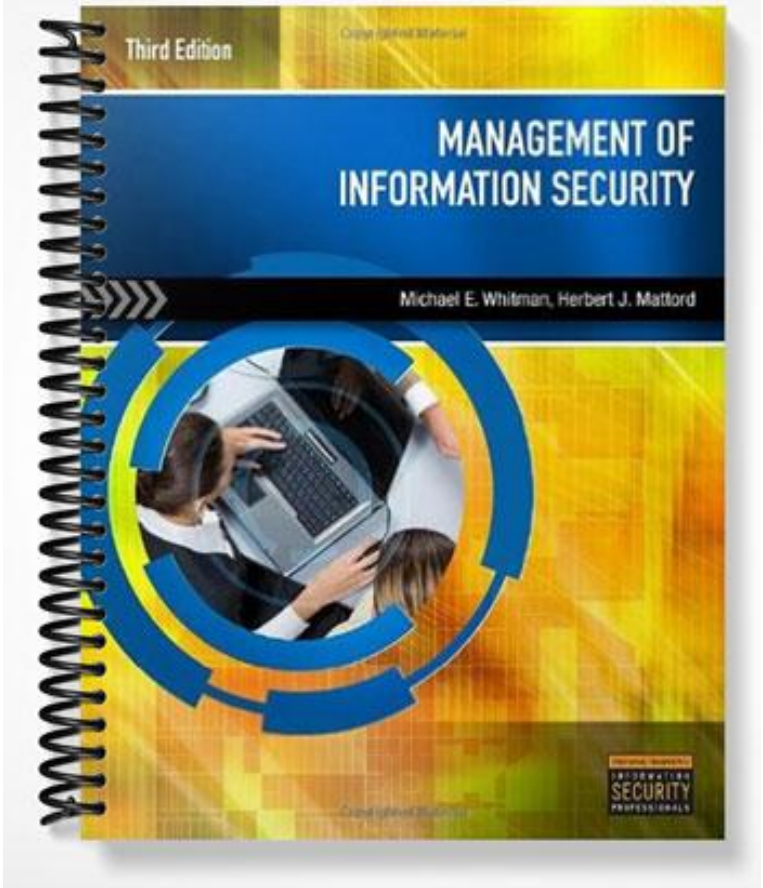
TEST BANK


Third Edition
MANAGEMENT OF
INFORMATION SECURITY
Michael E. Whitman, Herbert J. Mattord
SECURITY

TRUE/FALSE

1. Because it sets out general business intentions, a mission statement does not need to be concise.

   ANS: F PTS: 1 REF: 42

2. Vision statements should be ambitious.

   ANS: T PTS: 1 REF: 42

3. A vision statement is meant to be a factual depiction of the current state of the organization.

   ANS: F PTS: 1 REF: 42

4. A clearly directed strategy flows from top to bottom.

   ANS: T PTS: 1 REF: 43

5. Strategic planning has a more short-term focus than tactical planning.

   ANS: F PTS: 1 REF: 43

6. CISOs use the operational plan to organize, prioritize, and acquire resources for major projects.

   ANS: T PTS: 1 REF: 45

7. Implementation of information security can be accomplished only with a top-down approach.

   ANS: F PTS: 1 REF: 54

8. The champion in a top-down approach to security implementation is usually a network administrator.

   ANS: F PTS: 1 REF: 55

9. The success of information security plans can be enhanced by using a formal methodology like that of the systems development life cycle.

   ANS: T PTS: 1 REF: 55

10. The CISO plays a more active role in the development of the planning details than does the CIO.

    ANS: T PTS: 1 REF: 53

11. The security governance responsibilities of mid-level managers in the organization includes implementing, auditing, enforcing and assessing compliance.

    ANS: T PTS: 1 REF: 53

12. A good general governance framework based on the IDEAL model includes initiating, developing, evaluating, acting and leading.

ANS: F PTS: 1 REF: 52

13. In order to build programs suited to their needs, organizations should conduct an annual information security evaluation, the results of which the CISO should review with staff and then report to the board of directors.

    ANS: F PTS: 1 REF: 51

14. Benefits of Information Security Governance include optimization of the allocation of limited security safeguards.

    ANS: F PTS: 1 REF: 50

15. Boards of Directors for Information Security Governance should follow essential practices including identifying information security leaders, holding them accountable and ensuring support for them.

