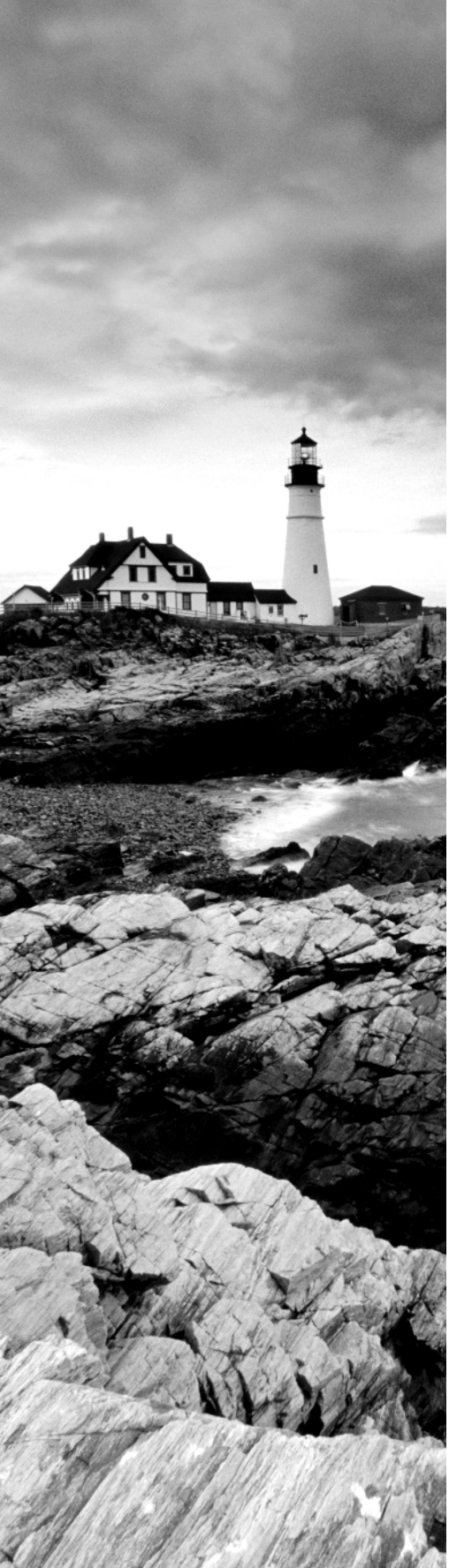
Chapter 1

Security Operations and Administration (Domain 1)

THE SSCP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- ✓ **Domain 1.0: Security Operations and Administration**
  - **1.1 Comply with codes of ethics**
    - $(ISC)^2$ Code of Ethics
    - Organizational code of ethics
  - **1.2 Understand security concepts**
    - Confidentiality
    - Integrity
    - Availability
    - Accountability
    - Privacy
    - Non-repudiation
    - Least privilege
    - Segregation of duties (SoD)
  - **1.3 Identify and implement security controls**
    - Technical controls (e.g., session timeout, password aging)
    - Physical controls (e.g., mantraps, cameras, locks)
    - Administrative controls (e.g., security policies, standards, procedures, baselines)
    - Assessing compliance
    - Periodic audit and review
  - **1.4 Document and maintain functional security controls**
    - Deterrent controls
    - Preventative controls



- Detective controls
- Corrective controls
- Compensating controls

- **1.5 Participate in asset management lifecycle (hardware, software, and data)**
  - Process, planning, design, and initiation
  - Development/Acquisition
  - Inventory and licensing
  - Implementation/Assessment
  - Operation/Maintenance
  - Archiving and retention requirements
  - Disposal and destruction
- **1.6 Participate in change management lifecycle**
  - Change management (e.g., roles, responsibilities, processes)
  - Security impact analysis
  - Configuration management (CM)
- **1.7 Participate in implementing security awareness and training (e.g., social engineering/phishing)**
- **1.8 Collaborate with physical security operations (e.g., data center assessment, badging)**

