Chapter 5 Study Guide

Indicate whether the statement is true or false.

1. Baselining is the comparison of past security activities and events against the organization's current performance.
   a. True
   b. False

2. To determine if the risk to an information asset is acceptable or not, you estimate the expected loss the organization will incur if the risk is exploited.
   a. True
   b. False

3. A security clearance is a component of a data classification scheme that assigns a status level to systems to designate the maximum level of classified data that may be stored on it.
   a. True
   b. False

4. Some information security experts argue that it is virtually impossible to determine the true value of information and information-bearing assets.
   a. True
   b. False

5. Identifying human resources, documentation, and data information assets of an organization is less difficult than identifying hardware and software assets.
   a. True
   b. False

6. You should adopt naming standards that do not convey information to potential system attackers.
   a. True
   b. False

7. When determining the relative importance of each asset, refer to the organization's mission statement or statement of objectives to determine which elements are essential, which are supportive, and which are merely adjuncts.
   a. True
   b. False

8. Process-based measures are performance measures that are focused on numbers and less strategic than metric-based measures.
   a. True
   b. False

9. According to Sun Tzu, if you know your self and know your enemy you have an average chance to be successful in an engagement.
   a. True
   b. False

Chapter 5 Study Guide

10. Cost Benefit Analyses (CBAs) cannot be calculated after controls have been functioning for a time, as observation over time prevents precision in evaluating the benefits of the safeguard and determining whether it is functioning as intended.

a. True
b. False

11. In addition to their other responsibilities, the three communities of interest are responsible for determining which control options are cost effective for the organization,

a. True
b. False

12. Know yourself means identifying, examining, and understanding the threats facing the organization.

a. True
b. False

13. You cannot use qualitative measures to rank information asset values.

a. True
b. False

14. Residual risk is the risk that that has not been removed, shifted, or planned for after vulnerabilities have been completely resolved.

a. True
b. False

15. The threats-vulnerabilities-assets (TVA) worksheet is a document that shows a comparative ranking of prioritized assets against prioritized threats, with an indication of any vulnerabilities in the asset/threat pairings.

a. True
b. False

16. If the acceptance strategy is used to handle every vulnerability in the organization, its managers may be unable to conduct proactive security activities and portray an apathetic approach to security in general

a. True
b. False

17. Operational feasibility is an assessment of whether the organization can acquire the technology necessary to implement and support the proposed control.

a. True
b. False

18. A best practice proposed for a small to medium business will be similar to one used to help design control strategies for a large multinational company.

a. True
b. False

Chapter 5 Study Guide

19. Risk control is the application of mechanisms to reduce the potential for loss or change to an organization's information assets.

a. True

b. False

20. Within a data classification scheme, comprehensive means that an information asset should fit in only one category.

a. True

b. False

21. Organizations should communicate with system users throughout the development of the security program, letting them know that change are coming, and reduce resistance to expected change through communication, education, and involvement.

a. True

b. False

22. The results from risk assessment activities can be delivered in a number of ways: a report on a systematic approach to risk control, a project-based risk assessment, or a topic-specific risk assessment.

a. True

b. False

23. A data classification scheme is a formal access control methodology used to assign a level of availability to an information asset and thus restrict the number of people who can access it.

a. True

b. False

24. The defense control strategy is the risk control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards, but is not the preferred approach to controlling risk.

a. True

b. False

25. In a cost-benefit analysis, a single loss expectancy (SLE) is the calculated value associated with the most likely loss from an attack, with the SLE being the product of the asset's value and the annualized loss expectancy.

a. True

b. False

26. When it is necessary to calculate, estimate, or derive values for information assets, you might give consideration to the value incurred from the cost of protecting the information.

a. True

b. False

27. The value of information to the organization's competition should influence the asset's valuation.

a. True

b. False

Chapter 5 Study Guide

28. One advantage to benchmarking is that best practices change very little over time.
    a. True
    b. False

29. Best business practices are often called recommended practices.
    a. True
    b. False

30. The upper management of an organization must structure the IT and information security functions to defend the organization's information assets.
    a. True
    b. False

