

Management 414: SANS CISSP® 10 Domains +S QUIZ-Domain 10

1. What security control is most often overlooked?
 - a) Physical security
 - b) Technical security
 - c) Administrative security
 - d) Personnel security
2. Information security has been aligned toward the accomplishment of three objectives: Confidentiality, Integrity, and:
 - a) Assurance
 - b) Availability
 - c) Accomplishment
 - d) Measurability
3. Which of the following objectives does the physical security realm include besides the Confidentiality, Integrity, and Availability (CIA) model?
 - a) Security
 - b) Safety
 - c) Assurance
 - d) Logistics
4. What is the top priority when physical security measures are implemented?
 - a) Confidentiality
 - b) Safety
 - c) Availability
 - d) Integrity
5. When implementing evacuation procedures, which of the following should be included?
 - a) Servers to shut down
 - b) Meeting points
 - c) Backup tapes to acquire
 - d) Locking file cabinets
6. When designing emergency procedure signage that you plan on posting throughout your organization, what color is recommended?
 - a) Red
 - b) Yellow
 - c) Brown
 - d) Blue
7. Who is responsible for beginning the process of accounting for all employees in the case of evacuation?
 - a) Safety Warden
 - b) Meeting Point Leader

Management 414: SANS CISSP® 10 Domains +S QUIZ-Domain 10

- c) Technical Manager
 - d) Employee
8. Who is responsible for checking that each individual in his or her area has begun evacuation?
- a) Meeting Point Leader
 - b) Safety Warden
 - c) Employee
 - d) Technical Manager
9. Which of the following is the association of a unique identity with an individual presenting himself unknowingly or knowingly to an access control system?
- a) Identification
 - b) Authentication
 - c) Authorization
 - d) Integrity
10. Which of the following is the confirmation that an individual is who she claims to be?
- a) Authorization
 - b) Identification
 - c) Authentication
 - d) Integrity
11. Which of the following is the determination of the functions or activities that an individual is permitted to perform?
- a) Authorization
 - b) Authentication
 - c) Identification
 - d) Accounting
12. Which of the following is considered a deterring physical control?
- a) Locks
 - b) Fences
 - c) Guards
 - d) Mantraps
13. Which of the following is considered a preventative physical control?
- a) Guards
 - b) Motion Detector
 - c) Security lights
 - d) Locks

Management 414: SANS CISSP® 10 Domains +S QUIZ-Domain 10

14. Which of the following is considered a detective physical control?
 - a) Fences
 - b) Guards
 - c) Security lights
 - d) Mantraps

15. How many feet high should a fence be to deter a determined intruder?
 - a) 8 feet
 - b) 6 feet
 - c) 3 feet
 - d) 2 feet

16. Which of the following is a drawback in using dogs to maintain physical security?
 - a) Easy to maintain
 - b) Low in cost
 - c) Liability issues
 - d) Reliable

17. With regard to biometric access control, what is a False Reject Rate (FRR) Type I error?
 - a) Percent of authentic persons rejected as unidentified
 - b) Percent of impostors accepted as authentic
 - c) Percent at which all is considered equal
 - d) False acceptance

18. What is the appropriate temperature range for system reliability and operator comfort?
 - a) 60-64F
 - b) 70-74F
 - c) 64-68F
 - d) 75-79F

19. What CANNOT be used to suppress a Class B fire?
 - a) Halon
 - b) CO₂
 - c) Soda Acid
 - d) Water

20. What CANNOT be used to suppress a Class C fire?
 - a) Soda Acid
 - b) Gas
 - c) CO₂

21. Which of the following principles below is the need to ensure that information is disclosed only to those who are authorized to view the information?
- a) Integrity
 - b) Confidentiality
 - c) Availability
 - d) Safety
22. What is the top priority when working with physical security?
- a) Confidentiality
 - b) Integrity
 - c) Safety
 - d) Availability
23. Which type of controls are designed to ensure that unauthorized personnel do not have the capability to enter restricted areas?
- a) Deterrent
 - b) Detective
 - c) Corrective
 - d) Preventive
24. Which of the following is considered a preventive physical control?
- a) Fences
 - b) Guards
 - c) Security Lights
 - d) Mantrap
25. Which of the following is considered a detective physical control?
- a) Mantrap
 - b) Closed Circuit Television (CCTV)
 - c) Fences
 - d) Locks
26. Which of the following is meant to simply deter casual trespassers?
- a) 6-7 foot fences
 - b) 3-4 foot fences
 - c) 8 foot fences
 - d) 1-2 foot fences
27. What is the most common means of putting out a class A fire?
- a) Halon
 - b) Gas
 - c) Water
 - d) Soda Acid

Management 414: SANS CISSP® 10 Domains +5 QUIZ-Domain 10

28. When talking about biometric access controls, which of the following is a Type I error?
- a) False reject rate
 - b) Crossover error rate
 - c) False accept rate
29. Which of the following refers to an error where the percent of unenrolled or impostors are accepted as authentic?
- a) Type II error
 - b) Crossover error rate
 - c) Type I error
30. Which of the following is considered a Class B fire?
- a) Liquid such as coolants
 - b) Electrical such as wires
 - c) Common combustibles such as wood products
31. Which of the following information security objectives refers to the need to ensure that the business purpose of the system can be met?
- a) Safety
 - b) Integrity
 - c) Confidentiality
 - d) Availability
32. Which of the following information security objectives refers to the need to ensure that the information is not disclosed to unauthorized parties?
- a) Safety
 - b) Integrity
 - c) Availability
 - d) Confidentiality
33. Threats such as smoke and fire, toxins, and water/flood fall under which of the following categories of security?
- a) Corporate Security
 - b) Equipment security
 - c) Access security
 - d) Physical security
34. Which of the following choices is NOT an access control type?
- a) Reactive
 - b) Corrective
 - c) Preventive
 - d) Deterrent

Management 414: SANS CISSP® 10 Domains +5 QUIZ-Domain 10

35. There are several drawbacks when using security guards. Given the choices below, which is NOT a drawback?
- a) Cost
 - b) Deterrent
 - c) Training
 - d) Reliability
 - e) Availability
36. Which of the following biometric access control choices measures the blood vessels of the eye?
- a) Fingerprint
 - b) Facial recognition
 - c) Iris scan
 - d) Retina pattern
37. In most situations, if you had to pick a type of error, which of the following choices would you pick?
- a) Internal error rate
 - b) Type I error
 - c) Crossover error rate
 - d) Type II error
38. Which of the following biometric access control techniques has the quickest response time and lowest Crossover error rate?
- a) Voice pattern
 - b) Iris scan
 - c) Palm scan
 - d) Hand geometry
39. Which of the following classes of fires is the most common?
- a) Class D
 - b) Class C
 - c) Class A
 - d) Class B