1. Maddox is conducting an information audit for his organization. Which one of the following elements that he discovered is least likely to be classified as PII when used in isolation?
   - **A.** Street addresses
   - **B.** Item codes
   - **C.** Mobile phone numbers
   - **D.** Social Security numbers

2. Carl recently assisted in the implementation of a new set of security controls designed to comply with legal requirements. He is concerned about the long-term maintenance of those controls. Which one of the following is a good way for Carl to ease his concerns?
   - **A.** Firewall rules
   - **B.** Policy documents
   - **C.** Security standards
   - **D.** Periodic audits

3. Darlene was recently offered a consulting opportunity as a side job. She is concerned that the opportunity might constitute a conflict of interest. Which one of the following sources is most likely to provide her with appropriate guidance?
   - **A.** Organizational code of ethics
   - **B.** $(ISC)^2$ code of ethics
   - **C.** Organizational security policy
   - **D.** $(ISC)^2$ security policy

4. Which one of the following is an administrative control that can protect the confidentiality of information?
   - **A.** Encryption
   - **B.** Nondisclosure agreement
   - **C.** Firewall
   - **D.** Fault tolerance

5. Chris is worried that the laptops that his organization has recently acquired were modified by a third party to include keyloggers before they were delivered. Where should he focus his efforts to prevent this?
   - **A.** His supply chain
   - **B.** His vendor contracts
   - **C.** His post-purchase build process
   - **D.** The original equipment manufacturer (OEM)

6. The $(ISC)^2$ code of ethics applies to all SSCP holders. Which of the following is not one of the four mandatory canons of the code?
   - **A.** Protect society, the common good, the necessary public trust and confidence, and the infrastructure.
   - **B.** Disclose breaches of privacy, trust, and ethics.
   - **C.** Provide diligent and competent service to the principles.
   - **D.** Advance and protect the profession.

7. Which one of the following control categories does not accurately describe a fence around a facility?
   - **A.** Physical
   - **B.** Detective
   - **C.** Deterrent
   - **D.** Preventive

8. Which one of the following actions might be taken as part of a business continuity plan?
   - **A.** Restoring from backup tapes
   - **B.** Implementing RAID
   - **C.** Relocating to a cold site
   - **D.** Restarting business operations

9. Which one of the following is an example of physical infrastructure hardening?
   - **A.** Antivirus software
   - **B.** Hardware-based network firewall
   - **C.** Two-factor authentication
   - **D.** Fire suppression system

10. Mary is helping a computer user who sees the following message appear on his computer screen. What type of attack has occurred?

A. Availability

B. Confidentiality

C. Disclosure

D. Distributed

11. The Acme Widgets Company is putting new controls in place for its accounting department. Management is concerned that a rogue accountant may be able to create a new false vendor and then issue checks to that vendor as payment for services that were never rendered. What security control can best help prevent this situation?

A. Mandatory vacation

B. Separation of duties

C. Defense in depth

D. Job rotation

12. Beth is the security administrator for a public school district. She is implementing a new student information system and is testing the code to ensure that students are not able to alter their own grades. What principle of information security is Beth enforcing?

A. Integrity

B. Availability

C. Confidentiality

D. Denial

For questions 13–15, please refer to the following scenario.

Juniper Content is a web content development company with 40 employees located in two offices: one in New York and a smaller office in the San Francisco Bay Area. Each office has a local area network protected by a perimeter firewall. The local area network (LAN) contains modern switch equipment connected to both wired and wireless networks.

Each office has its own file server, and the information technology (IT) team runs software every hour to synchronize files between the two servers, distributing content between the offices. These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS-based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Juniper Content, and you are working to augment existing security controls to improve the organization's security.

13. Users in the two offices would like to access each other's file servers over the Internet. What control would provide confidentiality for those communications?

A. Digital signatures

B. Virtual private network

C. Virtual LAN

D. Digital content management

14. You are also concerned about the availability of data stored on each office's server. You would like to add technology that would enable continued access to files located on the server even if a hard drive in a server fails. What integrity control allows you to add robustness without adding additional servers?

