Chapter 02 - Planning for 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: 40

2. A clearly directed strategy flows from top to bottom rather than from bottom to top.

   ANS: T PTS: 1 REF: 41

3. A top-down approach to information security usually begins with a systems administrator’s attempt to improve the security of their systems.

   ANS: F PTS: 1 REF: 53

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

   ANS: F PTS: 1 REF: 66

5. Penetration testing is often conducted by contractors, who are commonly referred to as black-hats.

   ANS: F PTS: 1 REF: 67

MULTIPLE CHOICE

1. Which of the following 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: 40

2. Which type of planning is the primary tool in determining the long-term direction taken by an organization?
   a. strategic
   b. tactical
   c. operational
   d. managerial

   ANS: A PTS: 1 REF: 41

3. Which of the following is true about planning?
   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: 42

4. In which level of planning are budgeting, resource allocation, and manpower critical components?
   a. strategic
   b. operational
   c. organizational
   d. tactical

ANS: D PTS: 1 REF: 43

5. Which type of planning is used to organize the ongoing, day-to-day performance of tasks?
a. Strategic
b. Tactical
c. Organizational
d. Operational

ANS: D PTS: 1 REF: 43

6. The basic outcomes of InfoSec governance should include all but which of the following?
a. Value delivery by optimizing InfoSec 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. Time management by aligning resources with personnel schedules and organizational objectives
d. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively

ANS: C PTS: 1 REF: 46

7. 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. Hold regular meetings with the CIO to discuss tactical InfoSect planning
b. Assign InfoSec to a key committee and ensure adequate support for that committee
c. Ensure the effectiveness of the corporation's InfoSec policy through review and approval
d. Identify InfoSec leaders, hold them accountable, and ensure support for them

ANS: A PTS: 1 REF: 46

8. Which of the following should be included in an InfoSec governance program?
a. An InfoSec time management policy
b. An InfoSec risk management methodology
c. An InfoSec project management assessment from an outside consultant
d. All of these are components of the InfoSec governance program

ANS: B PTS: 1 REF: 46-47

9. 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: 48

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

ANS: B PTS: 1 REF: 48

11. Which of the following is an information security governance responsibility of the Chief Security Officer?
a. Communicate policies and the program
b. Set security policy, procedures, programs and training
c. Brief the board, customers and the public

d. Implement policy, report security vulnerabilities and breaches

ANS: B PTS: 1 REF: 49

12. Which of the following is a key advantage of the bottom-up approach to security implementation?
a. strong upper-management support
b. a clear planning and implementation process
c. utilizes the technical expertise of the individual administrators
d. coordinated planning from upper management

ANS: C PTS: 1 REF: 53

13. Which of the following is a key step needed in order for a JAD approach to be successful?
a. prepare software demonstrations
b. organize workshop activities
c. provide sequence-driven policies
d. use event-driven procedures

ANS: B PTS: 1 REF: 54

14. In which model in the SecSDLC does the work products of each phase fall into the next phase to serve as its starting point?
a. continuous
b. cycle-based
c. circular
d. waterfall

ANS: D PTS: 1 REF: 55

15. What is the first phase of the SecSDLC?
a. analysis
b. investigation
c. logical design
d. physical design

ANS: B PTS: 1 REF: 55

16. In which phase of the SecSDLC does the risk management task occur?
a. physical design
b. implementation
c. investigation
d. analysis

ANS: D PTS: 1 REF: 56

17. Blackmail threat of informational disclosure is an example of which threat category?
a. Espionage or trespass
b. Information extortion
c. Sabotage or vandalism
d. Compromises of intellectual property

ANS: B PTS: 1 REF: 57

18. Which of the following is a feature left behind by system designers or maintenance staff that allows quick access to a system at a later time by bypassing access controls?
a. brute force
b. DoS
c. back door
d. hoax

ANS: C PTS: 1 REF: 59

19. Which type of attack involves sending a large number of connection or information requests to a target?
a. malicious code
b. denial-of-service (DoS)
c. brute force
d. spear fishing

ANS: B PTS: 1 REF: 59

20. Which of the following set the direction and scope of the security process and provide detailed instruction for its conduct?

a. system controls
b. technical controls
c. operational controls
d. managerial controls

ANS: D PTS: 1 REF: 61

COMPLETION

1. The impetus to begin an SDLC-based project may be ____________________, that is, a response to some activity in the business community, inside the organization, or within the ranks of employees, customers, or other stakeholders.