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

31. The formal decision making process used when considering the economic feasibility of implementing information security controls and safeguards is called a(n) _____.
    a. ARO b. CBA
    c. ALE d. SLE

32. The first phase of risk management is _____.
    a. risk identification b. design
    c. risk control d. risk evaluation

33. The concept of competitive _____ refers to falling behind the competition.
    a. disadvantage b. drawback
    c. failure d. shortcoming

34. _____ plans usually include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the flood waters recede.
    a. IR b. DR
    c. BC d. BR

35. A(n) _____ is a formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it..
    a. security clearance scheme b. data recovery scheme
    c. risk management scheme d. data classification scheme

36. Federal agencies such as the NSA, FBI, and CIA use specialty classification schemes. For materials that are not considered 'National Security Information', _____ data is the lowest level classification.
    a. Sensistive b. Confidential
    c. Unclassified d. Public

37. A(n) _____ is an authorization issued by an organization for the repair, modification, or update of a piece of equipment.
    a. IP b. FCO
    c. CTO d. HTTP

Chapter 5 Study Guide

38. The _____ is the difference between an organization's observed and desired performance.
a. performance gap b. objective
c. issue delta d. risk assessment

39. When organizations adopt security measures for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances. This is referred to as _____.
a. baselining b. best practices
c. benchmarking d. standards of due care

40. Risk _____ defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility.
a. benefit b. appetite
c. acceptance d. avoidance

41. _____ is an asset valuation approach that uses categorical or non-numeric values rather than absolute numerical measures.
a. Qualitative assessment b. Metric-centric model
c. Quantitative assessment d. Value-specific constant

42. Management of classified data includes its storage and _____.
a. distribution b. portability
c. destruction d. All of the above

43. The _____ plan specifies the actions an organization can and should take while an adverse event (that could result in loss of an information asset or assets, but does not currently threaten the viability of the entire organization) is in progress.
a. BC b. DR
c. IR d. BR

44. The _____ strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.
a. defense b. transfer
c. mitigation d. acceptance

45. _____ equals the probability of a successful attack times the expected loss from a successful attack plus an element of uncertainty.
a. Loss Magnitude b. Risk
c. Loss Frequency d. Loss

46. In a(n) _____, assets or threats can be prioritized by identifying criteria with differing levels of importance, assigning a score for each of the criteria and then summing and ranking those scores.
a. threat assessment b. risk management program
c. weighted factor analysis d. data classification scheme

Chapter 5 Study Guide

47. _____ assigns a status level to employees to designate the maximum level of classified data they may access.
a. security clearance scheme b. data recovery scheme
c. risk management scheme d. data classification scheme

48. _____ is simply how often you expect a specific type of attack to occur.
a. ARO b. CBA
c. ALE d. SLE

49. The _____ control strategy attempts to shift risk to other assets, other processes, or other organizations.
a. transfer b. defend
c. accept d. mitigate

50. The calculation of the likelihood of an attack coupled with the attack frequency to determine the expected number of losses within a specified time range is called the _____.
a. loss frequency b. annualized loss expectancy
c. likelihood d. benefit of loss

51. There are individuals who search trash and recycling — a practice known as _____ — to retrieve information that could embarrass a company or compromise information security.
a. shoulder surfing b. dumpster diving
c. pretexting d. corporate espionage

52. The _____ control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards.
a. termination b. defense
c. transfer d. mitigate

53. Risk _____ is the application of security mechanisms to reduce the risks to an organization's data and information systems.
a. management b. control
c. identification d. security

54. _____ feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders.
a. Organizational b. Technical
c. Operational d. Political

55. _____ addresses are sometimes called electronic serial numbers or hardware addresses.
a. HTTP b. IP
c. DHCP d. MAC