Chapter 4 Study Guide

Indicate whether the statement is true or false.

1. Database shadowing duplicates data in real-time data storage, but does not backup the databases at the remote site.
    a. True
    b. False

2. A disaster recovery plan is a plan that shows the organization's intended efforts to restore operations at the original site in the aftermath of a disaster.
    a. True
    b. False

3. An attack, breach of policy, or other incident always constitutes a violation of law, requiring notification of law enforcement.
    a. True
    b. False

4. A standard is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties.
    a. True
    b. False

5. Failure to develop an information security system based on the organization's mission, vision, and culture guarantees the failure of the information security program.
    a. True
    b. False

6. The policy administrator is responsible for the creation, revision, distribution, and storage of the policy.
    a. True
    b. False

7. ISO/IEC 17799 is widely considered more useful than any other information security management approach.
    a. True
    b. False

8. Good security programs begin and end with policy.
    a. True
    b. False

9. You can create a single comprehensive ISSP document covering all information security issues.
    a. True
    b. False

Chapter 4 Study Guide

10. To remain viable, security policies must have a responsible individual, a schedule of reviews, a method for making recommendations for reviews, and a policy issuance and planned revision date.

a. True

b. False

11. Administrative controls guide the development of education, training, and awareness programs for users, administrators, and management.

a. True

b. False

12. NIST Special Publication 800-18 Rev. 1, The Guide for Developing Security Plans for Federal Information Systems, includes templates for major application security plans, and provides detailed methods for assessing, designing, and implementing controls and plans for applications of varying size.

a. True

b. False

13. To achieve defense in depth, an organization must establish multiple layers of security controls and safeguards.

a. True

b. False

14. The global information security community has universally agreed with the justification for the code of practices as identified in the ISO/IEC 17799.

a. True

b. False

15. The security framework is a more detailed version of the security blueprint.

a. True

b. False

16. Management controls address the design and implementation of the security planning process and security program management.

a. True

b. False

17. A managerial guidance SysSP document is created by the IT experts in a company to guide management in the implementation and configuration of technology.

a. True

b. False

18. The ISSP sets out the requirements that must be met by the information security blueprint or framework.

a. True

b. False

19. A policy should state that if employees violate a company policy or any law using company technologies, the company will protect them, and the company is liable for the employee's actions.

a. True

b. False

Chapter 4 Study Guide

20. In 2014, NIST published a new Cybersecurity Framework to create a mandatory framework for managing cybersecurity risk for the delivery of critical infrastructure services, based on vendor-specific technologies.

a. True

b. False

21. Information security safeguards provide two levels of control: preventative and remedial.

a. True

b. False

22. Every member of the organization's InfoSec department must have a formal degree or certification in information security.

a. True

b. False

23. A cold site provides many of the same services and options of a hot site, but at a lower cost.

a. True

b. False

24. Each policy should contain procedures and a timetable for periodic review.

a. True

b. False

25. ACLs are more specific to the operation of a system than rule-based policies and they may or may not deal with users directly.

a. True

b. False

26. Disaster recovery personnel must know their roles without supporting documentation, which is a function of preparation, training and rehearsal.

a. True

b. False

27. Hot swapping is a RAID implementation (typically referred to as RAID Level 1) in which the computer records all data to twin drives simultaneously, providing a backup if the primary drive fails.

a. True

b. False

28. Security training provides detailed information and hands-on instruction to employees to prepare them to perform their duties securely.

a. True

b. False

Chapter 4 Study Guide

29. NIST 800-14's Principles for Securing Information Technology Systems, can be used to make sure the needed key elements of a successful
effort are factored into the design of an information security program and to produce a blueprint for an effective security architecture.

a. True

b. False

30. Many industry observers claim that ISO/IEC 17799, the precursor to ISO/IEC 27001, is not as complete as other frameworks.

a. True

b. False

Indicate the answer choice that best completes the statement or answers the question.