A. Server clustering

B. Load balancing

C. RAID

D. Scheduled backups

15. Finally, there are historical records stored on the server that are extremely important to the business and should never be modified. You would like to add an integrity control that allows you to verify on a periodic basis that the files were not modified. What control can you add?

A. Hashing

B. ACLs

C. Read-only attributes

D. Firewalls

16. An accounting employee at Doolittle Industries was recently arrested for participation in an embezzlement scheme. The employee transferred money to a personal account and then shifted funds around between other accounts every day to disguise the fraud for months. Which one of the following controls might have best allowed the earlier detection of this fraud?

A. Separation of duties

B. Least privilege

C. Defense in depth

D. Mandatory vacation

17. Yolanda is writing a document that will provide configuration information regarding the minimum level of security that every system in the organization must meet. What type of document is she preparing?

A. Policy

B. Baseline

C. Guideline

D. Procedure

18. Frank discovers a keylogger hidden on the laptop of his company's chief executive officer. What information security principle is the keylogger most likely designed to disrupt?

A. Confidentiality

B. Integrity

C. Availability

D. Denial

19. Susan is working with the management team in her company to classify data in an attempt to apply extra security controls that will limit the likelihood of a data breach. What principle of information security is Susan trying to enforce?

A. Availability

B. Denial

C. Confidentiality

D. Integrity

20. Gary is implementing a new website architecture that uses multiple small web servers behind a load balancer. What principle of information security is Gary seeking to enforce?

A. Denial

B. Confidentiality

C. Integrity

D. Availability

21. Which one of the following is not an example of a technical control?

A. Session timeout

B. Password aging

C. Encryption

D. Data classification

For questions 22–25, please refer to the following scenario.

Jasper Diamonds is a jewelry manufacturer that markets and sells custom jewelry through their website. Bethany is the manager of Jasper's software development organization, and she is working to bring the company into line with industry standard practices. She is developing a new change management process for the organization and wants to follow commonly accepted approaches.

22. Jasper would like to establish a governing body for the organization's change management efforts. What individual or group within an organization is typically responsible for reviewing the impact of proposed changes?

A. Chief information officer

B. Senior leadership team

C. Change control board

D. Software developer

23. During what phase of the change management process does the organization conduct peer review of the change for accuracy and completeness?

A. Recording

B. Analysis/Impact Assessment

C. Approval

D. Decision Making and Prioritization

24. Who should the organization appoint to manage the policies and procedures surrounding change management?

A. Project manager

B. Change manager

C. System security officer

D. Architect

25. Which one of the following elements is not a crucial component of a change request?

A. Description of the change

B. Implementation plan

C. Backout plan

D. Incident response plan

26. Ben is designing a messaging system for a bank and would like to include a feature that allows the recipient of a message to prove to a third party that the message did indeed come from the purported originator. What goal is Ben trying to achieve?

A. Authentication

B. Authorization

C. Integrity

D. Nonrepudiation

27. What principle of information security states that an organization should implement overlapping security controls whenever possible?

A. Least privilege

B. Separation of duties

C. Defense in depth

D. Security through obscurity

28. Which one of the following is not a goal of a formal change management program?

A. Implement change in an orderly fashion.

B. Test changes prior to implementation.

C. Provide rollback plans for changes.

D. Inform stakeholders of changes after they occur.

29. Ben is assessing the compliance of his organization with credit card security requirements. He finds payment card information stored in a database. Policy directs that he remove the information from the database, but he cannot do this for operational reasons. He obtained an exception to policy and is seeking an appropriate compensating control to mitigate the risk. What would be his best option?

