that limits all teams to two people
D. A guideline for hiring practices

14. Physical access controls are:
A. Intangible mechanisms
B. Items you can physically touch
C. Purely software-based solutions
D. Theoretical concepts

15. Why are physical access controls necessary?
A. To increase productivity
B. To reduce utility costs
C. To protect assets, including people
D. To improve aesthetic appeal

16. Which of the following is an example of a physical access control?
A. Firewall
B. Antivirus software
C. Locked doors
D. Password policy

17. What does CPTED stand for?
A. Computer Programming Technique for Electronic Devices
B. Crime Prevention Through Environmental Design
C. Centralized Protocol for Threat Evaluation and Detection
D. Critical Path to Enterprise Development

18. What is a primary goal of CPTED?
A. To increase criminal activity
B. To create safer workspaces through passive design elements
C. To eliminate the need for security personnel
D. To reduce construction costs

19. Which of the following is a form of biometric authentication?
A. Password
B. Security token
C. Fingerprint scan
D. Key fob

20. What are the two primary forms of biometrics?
A. Digital and analog
B. Hardware and software
C. Physiological and behavioral
D. Internal and external

21. Which of the following is an example of behavioral biometrics?
A. Fingerprint
B. Retinal scan
C. Voiceprint
D. Palm scan

22. What is a potential drawback of biometric systems?
A. They are inexpensive to implement
B. Users may consider them an invasion of privacy
C. They are highly inaccurate
D. They require no maintenance

23. What is the primary purpose of security cameras?
A. To improve video quality
B. To provide flexible surveillance and monitoring
C. To increase internet bandwidth
D. To replace all other security measures

24. What is the main function of an alarm system?
A. To play music
B. To control room temperature
C. To alert appropriate personnel when unexpected events occur
D. To increase property value

25. Why are physical security logs essential?
A. To support marketing initiatives
B. To improve system performance
C. To support business requirements and potential legal needs
D. To entertain security personnel

26. What is a log anomaly?
A. A normal, everyday occurrence
B. Anything out of the ordinary in a log
C. A type of computer virus
D. A software bug

27. Logical access controls are:
A. Tangible methods limiting physical access
B. Electronic methods limiting access to systems
C. Always ineffective
D. Obsolete security measures

28. Which of the following is an example of a logical access control?
A. Security guard
B. Fence
C. Password
D. Locked door

29. In Discretionary Access Control (DAC), who typically controls access to an object?
A. System administrator only
B. Government regulators
C. The object's owner
D. Random users

30. What type of access control policy is enforced over all subjects and objects in Mandatory Access Control (MAC)?
A. A flexible policy
B. A user-defined policy
C. A uniformly enforced policy

D. No policy

31. In a MAC system, who can modify the security rules?
A. Any user
B. Only designated security administrators
C. All employees
D. External consultants

32. What does RBAC stand for?
A. Remote Backup Access Control
B. Role-Based Access Control
C. Relational Database Access Control
D. Restricted Bandwidth Access Control

33. How are user permissions set up in RBAC?
A. Based on seniority
B. Based on roles
C. Randomly assigned
D. Always set to maximum privileges

34. What is "privilege creep"?
A. A type of computer virus
B. A gradual increase in access rights beyond what is needed
C. A method for granting privileges quickly
D. A way to restrict all user access

35. What is defence in depth?
A. A single layer of security
B. A strategy integrating multiple layers of security
C. A physical defensive wall
D. A type of encryption algorithm

36. Which of the following is an example of defence in depth?
A. Using only a username for authentication
B. Implementing a single firewall
C. Using multi-factor authentication
D. Granting all users administrative privileges

37. What is the primary difference between Discretionary Access Control (DAC) and Mandatory Access Control (MAC)?
A. DAC is always more secure than MAC
B. MAC is always more user-friendly than DAC
C. In DAC, the object owner has discretion over access; in MAC, access is mandated by central authority
D. There is no difference between the two

38. In Role-Based Access Control (RBAC), what does each role represent?
A. Users with different permissions

B. Users with similar or identical permissions
C. Only managers
D. Only entry-level employees

39. What is an access control list primarily used for?
A. To show which subjects have permissions for a specific object
B. To list all employees in alphabetical order
C. To track vacation days
D. To assign parking spots

40. What should be the first consideration when implementing physical access controls?
A. Cost
B. Aesthetics
C. Security of personnel
D. Compatibility with existing systems

41. What is a potential issue with extensive logging?
A. It provides too little information
B. It can lead to information overload
C. It is always 100% accurate
D. It requires no storage space

42. What is the main purpose of a mantrap in physical security?
A. To catch insects
B. To provide a resting area for security guards
C. To control access to a restricted area
D. To improve office decor

43. Which of the following is a characteristic of a good access control system?
A. It grants everyone the same level of access
B. It is highly complex and difficult to use
C. It allows access based on the principle of least privilege
D. It requires no maintenance or updates

44. What does "need-to-know" refer to in access control?
A. Granting access to all information
B. Restricting access to only the information required for one's work
C. A type of security software
D. A method for encrypting data

45. Which type of access control is typically the most granular?
A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Role-Based Access Control (RBAC)
D. Rule-Based Access Control

46. What is tailgating in the context of physical security?
A. Following too closely while driving

B. A method of secure coding
C. Following an authorized person through a secure entrance without permission
D. A technique for backing up data

47. What is social engineering?
A. A branch of sociology
B. The use of deception to manipulate individuals into divulging confidential information
C. A method for designing social networks
D. A team-building exercise

48. Which of the following is true about authentication?
A. It's the same as authorization
B. It's the process of verifying the identity of a user or system
C. It's only necessary for low-security systems
D. It's a one-time process that never needs to be repeated

49. What is non-repudiation in information security?
A. The ability of a system to grow with increased demands
B. The assurance that someone cannot deny the validity of something
C. A type of encryption algorithm
D. A method for password recovery

50. What is the primary goal of an information security program?
A. To make systems completely unhackable
B. To eliminate all risks
C. To preserve the confidentiality, integrity, and availability of information
D. To reduce the need for employee training

Answer Key: Chapter 3

1. B
2. A
3. B
4. B
5. B
6. B
7. B
8. B
9. C
10. B
11. B
12. C
13. A
14. B
15. C
16. C
17. B
18. B
19. C
20. C
21. C
22. B
23. B
24. C
25. C
26. B
27. B
28. C
29. C
30. C
31. B
32. B
33. B
34. B
35. B
36. C
37. C
38. B
39. A
40. C
41. B
42. C
43. C
44. B
45. C
46. C
47. B
48. B
49. B
50. C