    ANS: T PTS: 1 REF: 50

16. The basic outcomes of information security governance should include strategic alignment of information security with business strategy to support strategic planning.

    ANS: F PTS: 1 REF: 49

17. Information security governance consists of the leadership, organizational structures, and processes that safeguard information. Critical to the success of these structures and processes is effective interoperability between all parties, which requires constructive relationships, a common language, and shared commitment to addressing the issues.

    ANS: F PTS: 1 REF: 49

18. According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide strategic direction and establishment of objectives.

    ANS: T PTS: 1 REF: 49

19. The primary goal of internal monitoring is to maintain an informed awareness of the state of all of the organization's networks, information systems, and information security defenses.

    ANS: T PTS: 1 REF: 66

20. Penetration testing is often conducted by consultants or outsourced contractors, who are commonly referred to as hackers, ninja teams or black teams.

    ANS: F PTS: 1 REF: 67

MODIFIED TRUE/FALSE

1. The <u>values statement</u> of a business is like its identity card. _____

   ANS: F, mission statement

PTS: 1 REF: 42

2. Tactical planning is the basis for the long-term direction taken by the organization. _____

ANS: F, Strategic

PTS: 1 REF: 43

3. Strategic plans are used to create tactical plans. _____

ANS: T PTS: 1 REF: 45

4. Some companies refer to operational planning as intermediate planning. _____

ANS: F, tactical

PTS: 1 REF: 45

5. The top-down approach to security implementation might begin as a grass-roots effort in which systems administrators attempt to improve the security of their systems. _____

ANS: F, bottom-up

PTS: 1 REF: 54

6. In a(n) methodology, a problem is solved based on a structured sequence of procedures. _____

ANS: T PTS: 1 REF: 55

7. Information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide strategic direction, verification that risk management practices are appropriate, and validation that the organization's assets are used properly. _____

ANS: T PTS: 1 REF: 49

8. The impetus to begin a SDLC-based project may be either event-driven or personnel-driven. _____

ANS: F, plan-driven

PTS: 1 REF: 55

9. Boards of directors should supervise strategic information security objectives by verifying that management's investment in information security is properly aligned with organizational strategies and the organization's competitive environment. _____

ANS: F, risk

PTS: 1 REF: 49

10. The basic outcomes of information security governance should include risk management by executing appropriate measures to manage and mitigate threats to information resources.
_____

ANS: T PTS: 1 REF: 49

11. According to NACD, boards of directors should identify information security risks, hold them accountable, and ensure support for them. _____

ANS: F, leaders

PTS: 1 REF: 50

12. Information security governance benefits include increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels
_____

ANS: T PTS: 1 REF: 50

13. The information security governance framework generally includes a comprehensive security strategy explicitly linked with business and IT risks. _____

ANS: F, objectives

PTS: 1 REF: 50

14. In order to build security programs suited to their needs, the CGTF recommends organizations conduct periodic testing and evaluation of the legality of information security policies and procedures.
_____

ANS: T, effectiveness

PTS: 1 REF: 51

15. Organizations following the IDEAL Governance framework would determine where you are relative to where you want to be in the evaluation phase. _____

ANS: F, diagnosing

PTS: 1 REF: 52

16. The primary role of the chief information officer is to oversee overall "corporate security posture" for which he/she is accountable to the board. _____

ANS: F, executive

PTS: 1 REF: 53

17. The CISO is also known as the chief security officer, director of information security or information security manager. _____

ANS: T PTS: 1 REF: 53

18. According to *Information Security Roles and Responsibilities Made Easy*, the Chief Information Security Officer must understand the fundamental information technology activities performed by the company and, based on this understanding, suggest appropriate information security solutions that uniquely protect these activities. _____

    ANS: F, business

    PTS: 1 REF: 53

19. A bottom-up approach to information security implementation begins with security managers who see to improve the security of their systems. _____

    ANS: F, system administrators

    PTS: 1 REF: 54

20. A(n) vulnerability is an identified weakness of a controlled information asset and is the result of absent or inadequate controls. _____

    ANS: T PTS: 1 REF: 59

MULTIPLE CHOICE

1. The ____ explicitly declares the business of the organization and its intended areas of operations.
   a. vision statement
   b. values statement
   c. mission statement
   d. business statement

   ANS: C PTS: 1 REF: 42

2. ____ statements are meant to express the aspirations of the organization.
   a. Mission
   b. Vision
   c. Values
   d. Business