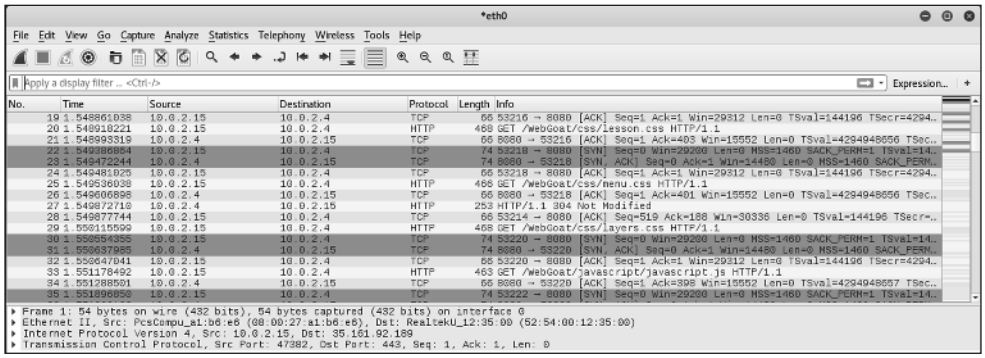
A. Purchasing insurance

B. Encrypting the database contents

C. Removing the data

D. Objecting to the exception

30. You discover that a user on your network has been using the Wireshark tool, as shown here. Further investigation revealed that he was using it for illicit purposes. What pillar of information security has most likely been violated?



A. Integrity

B. Denial

C. Availability

D. Confidentiality

31. Which one of the following is the first step in developing an organization's vital records program?

A. Identifying vital records

B. Locating vital records

C. Archiving vital records

D. Preserving vital records

32. Which one of the following security programs is designed to provide employees with the knowledge they need to perform their specific work tasks?

A. Awareness

B. Training

C. Education

D. Indoctrination

33. Which one of the following security programs is designed to establish a minimum standard common denominator of security understanding?

A. Training

B. Education

C. Indoctrination

D. Awareness

34. Chris is responsible for workstations throughout his company and knows that some of the company's workstations are used to handle proprietary information. Which option best describes what should happen at the end of their lifecycle for workstations he is responsible for?

A. Erasing

B. Clearing

C. Sanitization

D. Destruction

35. What term is used to describe a set of common security configurations, often provided by a third party?

A. Security policy

B. Baseline

C. DSS

D. NIST SP 800-53

36. Which one of the following administrative processes assists organizations in assigning appropriate levels of security control to sensitive information?

