

**Management 414: SANS CISSP® 10 Domains +S QUIZ—Domain 4**

1. Which of the following is NOT a recommended consideration pertaining to application controls?
  - a) Potential risk
  - b) End-user opinion
  - c) Available controls
  - d) Environment type
2. Which type of environment has everything organized, controlled and performed from one location?
  - a) Decentralized
  - b) Distributed
  - c) Centralized
  - d) Compartmentalized
3. Which type of environment has multiple independent locations with little or no communications between the entities?
  - a) Centralized
  - b) Decentralized
  - c) Distributed
  - d) Compartmentalized
4. In the context of Object Oriented Systems, which of the following best describes an object?
  - a) A function or set of functions accessible only through its Application Program Interfaces (API)
  - b) A 'black box' that receives and sends messages
  - c) A code module that publishes both its code and data
  - d) A code subroutine that contains both code and data
5. Which type of environment has communication and coordination between multiple locations?
  - a) Distributed
  - b) Centralized
  - c) Decentralized
  - d) Compartmentalized
6. Which of the following is NOT a mode of operation?
  - a) System High Mode
  - b) Compartment Mode
  - c) System Low Mode
  - d) Multi-level Secure Mode
7. Which of the following modes is relatively simple and can be implemented with most operating systems?
  - a) System High Mode
  - b) Compartment Mode

**Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 4**

- c) Security Mode
  - d) Decompartment Mode
8. What is the method ActiveX relies on for security?
- a) NTLM
  - b) Symmetrical encryption
  - c) Digital signatures
  - d) Sand-boxing
9. What is the main reason to consider security in the change control process?
- a) To ensure that changes are securely recoded, tested and documented
  - b) To ensure that id, control and configuration audit is performed in a secure manner
  - c) To ensure that release, archiving and acceptance testing is performed securely
  - d) To ensure that security mechanisms are not negatively impacted by the proposed changes
10. At which critical step in the development process does the project manager expect to see the security risks defined?
- a) Design analysis
  - b) System design specifications
  - c) Project initiation
  - d) Installation
11. One of the most commonly exploited security vulnerabilities - buffer overflows - are addressed in which phase of the development process?
- a) System design specification
  - b) Design analysis
  - c) Operation and maintenance
  - d) Programming and testing
12. What is the main concern with simply deleting files during the destruction phase of the development process?
- a) There is no concern.
  - b) Deleted data can still be extracted from hard drives.
  - c) Deleted data still uses up a small portion of the capacity of the hard drive.
  - d) Ease dropping
13. Requiring a biometric fingerprint to enter a server room, followed by a username and password at the system console, followed by a pin to access the application, best represents which operational control?
- a) Least privilege
  - b) Continuity of operations
  - c) Layered defense
  - d) Separation of duties

**Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 4**

14. Which software development model has unique, discrete, sequential phases?
  - a) Spiral model
  - b) Top-down model
  - c) Waterfall model
  - d) Bottom-up model
  
15. Which mode of operation is difficult to implement and cannot be done with most operating systems?
  - a) Client/Server Mode
  - b) Compartment Mode
  - c) System High Mode
  - d) System Low Mode
  
16. Which of the following systems can be thought of as a group of independent units that can be requested to perform certain operations or exhibit specific behaviors?
  - a) Role-Based System
  - b) Object-Oriented System
  - c) Access Control System
  - d) Rapid Prototyping System
  
17. Which of the following defines an industry standard that enables programs written in different languages and using different platforms and operating systems to interface and communicate?
  - a) COBRA
  - b) CORBA
  - c) BOA
  - d) DCOM
  
18. There are three commonly used application development methodologies. Which of the following are those three methodologies?
  - a) RAIN, RAD, and RAT
  - b) Traditional, modern, and hybrid
  - c) Open source, closed source, and proprietary
  - d) Waterfall, spiral, and RAD
  
19. What are the characteristics of the Waterfall methodology of application development?
  - a) The project is divided into sequential stages, each with specific milestones
  - b) The phases of the project seamlessly flow from one into the next
  - c) While the project's overall flow is forward, sub-tasks called eddies are spun off as needed
  - d) As design specifications evolve the project is able to adjust and flow forward
  
20. What is the main factor that drives the spiral model of application development?
  - a) Risk
  - b) Cost

- c) Performance
  - d) Availability
21. What is the fundamental characteristic of the Rapid Application Development (RAD) model of application development?
- a) Applications are developed that run very fast
  - b) 75% of all applications are developed this way
  - c) Applications have 25% more functionality
  - d) Applications are developed very quickly
22. What is the basic function of output controls?
- a) That output is complete and accurate
  - b) Protection against unauthorized or accidental output of sensitive data
  - c) Insure that only those who are authorized have access to output
  - d) To maintain audit trails that trace back to the input data
23. What function does a reference monitor perform?
- a) Maintains the referential integrity of sensitive data
  - b) Monitors all references to sensitive data
  - c) Implements the Security Kernel
  - d) Validation of every single access request
24. What principle is violated when developers review implementation details?
- a) Non-disclosure agreement
  - b) Confidentiality
  - c) Separation of duties
  - d) The principle of least privilege
25. What principle can be described as providing users with the minimum level of privilege required to complete a task?
- a) Sand-boxing
  - b) Fixed function authorization
  - c) The principle of least privilege
  - d) Separation of duties
26. What term is used to describe a structured approach to documenting and approving changes to systems?
- a) Operations management
  - b) Change control
  - c) Systems life cycle management
  - d) Segregation of duties
27. What is the name of the application development model in which you start with the lower level details, bundled them into higher level components and finally into a production system?
- a) Bottom-up model
  - b) Object-Oriented model

**Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 4**

- c) Spiral-up model
  - d) Component-mode model
28. What type of software program operates as an agent on behalf of a user or another program?
- a) Bots
  - b) Applets
  - c) Processes
  - d) Bytecode
29. What is one of the most useful ways of addressing the Availability requirement of the CIA definition of security?
- a) Memorandums of Agreement
  - b) Software life cycle management
  - c) Operational integrity procedures
  - d) Service Level Agreements
30. What is it that allows Java to be a cross platform programming language?
- a) Java is executed within a virtual sandbox which is processor independent
  - b) The Java Virtual Machine (JVM) converts the bytecode into machine language for that CPU
  - c) Java applets are compiled into the bytecode specifically for the requesting processor
  - d) The Java Virtual Machine (JVM) is compiled in processor independent bytecode