   ANS: B PTS: 1 REF: 42

3. Which of the following is true about mission statements?
   a. They should be ambitious
   b. They express what the organization is
   c. They express the aspirations of the organization
   d. They are not meant to be probable

   ANS: B PTS: 1 REF: 42

4. Vision statements are meant to be ____.
   a. probable
   b. realistic
   c. factual
   d. ambitious

   ANS: D PTS: 1 REF: 42

5. The ____ statement contains a formal set of organizational principles, standards, and qualities.
   a. vision
   b. mission
   c. values
   d. business

   ANS: C PTS: 1 REF: 40-41

6. The long-term direction taken by the organization is based on ____ planning.
   a. strategic
   b. tactical
   c. operational
   d. managerial

   ANS: A PTS: 1 REF: 43

7. Which of the following is true?
   a. Strategic plans are used to create tactical plans
   b. Tactical plans are used to create strategic plans
   c. Operational plans are used to create tactical plans
   d. Operational plans are used to create strategic plans

   ANS: A PTS: 1 REF: 43

8. Tactical planning usually has a focus of ____.
   a. one to five days
   b. one to three months
   c. one to three years
   d. five or more years

   ANS: C PTS: 1 REF: 45

9. Budgeting, resource allocation, and manpower are critical components of the ____ plan.
   a. strategic
   b. operational
   c. organizational
   d. tactical

   ANS: D PTS: 1 REF: 45

10. Tactical planning is also referred to as ____.
    a. strategic planning
    b. project planning
    c. organizational planning
    d. operational planning

    ANS: B PTS: 1 REF: 45

11. ____ plans are used to organize the ongoing, day-to-day performance of tasks.
    a. Strategic
    b. Tactical
    c. Organizational
    d. Operational

    ANS: D PTS: 1 REF: 45

12. Operational plans are used by ____.
    a. managers
    b. security managers
    c. the CISO
    d. the CIO

    ANS: A PTS: 1 REF: 45

13. Information security ____ must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach.
    a. objectives
    b. plans
    c. governance
    d. practices

    ANS: A PTS: 1 REF: 49

14. The basic outcomes of information security governance should include all but which of the following?
    a. Value delivery by optimizing information security investments in support of organizational objectives
    b. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved

c. Resource management by executing appropriate measures to manage and mitigate risks to information technologies
d. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively

ANS: C PTS: 1 REF: 49-50

15. According to the IGTI, Boards of directors should supervise strategic information security objectives by all but which of the following?
a. Inculcating a culture that recognizes the criticality of information and information security to the organization
b. Verifying that management's investment in information security is properly aligned with organizational budgets and the organization's financial environment
c. Assuring that a comprehensive information security program is developed and implemented
d. Demanding reports from the various layers of management on the information security program's effectiveness and adequacy

ANS: B PTS: 1 REF: 49

16. The National Association of Corporate Directors (NACD) recommends four essential practices for boards of directors. Which of the following is NOT one of these recommended practices?
a. Place information security at the top of the board's agenda
b. Assign information security to a key committee and ensure adequate support for that committee
c. Ensure the effectiveness of the corporation's information security policy through review and approval
d. Identify information security leaders, hold them accountable, and ensure support for them

ANS: A PTS: 1 REF: 50

17. Which of the following is NOT a significant benefit of information security governance?
a. Optimization of the allocation of limited security resources
b. A level of assurance that critical decisions are not based on faulty information
c. Increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels
d. All of these are benefits of information security governance

ANS: D PTS: 1 REF: 50

18. The information security governance framework generally consists of which of the following?
a. Security policies that address each aspect of strategy, control, and regulation
b. A security strategy that talks about the value of information technologies protected
c. Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
d. All of these are components of the information security governance framework

ANS: B PTS: 1 REF: 50

19. According to the Corporate Governance Task Force (CGTF), in order to build programs suited to their needs, organizations should do all but which of the following?
a. Create and execute a plan for punitive action for employees who fail to resolve information security deficiencies
b. Use security best practices guidance, such as ISO 17799, to measure information security performance

c. Establish plans, procedures, and tests to provide continuity of operations
d. Develop plans and initiate actions to provide adequate information security for networks, facilities, systems, and information