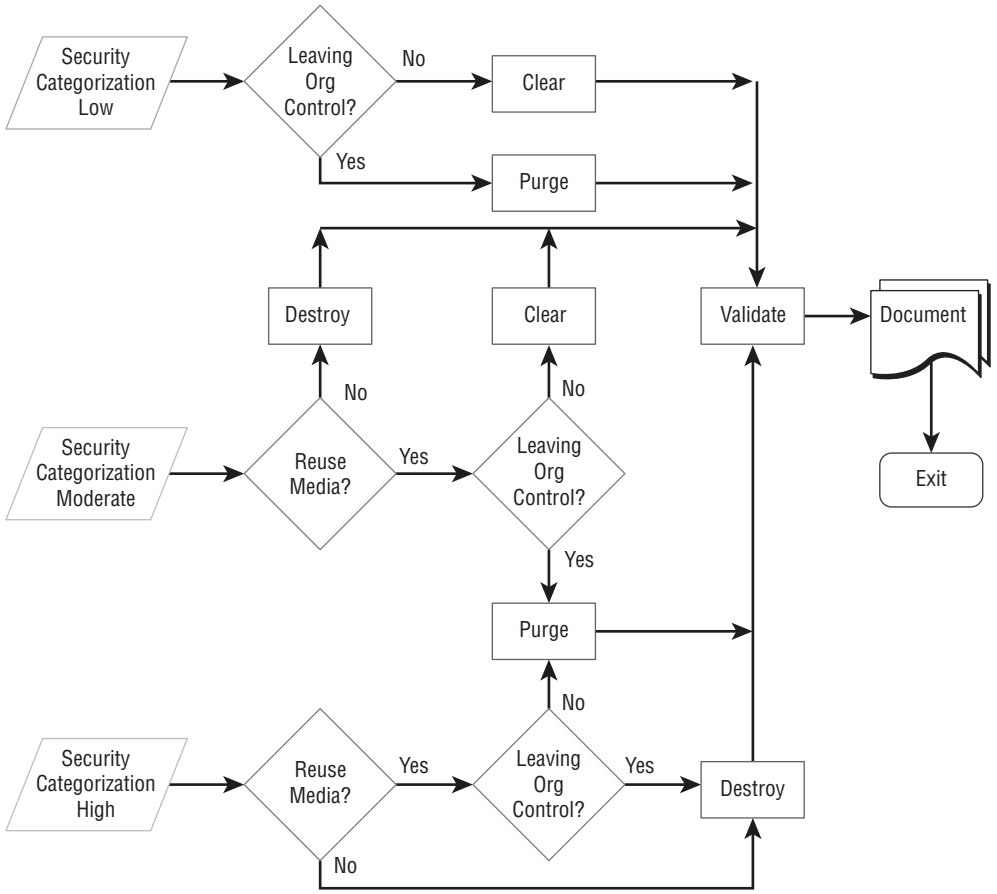
A. Information classification

B. Remanence

C. Transmitting data

D. Clearing

37. Ben is following the National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines for sanitization and disposition as shown here. He is handling information that his organization classified as sensitive, which is a moderate security categorization in the NIST model. If the media is going to be sold as surplus, what process does Ben need to follow?



Source: NIST SP 800-88

A. Destroy, validate, document

B. Clear, purge, document

C. Purge, document, validate

D. Purge, validate, document

38. Ben has been tasked with identifying security controls for systems covered by his organization's information classification system. Why might Ben choose to use a security baseline?

A. It applies in all circumstances, allowing consistent security controls.

B. They are approved by industry standards bodies, preventing liability.

C. They provide a good starting point that can be tailored to organizational needs.

D. They ensure that systems are always in a secure state.

39. Retaining and maintaining information for as long as it is needed is known as what?

A. Data storage policy

B. Data storage

C. Asset maintenance

D. Record retention

40. Referring to the figure shown here, what is the earliest stage of a fire where it is possible to use detection technology to identify it?

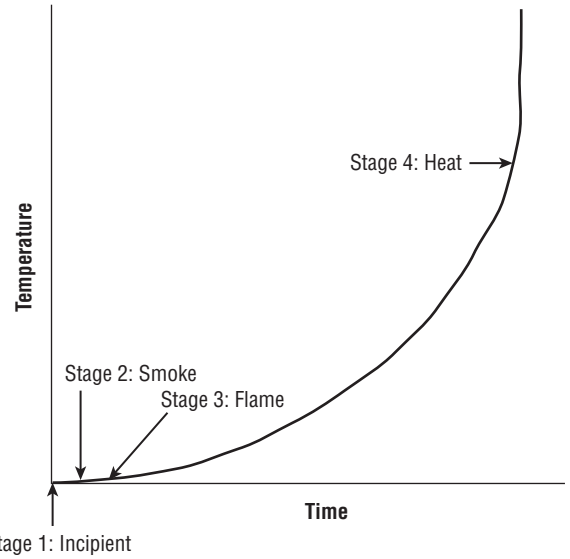


Image reprinted from *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

A. Incipient

B. Smoke

C. Flame

D. Heat

41. What type of fire suppression system fills with water when the initial stages of a fire are detected and then requires a sprinkler head heat activation before dispensing water?

A. Wet pipe

B. Dry pipe

C. Deluge

D. Preaction

42. Ralph is designing a physical security infrastructure for a new computing facility that will remain largely unstaffed. He plans to implement motion detectors in the facility but would also like to include a secondary verification control for physical presence. Which one of the following would best meet his needs?

