Chapter 11 Study Guide

Indicate whether the statement is true or false.

1. In most cases, organizations look for a technically qualified information security generalist who has a solid understanding of how an organization operates.

a. True

b. False

2. "Know more than you say, and be more skillful than you let on" advise for information security professionals indicates the actions taken to protect information should not interfere with users' actions.

a. True

b. False

3. Security managers are accountable for the day-to-day operation of the information security program.

a. True

b. False

4. "Builders" in the field of information security provide day-to-day systems monitoring and use to support an organization's goals and objectives.

a. True

b. False

5. The process of integrating information security perspectives into the hiring process begins with reviewing and updating all job descriptions.

a. True

b. False

6. The SSCP examination is much more rigorous that the CISSP examination.

a. True

b. False

7. In many organizations, information security teams lacks established roles and responsibilities.

a. True

b. False

8. A background check must always be conducted to determine the level of trust the business can place in a candidate for an information security position.

a. True

b. False

9. The organization should integrate the security awareness education into a new hire's ongoing job orientation and make it a part of every employee's on-the-job security training.

a. True

b. False

Chapter 11 Study Guide

10. To maintain a secure facility, all contract employees should be escorted from room to room, as well as into and out of the facility.

   a. True

   b. False

11. CompTIA offers a vendor-specific certification program called the Security+ certification.

   a. True

   b. False

12. The security manager position is much more general than that of CISO.

   a. True

   b. False

13. The use of standard job descriptions can increase the degree of professionalism in the information security field.

   a. True

   b. False

14. The CISSP-ISSEP concentration focuses on the knowledge areas that are part of enterprise security management.

   a. True

   b. False

15. The information security function cannot be placed within protective services.

   a. True

   b. False

16. Organizations are not required by law to protect employee information that is sensitive or personal.

   a. True

   b. False

17. The CISSP concentration concentrations are available for CISSPs to demonstrate knowledge that is already a part of the CISSP CBK.

   a. True

   b. False

18. The position of security technician can be offered as an entry-level position.

   a. True

   b. False

19. Existing information security-related certifications are typically well understood by those responsible for hiring in the organizations.

   a. True

   b. False

Chapter 11 Study Guide

20. The general management community of interest must work with the information security professionals to integrate solid information security concepts into the personnel management practices of the organization.

a. True

b. False

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

21. The breadth and depth covered in each of the domains makes the __________ one of the most difficult-to-attain certifications on the market.

a. NSA b. CISO

c. CISSP d. ISEP

22. The International Society of Forensic Computer Examiners (ISFCE) offers which certifications?

a. Certified Computer Examiner (CCE) b. Master Certified Computer Examiner (MCCE)

c. both a & b d. neither a nor b

23. Many who move to business-oriented information security were formerly__________ who were often involved in national security or cybersecurity .

a. marketing managers b. military personnel

c. business analysts d. lawyers

24. __________ are hired by the organization to serve in a temporary position or to supplement the existing workforce.

a. Temporary employees b. Consultants

c. Contractors d. Self-employees

25. Many organizations use a(n) __________ interview to remind the employee of contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee’s tenure in the organization.

a. hostile b. departure

c. exit d. termination

26. Which of the following is not one of the categories of positions as defined by Schwartz, Erwin, Weafer, and Briney?

a. definer b. user

c. builder d. administrator

27. Like the CISSP, the SSCP certification is more applicable to the security__________ than to the security __________,

a. technician, manager b. manager, engineer

c. manager, technician d. technician, executive

28. __________ are the technically qualified individuals tasked to configure firewalls, deploy IDSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that an organization’s security technology is properly implemented.

a. CSOs b. CISOs

c. Security managers d. Security technicians

Chapter 11 Study Guide

29. The model commonly used by large organizations places the information security department within the __________ department.

a. management b. information technology
c. financial d. production

30. The information security function can be placed within the __________.

a. insurance and risk management function
b. administrative services function
c. legal department
d. All of the above

31. The ISSEP allows CISSP certificate holders to demonstrate expert knowledge of all of these except __________.

a. Systems security engineering b. Technical management
c. International laws d. Certification and accreditation/risk management framework

32. The CISA credential is touted by ISACA as the certification that is appropriate for all but which type of professionals?

a. accounting b. security
c. networking d. auditing

33. __________ is the requirement that every employee be able to perform the work of another employee.

a. Two-man control b. Collusion
c. Duty exchange d. Task rotation

34. __________ is a cornerstone in the protection of information assets and in the prevention of financial loss.

a. Fire suppression b. Business separation
c. Separation of duties d. Collusion

35. The __________ position is typically considered the top information security officer in the organization.

a. CISO b. CFO
c. CTO d. CEO

36. Many enter the field of information security from technical professionals such as __________ who find themselves working on information security applications and processes more often than traditional IT assignments.

a. networking experts or systems administrators b. database administrators
c. programmers d. All of the above

37. According to Schwartz, Erwin, Weafer, and Briney "__________" are the real techies who create and install security solutions.

a. Builders b. Administrators
c. Engineers d. Definers

38. The ISSMP examination is designed to provide CISSPs with a mechanism to demonstrate competence in __________.

a. Enterprise security management practices b. Security management practices
c. Business continuity planning and disaster recovery planning d. All of the above

Chapter 11 Study Guide

39. In recent years, the __________ certification program has added a set of concentration exams.

a. ISSEP	b. ISSMP
c. ISSAP	d. CISSP

40. System Administration, Networking, and Security Organization is better known as __________.

a. SANO	b. SAN
c. SANS	d. SANSO