ANS: A PTS: 1 REF: 51

20. According to the Corporate Governance Task Force (CGTF), in order to build programs suited to their needs, organizations should do all but which of the following?
a. Conduct periodic testing and evaluation of the effectiveness of information security policies and procedures
b. Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability
c. Conduct an annual information security evaluation, the results of which the CISO should review with security staff and then report to the board of directors
d. Implement policies and procedures based on risk assessments to secure information assets

ANS: C PTS: 1 REF: 51

21. According to the Corporate Governance Task Force (CGTF), which phase in the IDEAL model and framework lays the groundwork for a successful improvement effort?
a. Initiating
b. Establishing
c. Acting
d. Learning

ANS: A PTS: 1 REF: 52

22. According to the Corporate Governance Task Force (CGTF), during which phase in the IDEAL model and framework does the organization plan the specifics of who it will reach its destination?
a. Initiating
b. Establishing
c. Acting
d. Learning

ANS: B PTS: 1 REF: 52

23. According to the Corporate Governance Task Force (CGTF), during which phase in the IDEAL model and framework does the organization do the work according to the plan?
a. Initiating
b. Establishing
c. Acting
d. Learning

ANS: C PTS: 1 REF: 52

24. According to the Corporate Governance Task Force (CGTF), during which phase in the IDEAL model and framework does the organization improve its ability to adopt new improvements in the future?
a. Initiating
b. Establishing
c. Acting
d. Learning

ANS: D PTS: 1 REF: 52

25. Which of the following is an information security governance responsibility of the CEO?
a. Communicate policies and the program
b. Set security policy, procedures, programs and training for the organization
c. brief the board, customers and the public
d. implement policy, report security vulnerabilities and breaches

ANS: C PTS: 1 REF: 53

26. Which of the following is an nformation security governance responsibility of the CISO?
a. Communicate policies and the program

b. Set security policy, procedures, programs and training for the organization
c. Brief the board, customers and the public
d. Implement policy, report security vulnerabilities and breaches

ANS: B PTS: 1 REF: 53

27. Which of the following is an information security governance responsibility of the organization's employees?
a. Communicate policies and the program
b. Set security policy, procedures, programs and training for the organization
c. Brief the board, customers and the public
d. Implement policy, report security vulnerabilities and breaches

ANS: D PTS: 1 REF: 53

28. Which of the following is a characteristic of the bottom-up approach to security implementation?
a. Strong upper-management support
b. A clear planning and implementation process
c. Systems administrators attempting to improve the security of their systems
d. Ability to influence organizational culture

ANS: C PTS: 1 REF: 54

29. A ____ is a formal approach to solving a problem based on a structured sequence of procedures.
a. plan
b. methodology
c. program
d. control

ANS: B PTS: 1 REF: 55

30. A SDLC-based project may be started by an event-driven or a ____ impetus.
a. plan-driven
b. process-driven
c. sequence-driven
d. personnel-driven

ANS: A PTS: 1 REF: 55

31. A SDLC-based project that is the result of a carefully developed strategy is said to be ____.
a. employee-driven
b. plan-driven
c. sequence-driven
d. event-driven

ANS: B PTS: 1 REF: 55

32. At the end of each phase of the security systems development life cycle (SecSDLC), a ____ takes place.
a. brainstorming session
b. structured discussion
c. structured review
d. planning session

ANS: C PTS: 1 REF: 55

33. In the security systems development life cycle (SecSDLC), the work products of each phase fall into the next phase to serve as its starting point, which is known as the ____ model.
a. continuous
b. cycle-based
c. circular
d. waterfall

ANS: D PTS: 1 REF: 55

34. The first phase of the security systems development life cycle (SecSDLC) is the ____ phase.

a. analysis
b. investigation
c. logical design
d. physical design

ANS: B PTS: 1 REF: 56

35. At the end of the investigation phase of the security systems development life cycle (SecSDLC), a ____ analysis is performed.
a. effort-value
b. value
c. worthiness
d. feasibility

ANS: D PTS: 1 REF: 56

36. The ____ phase of the security systems development life cycle (SecSDLC) assesses the organization's readiness, its current systems status, and its capability to implement and then support the proposed systems.
a. physical design
b. implementation
c. investigation
d. analysis

ANS: D PTS: 1 REF: 56

37. A(n) ____ is a category of objects, persons or other entities that represent a constant threat to an asset.
a. threat
b. vulnerability
c. risk
d. exploit

ANS: A PTS: 1 REF: 57

38. A(n) ____ is a category of objects, persons or other entities that represent a constant threat to an asset.
a. threat
b. vulnerability
c. risk
d. exploit