A. CCTV

B. IPS

C. Turnstiles

D. Faraday cages

43. Referring to the figure shown here, what is the name of the security control indicated by the arrow?

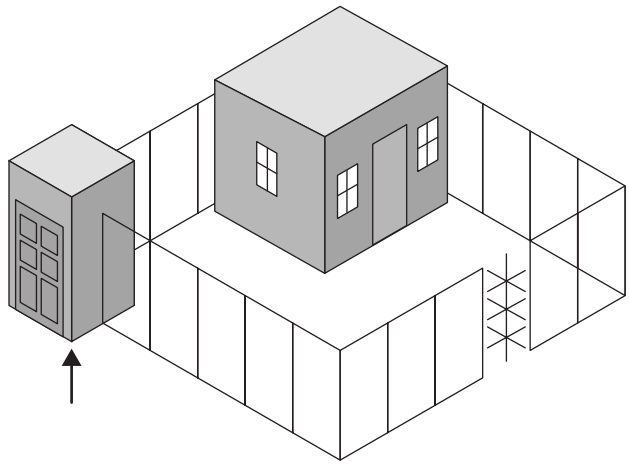


Image reprinted from *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 7th Edition* © John Wiley & Sons 2015, reprinted with permission.

A. Mantrap

B. Turnstile

C. Intrusion prevention system

D. Portal

44. Which one of the following does not describe a standard physical security requirement for wiring closets?

A. Place only in areas monitored by security guards.

B. Do not store flammable items in the closet.

C. Use sensors on doors to log entries.

D. Perform regular inspections of the closet.

45. Betty is concerned about the use of buffer overflow attacks against a custom application developed for use in her organization. What security control would provide the strongest defense against these attacks?

A. Firewall

B. Intrusion detection system

C. Parameter checking

D. Vulnerability scanning

46. Juan is retrofitting an existing door to his facility to include a lock with automation capabilities. Which one of the following types of lock is easiest to install as a retrofit to the existing door?

A. Mantrap

B. Electric lock

C. Magnetic lock

D. Turnstile

47. Rhonda is considering the use of new identification cards for physical access control in her organization. She comes across a military system that uses the card shown here. What type of card is this?

A. Smart card

B. Proximity card

C. Magnetic stripe card

D. Phase three card

48. Which one of the following facilities would have the highest level of physical security requirements?

A. Data center

B. Network closet

C. SCIF

D. Cubicle work areas

49. Glenda is investigating a potential privacy violation within her organization. The organization notified users that it was collecting data for product research that would last for six months and then disposed of the data at the end of that period. During the time that they had the data, they also used it to target a marketing campaign. Which principle of data privacy was most directly violated?

A. Data minimization

B. Accuracy

C. Storage limitations

D. Purpose limitations

50. What type of access control is composed of policies and procedures that support regulations, requirements, and the organization's own policies?

A. Corrective

B. Logical

C. Compensating

D. Administrative

51. Match each of the numbered security controls listed with exactly one of the lettered categories shown. Choose the category that best describes each control. You may use each control category once, more than once, or not at all.

Controls

1. Password

2. Account reviews

3. Badge readers

4. MFA

5. IDP

Categories

A. Administrative

B. Technical

C. Physical

52. Which of the following access control categories would not include a door lock?

A. Physical

B. Corrective

C. Preventative

D. Deterrent

For questions 53–54, please refer to the following scenario.

Gary was recently hired as the first chief information security officer (CISO) for a local government agency. The agency recently suffered a security breach and is attempting to build a new information security program. Gary would like to apply some best practices for security operations as he is designing this program.

53. As Gary decides what access permissions he should grant to each user, what principle should guide his decisions about default permissions?

A. Separation of duties

B. Least privilege

C. Aggregation

D. Separation of privileges

54. As Gary designs the program, he uses the matrix shown here. What principle of information security does this matrix most directly help enforce?

Roles/Tasks	Application Programmer	Security Administrator	Database Administrator	Database Server Administrator	Budget Analyst	Accounts Receivable	Accounts Payable	Deploy Patches	Verify Patches
Application Programmer		X	X	X					
Security Administrator	X		X	X	X	X	X	X	
Database Administrator	X	X		X					
Database Server Administrator	X	X	X						
Budget Analyst		X				X	X		
Accounts Receivable		X			X		X		
Accounts Payable		X			X	X			
Deploy Patches		X							X
Verify Patches								X	
	Potential Areas of Conflict								

A. Segregation of duties

B. Aggregation

C. Two-person control

D. Defense in depth

55. Lydia is processing access control requests for her organization. She comes across a request where the user does have the required security clearance, but there is no business justification for the access. Lydia denies this request. What security principle is she following?