31. According to NIST SP 800-14's security principles, security should _____.

a. support the mission of the organization b. require a comprehensive and integrated approach

c. be cost-effective d. All of the above

32. _____ is a strategy for the protection of information assets that uses multiple layers and different types of controls (managerial, operational, and technical) to provide optimal protection.

a. Networking b. Proxy

c. Defense in depth d. Best-effort

33. _____ controls address personnel security, physical security, and the protection of production inputs and outputs.

a. Informational b. Operational

c. Technical d. Managerial

34. RAID is an acronym for a _____ array of independent disk drives that stores information across multiple units to spread out data and minimize the impact of a single drive failure.

a. replicated b. resistant

c. random d. redundant

35. The CPMT conducts the BIA in three stages. Which of the following is NOT one of those stages?

a. Determine mission/business processes and recovery criticality

b. Identify recovery priorities for system resources

c. Identify resource requirements

d. All of these are BIA stages

36. Standards may be published, scrutinized, and ratified by a group, as in formal or _____standards.

a. de formale b. de public

c. de jure d. de facto

37. The spheres of security are the foundation of the security framework and illustrate how information is under attack from a variety of sources, with far fewer protection layers between the information and potential attackers on the _____ side of the organization.

a. technology b. Internet

c. people d. operational

Chapter 4 Study Guide

38. The stated purpose of ISO/IEC 27002 is to “offer guidelines and voluntary directions for information security _____."

a. implementation b. certification
c. management d. accreditation

39. A(n) _____ is a document containing contact information for the people to be notified in the event of an incident.

a. emergency notification system b. alert roster
c. phone list d. call register

40. The transfer of large batches of data to an off-site facility, usually through leased lines or services, is called ____.

a. off-site storage b. remote journaling
c. electronic vaulting d. database shadowing

41. Security _____ are the areas of trust within which users can freely communicate.

a. perimeters b. domains
c. rectangles d. layers

42. When BS 7799 first came out, several countries, including the United States, Germany, and Japan, refused to adopt it, claiming that it had fundamental problems. Which of the following is NOT one of those problems

a. The standard lacked the measurement precision associated with a technical standard.
b. It was not as complete as other frameworks.
c. The standard was hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.
d. The global information security community had already defined a justification for a code of practice, such as the one identified in ISO/IEC 17799.

43. The goals of information security governance include all but which of the following?

a. Regulatory compliance by using information security knowledge and infrastructure to support minimum standards of due care
b. Strategic alignment of information security with business strategy to support organizational objectives
c. Risk management by executing appropriate measures to manage and mitigate threats to information resources
d. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved

44. _____often function as standards or procedures to be used when configuring or maintaining systems.

a. ESSPs b. EISPs
c. ISSPs d. SysSPs

45. _____ controls cover security processes that are designed by strategic planners and implemented by the security administration of the organization.

a. Managerial b. Technical
c. Operational d. Informational

Chapter 4 Study Guide

46. A fundamental difference between a BIA and risk management is that risk management focuses on identifying the threats, vulnerabilities, and
attacks to determine which controls can protect the information, while the BIA assumes _____.

a. controls have been bypassed b. controls have proven ineffective

c. controls have failed d. All of the above

47. A security _____ is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization.

a. plan b. framework

c. model d. policy

48. Redundancy can be implemented at a number of points throughout the security architecture, such as in _____

a. firewalls b. proxy servers

c. access controls d. All of the above

49. SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, provides best practices and security principles that can direct the security team in the development of a security _____.

a. plan b. standard

c. policy d. blueprint

50. The _____is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

a. SysSP b. EISP

c. GSP d. ISSP

51. The SETA program is a control measure designed to reduce the instances of _____ security breaches by employees.

a. intentional b. external

c. accidental d. physical

52. Incident _____ is the rapid determination of the scope of the breach of the confidentiality, integrity, and availability of information and information assets during or just following an incident.

a. damage assessment b. containment strategy

c. incident response d. disaster assessment

53. A ____ site provides only rudimentary services and facilities.

a. commercial b. warm

c. hot d. cold

54. A(n) _____ plan is a plan for the organization's intended strategic efforts over the next several years.

a. standard b. operational

c. tactical d. strategic

55. _____ is a strategy of using multiple types of technology that prevent the failure of one system from compromising the security of information.

a. Firewalling b. Hosting

c. Redundancy d. Domaining

Chapter 4 Study Guide

56. In early 2014, in response to Executive Order 13636, NIST published the Cybersecurity Framework that intends to allow organization to _____.

a. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process

b. assess progress toward a recommended target state

c. communicate among local, state and national agencies about cybersecurity risk

d. None of these