ANS: A PTS: 1 REF: 57

39. In the ____ phase of the security systems development life cycle (SecSDLC), the information obtained during the analysis phase is used to develop a proposed system-based solution for the business problem.
a. logical design
b. physical design
c. investigation
d. implementation

ANS: A PTS: 1 REF: 61

40. A(n) ____ approach to security implementation is frequently referred to as a grass-roots effort.
a. SDLC
b. SecSDLC
c. top-down
d. bottom-up

ANS: D PTS: 1 REF: 54

41. For any top-down approach to security implementation to succeed, the initiative must have a(n) ____ with influence to move the project forward.
a. SDLC
b. CISO
c. champion
d. mid-level administrator

ANS: C PTS: 1 REF: 54

42. The ____ phase is typically the most important phase of the security systems development life cycle (SecSDLC).
a. implementation
c. analysis

b. maintenance
d. logical design

ANS: B PTS: 1 REF: 65

43. The primary goal of ____ is the identification of specific, documented weaknesses and their timely resolution.
a. ethical hacking
b. SecSDLC
c. penetration testing and solutions
d. vulnerability assessment and remediation

ANS: D PTS: 1 REF: 67

44. ____ controls deal with managerial functions and lower-level planning such as disaster recovery and incident response planning.
a. Managerial
b. Operational
c. Technical
d. Tactical

ANS: B PTS: 1 REF: 62

45. ____ controls set the direction and scope of the security process and provide detailed instructions for its conduct.
a. Managerial
b. Operational
c. Technical
d. Tactical

ANS: A PTS: 1 REF: 62

46. Which of the following categories of threats describes an act of human error or failure?
a. piracy
b. blackmail of information disclosure
c. unauthorized access
d. accidents

ANS: D PTS: 1 REF: 57

47. Copyright infringement is an example of the ____ category of threat.
a. compromises to intellectual property
b. deliberate acts of espionage or trespass
c. acts of human error or failure
d. deliberate acts of theft

ANS: A PTS: 1 REF: 57

48. When an unauthorized individual gains access to information that an organization is trying to protect, the act is categorized as a(n) ____.
a. deliberate act of espionage or trespass
b. act of human error or failure
c. deliberate act of information extortion
d. deliberate act of theft

ANS: A PTS: 1 REF: 57

49. A(n) ____ is an act or event that exploits a vulnerability.
a. attack
b. exploit
c. threat
d. theft

ANS: A PTS: 1 REF: 59

50. A(n) ____ damages or steals an organization's information or physical asset.
a. attack culprit
b. threat entity
c. catalyst
d. threat agent

ANS: D PTS: 1 REF: 59

51. A(n) ____ is a technique or mechanism used to compromise a system.

a. exploit
b. signature
c. design
d. program

ANS: A PTS: 1 REF: 59

52. An identified weakness of a controlled system is known as a ____.
a. liability
b. threat
c. vulnerability
d. fault

ANS: C PTS: 1 REF: 59

53. A ____ is a feature left behind by system designers or maintenance staff.
a. virus
b. sniffer
c. worm
d. back door

ANS: D PTS: 1 REF: 59

54. The application of computing and network resources to try every possible combination of characters to crack a password is known as a ____ attack.
a. man-in-the-middle attack
b. denial-of-service (DoS)
c. dictionary attack
d. brute force

ANS: D PTS: 1 REF: 59

55. A ____ attack uses a list of common values to crack a password.
a. dictionary
b. distributed denial-of-service (DDoS)
c. brute force
d. man-in-the-middle

ANS: A PTS: 1 REF: 59

56. A ____ attack involves sending a large number of connection or information requests to a target.
a. man-in-the-middle
b. denial-of-service (DoS)
c. brute force
d. dictionary

ANS: B PTS: 1 REF: 59

57. ____ commonly specify who can access a particular set of information.
a. Data owners
b. Data users
c. Data custodians
d. Security managers

ANS: A PTS: 1 REF: 65

58. ____ are responsible for the security and use of a particular set of information.
a. Data owners
b. Data users
c. Data custodians
d. Security managers

ANS: A PTS: 1 REF: 65

59. ____ work directly with data owners and are responsible for the storage, maintenance and protection of the information.
a. Data owners
b. Data users
c. Data custodians
d. Security managers