A. Need to know

B. Least privilege

C. Separation of duties

D. Two-person control

56. Helen is implementing a new security mechanism for granting employees administrative privileges in the accounting system. She designs the process so that both the employee's manager and the accounting manager must approve the request before the access is granted. What information security principle is Helen enforcing?

A. Least privilege

B. Two-person control

C. Job rotation

D. Separation of duties

57. Which of the following is not true about the $(ISC)^2$ code of ethics?

A. Adherence to the code is a condition of certification.

B. Failure to comply with the code may result in revocation of certification.

C. The code applies to all members of the information security profession.

D. Members who observe a breach of the code are required to report the possible violation.

58. Javier is verifying that only IT system administrators have the ability to log on to servers used for administrative purposes. What principle of information security is he enforcing?

A. Need to know

B. Least privilege

C. Two-person control

D. Transitive trust

59. Connor's company recently experienced a denial-of-service attack that Connor believes came from an inside source. If true, what type of event has the company experienced?

A. Espionage

B. Confidentiality breach

C. Sabotage

D. Integrity breach

60. Which one of the following is not a canon of the $(ISC)^2$ code of ethics?

A. Protect society, the common good, necessary public trust and confidence, and the infrastructure.

B. Promptly report security vulnerabilities to relevant authorities.

C. Act honorably, honestly, justly, responsibly, and legally.

D. Provide diligent and competent service to principals.

61. When designing an access control scheme, Hilda set up roles so that the same person does not have the ability to provision a new user account and assign superuser privileges to an account. What information security principle is Hilda following?

A. Least privilege

B. Separation of duties

C. Job rotation

D. Security through obscurity

62. Which one of the following tools helps system administrators by providing a standard, secure template of configuration settings for operating systems and applications?

A. Security guidelines

B. Security policy

C. Baseline configuration

D. Running configuration

63. Tracy is preparing to apply a patch to her organization's enterprise resource planning system. She is concerned that the patch may introduce flaws that did not exist in prior versions, so she plans to conduct a test that will compare previous responses to input with those produced by the newly patched application. What type of testing is Tracy planning?

A. Unit testing

B. Acceptance testing

C. Regression testing

D. Vulnerability testing

64. Which one of the following security practices suggests that an organization should deploy multiple, overlapping security controls to meet security objectives?

A. Defense in depth

B. Security through obscurity

C. Least privilege

D. Separation of duties

65. What technology asset management practice would an organization use to ensure that systems meet baseline security standards?

A. Change management

B. Patch management

C. Configuration management

D. Identity management

66. The large business that Jack works for has been using noncentralized logging for years. They have recently started to implement centralized logging, however, and as they reviewed logs, they discovered a breach that appeared to have involved a malicious insider. How can Jack best ensure accountability for actions taken on systems in his environment?

A. Review the logs and require digital signatures for each log.

B. Require authentication for all actions taken and capture logs centrally.

C. Log the use of administrative credentials and encrypt log data in transit.

D. Require authorization and capture logs centrally.

67. Veronica is responsible for her organization's asset management program. During what stage of the process would she select the controls that will be used to protect assets from theft?

A. Implementation/assessment

B. Operation/maintenance

C. Inventory and licensing

D. Process, planning, design, and initiation

68. Under what type of software license does the recipient of software have an unlimited right to copy, modify, distribute, or resell a software package?

A. GNU Public License

B. Freeware

C. Open source

D. Public domain

69. When an attacker called an organization's help desk and persuaded them to reset a password due to the help desk employee's trust and willingness to help, what type of attack succeeded?

A. Trojan horse

B. Social engineering

C. Phishing

D. Whaling