ANS:
event-driven
event driven

PTS: 1 REF: 55

2. A ____________ overflow is an application error that occurs when the system can’t handle the amount of data that is sent.

ANS: buffer

PTS: 1 REF: 59

3. A(n) ___________ attack enables an attacker to extract secrets maintained in a security system by observing the time it takes the system to respond to various queries.

ANS: timing

PTS: 1 REF: 60

4. _________resources include people, hardware, and the supporting system elements and resources associated with the management of information in all its states.

ANS: Physical

PTS: 1 REF: 62

5. The ______________________ phase is the last phase of SecSDLC, but perhaps the most important.

ANS: maintenance and change

PTS: 1 REF: 65

6. 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: 66-67

MATCHING

a. attack
b. data owner
c. exploit
d. plan-driven
e. risk assessment
f. risk management
g. strategic planning
h. operational controls
i. technical controls
j. threat agent

1. usually a documented way to circumvent controls or take advantage of weaknesses in control systems
2. the process of moving an organization towards its vision by accomplishing its mission
3. an act that is an intentional or unintentional attempt to compromise the information and/or the systems that support it
4. assigns a comparative risk rating or score to each specific information asset
5. measures that use or implement a technical solution to reduce risk of loss in an organization
6. individual who determines the level of classification associated with data
7. measures that deal with the functionality of security in an organization
8. associated with assessing risks and then implementing or repairing controls to assure the confidentiality, integrity, and availability of information
9. a specific instance or component that represents a danger to an organization’s assets
10. the impetus for a project that is the result of a carefully developed planning strategy

1.	ANS: C	PTS: 1	REF: 59
2.	ANS: G	PTS: 1	REF: 41
3.	ANS: A	PTS: 1	REF: 59
4.	ANS: E	PTS: 1	REF: 60
5.	ANS: I	PTS: 1	REF: 62
6.	ANS: B	PTS: 1	REF: 64
7.	ANS: H	PTS: 1	REF: 61
8.	ANS: F	PTS: 1	REF: 60
9.	ANS: J	PTS: 1	REF: 59
10.	ANS: D	PTS: 1	REF: 55

SHORT ANSWER

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: 46

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: 48

3. There are twelve categories of threats to information security. List five of them and provide an example of each.

ANS:

Threat category	Example
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes,
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, etc.
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

PTS: 1 REF: 57

4. What is the role of planning in InfoSec management? What are the factors that affect planning?

ANS:
Planning usually involves many interrelated groups and organizational processes. The groups involved in planning represent the three communities of interest; they may be internal or external to the organization and can include employees, management, stockholders, and other outside stakeholder. Among the factors that affect planning are the physical environment, the political and legal environment, the competitive environment, and the technological environment.

PTS: 1 REF: 37-38

5. What is the values statement and what is its importance to an organization?

ANS:
One of the first positions that management must articulate is the values statement. The trust and confidence of stakeholders and the public are important factors for any organization. By establishing a formal set of organizational principles and qualities in a values statement, as well as benchmarks for measuring behavior against these published values, an organization makes its conduct and performance standards clear to its employees and the public.

PTS: 1 REF: 39

6. Contrast the vision statement with the mission statement.

ANS:
If the vision statement states where the organization wants to go, the mission statement describes how it wants to get there.

PTS: 1 REF: 41

7. How does tactical planning differ from strategic planning?

ANS:
Tactical planning has a more short-term focus than strategic planning—usually one to three years. It breaks down each applicable strategic goal into a series of incremental objectives. Each objective should be specific and ideally will have a delivery date within a year.

PTS: 1 REF: 43

8. According to the ITGI, what are the four supervisory tasks a board of directors should perform to ensure strategic InfoSec objectives are being met?

ANS:
Inculcate a culture that recognizes the criticality of information and InfoSec to the organization
Verify that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
Assure that a comprehensive InfoSec program is developed and implemented
Demand reports from the various layers of management on the InfoSec program's effectiveness and adequacy

PTS: 1 REF: 45

9. Describe the key approaches organizations are using to achieve unified ERM.

ANS:
Combining physical security and InfoSec under one leader as one business function
Using separate business functions that report to a common senior executive
Using a risk council approach to provide a collaborative approach to risk management

PTS: 1 REF: 49-50

10. What is necessary for a top-down approach to the implementation of InfoSec to succeed?

ANS:
For any top-down approach to succeed, high-level management must buy into the effort and provide its full support to all departments. Such an initiative must have a champion—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.

PTS: 1 REF: 54