ANS: C PTS: 1 REF: 65

60. ____ work with the information to perform their daily jobs supporting the mission of the organization..
a. Data owners
c. Data custodians

b. Data users
d. Security managers

ANS: B PTS: 1 REF: 65

COMPLETION

1. The _____ statement contains a formal set of organizational principles, standards, and qualities.

   ANS: values

   PTS: 1 REF: 40

2. Tactical plans are used to develop _____ plans.

   ANS: operational

   PTS: 1 REF: 45

3. The critical components of the _____ plan include budgeting, resource allocation, and manpower.

   ANS: tactical

   PTS: 1 REF: 45

4. Boards of directors should supervise strategic information security objectives by demanding _____ from the various layers of management on the information security program's effectiveness and adequacy

   ANS: reports

   PTS: 1 REF: 49

5. Boards of directors should Ensure the effectiveness of the corporation's information security _____ through review and approval.

   ANS: policy

   PTS: 1 REF: 50

6. Another significant benefit of information security governance is _____ for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response.

   ANS: accountability

   PTS: 1 REF: 50

7. The Carnegie Mellon University _____ information security governance model begins with a stimulus for change and loops through proposals for future actions.

   ANS: IDEAL

PTS: 1 REF: 52

8. The _____ has the primary responsibility for independent annual audit coordination.

   ANS:
   CISO
   Chief Information Security Officer
   CSO
   Chief Security Officer
   CRO
   Chief Risk Officer

   PTS: 1 REF: 53

9. Top-down information security initiatives must have a(n) _____ — ideally, an executive with sufficient influence to move the project forward, ensure that it is properly managed, and push for its acceptance throughout the organization.

   ANS: champion

   PTS: 1 REF: 55

10. The impetus to begin an SDLC-based project may be _____ that is a response to some activity in the business community, or plan-driven, the result of a carefully-developed planning strategy.

    ANS:
    event-driven
    event driven

    PTS: 1 REF: 55

11. According to Sun Tzu: if you know the _____ and know yourself, you need not fear the results of a hundred battles.

    ANS: enemy

    PTS: 1 REF: 57

12. A(n) _____ is an object, person, or other entity that represents a constant danger to an asset of an organization.

    ANS: threat

    PTS: 1 REF: 57

13. An act or event that exploits a vulnerability is known as a(n) _____.

    ANS: attack

    PTS: 1 REF: 59

14. A technique or mechanism that is used to compromise a system is called a(n) _____.

    ANS: exploit

    PTS: 1 REF: 59

15. A(n) _____ is an identified weakness of a controlled system in which necessary controls are not present or are no longer effective.

    ANS: vulnerability

    PTS: 1 REF: 59

16. In a(n) _____ attack, the attacker uses an e-mail or forged Web site to attempt to extract personal information from a user.

    ANS: phishing

    PTS: 1 REF: 60

17. A technique used to gain unauthorized access to computers, whereby the intruder sends network-level messages to a computer with an IP address indicating that the message is coming from a trusted host is known as a(n) _____ attack.

    ANS: spoofing

    PTS: 1 REF: 60

18. Controls or _____ are used to protect information from attacks by threats; the terms are also often used interchangeably.

    ANS: safeguards

    PTS: 1 REF: 61-62

19. Data _____ are responsible for the security and use of a particular set of information.

    ANS: owners

    PTS: 1 REF: 65

20. In _____ testing, security personnel simulate or perform specific and controlled attacks to compromise or disrupt their own systems by exploiting documented vulnerabilities.

    ANS: penetration

    PTS: 1 REF: 67

ESSAY

1. Information security governance yields significant benefits. List five.

ANS:
1. An increase in share value for organizations
2. Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels
3. Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care
4. Optimization of the allocation of limited security resources
5. Assurance of effective information security policy and policy compliance
6. A firm foundation for efficient and effective risk management, process improvement, and rapid incident response
7. A level of assurance that critical decisions are not based on faulty information
8. Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response.

PTS: 1 REF: 50

2. Describe what happens during each phase of the IDEAL General governance framework.

ANS:
Initiating - Lay the groundwork for a successful improvement effort.
Diagnosing - Determine where you are relative to where you want to be.
Establishing - Plan the specifics of how you will reach your destination.
Acting - Do the work according to the plan.
Learning - Learn from the experience and improve your ability to adopt new improvements in the future.

PTS: 1 REF: 52

3. List the twelve categories of threats to information security and provide an example of each.

ANS:

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

PTS: 1 REF: 57