TRUE/FALSE

1. Policies are put in place to support the organization's mission, vision, and strategic planning.

   ANS: T PTS: 1 REF: 36

2. The details of the allowable use of company-owned networks and the Internet would most likely be covered in the enterprise information security policy.

   ANS: F PTS: 1 REF: 38

3. A security framework specifies the tasks for deploying security tools in the order in which they are to be accomplished.

   ANS: F PTS: 1 REF: 41

4. Within the IETF, the Security Area Working Group acts as an advisory board for security topics that affect the various Internet-related protocols.

   ANS: T PTS: 1 REF: 47

5. Attack profiles should include scenarios depicting a typical attack, with details on the method, the indicators, and the broad consequences of the attack.

   ANS: T PTS: 1 REF: 55

MULTIPLE CHOICE

1. Practices, procedures, and guidelines effectively explain how to comply with ____.
   a. standards
   b. policies
   c. vision
   d. security blueprints

   ANS: B PTS: 1 REF: 35

2. The ____ of an organization is a written statement of its purpose.
   a. mission
   b. vision
   c. strategy
   d. policy

   ANS: A PTS: 1 REF: 36

3. The ____ is an executive-level document, usually drafted by or at least in cooperation with the organization's chief information officer.
   a. EISP
   b. ISSP
   c. managerial guidance SysSP
   d. technical specification SysSP

   ANS: A PTS: 1 REF: 37

4. The ____ is created by a systems administer to direct practices with many details.
   a. EISP
   b. ISSP
   c. managerial guidance SysSP
   d. technical specification SysSP

ANS: D PTS: 1 REF: 40

5. ____ are the specific instructions entered into a security system to regulate how it reacts to the data it receives.
   a. Access control matrices
   b. Capability rules
   c. Configuration rules
   d. Access control lists

   ANS: C PTS: 1 REF: 41

6. A security ____ is an outline of the overall information security strategy and a roadmap for planned changes to the organization's information security environment.
   a. policy
   b. blueprint
   c. standard
   d. framework

   ANS: D PTS: 1 REF: 41

7. The document ____ makes recommendations for establishing firewall policies and for selecting, configuring, testing, deploying, and managing firewall solutions.
   a. SP 800-53 A, Jul 2008: Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans
   b. SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations
   c. SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy
   d. SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

   ANS: C PTS: 1 REF: 45

8. The document ____ provides a systems developmental lifecycle approach to security assessment of information systems.
   a. SP 800-53 A, Jul 2008: Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans
   b. SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations
   c. SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy
   d. SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

   ANS: A PTS: 1 REF: 46

9. RFC 2196: Site Security Handbook is produced by ____.
   a. the ISO
   b. NIST
   c. the Security Area Working Group
   d. the Federal Agency Security Practices

   ANS: C PTS: 1 REF: 47

10. The ____ illustrates the ways in which people access information.
    a. sphere of use
    b. sphere of protection
    c. working control
    d. benchmark

    ANS: A PTS: 1 REF: 48

11. Within a SETA program, ____ is only available to some of the organization's employees.
    a. security-related trinkets
    b. security education
    c. security training
    d. security awareness programs

ANS: B PTS: 1 REF: 49

12. A(n) ____ plan addresses the identification, classification, response, and recovery from an incident.
    a. incident response
    b. disaster recovery
    c. attack profile
    d. business impact analysis

    ANS: A PTS: 1 REF: 51

13. The ____ plan typically focuses on restoring systems at the original site after disasters occur..
    a. DR
    b. IR
    c. BC
    d. BIA

    ANS: A PTS: 1 REF: 52

14. The first phase in the development of the contingency planning process is the ____.
    a. crisis plan
    b. disaster recovery plan
    c. incident response plan
    d. business impact analysis

    ANS: D PTS: 1 REF: 53

15. A(n) ____ is detailed description of the activities that occur during an attack.
    a. sphere of security
    b. contingency plan
    c. attack profile
    d. business impact analysis

    ANS: C PTS: 1 REF: 54

16. The analysis and prioritization of the business functions within the organization's departments, sections, divisions, groups, or other units to determine which are most vital to continued operations is called ____.
    a. an attack profile
    b. business unit analysis
    c. assessment of potential damage
    d. business impact analysis

    ANS: B PTS: 1 REF: 55

17. An attack scenario end case is categorized ____.
    a. as business-ending or salvageable
    b. on a scale of 1-10
    c. according to a grade of A-F.
    d. either as disastrous or not disastrous

    ANS: D PTS: 1 REF: 56

18. A(n) ____ is an attack against an information asset that poses a clear threat to the confidentiality, integrity, or availability of information resources.
    a. incident
    b. disaster
    c. crisis
    d. recovery

    ANS: A PTS: 1 REF: 56

19. When disaster threatens the viability of the organization at the primary site, disaster recovery undergoes a transition into ____.
    a. business continuity
    b. incident response
    c. attack planning
    d. crisis management

    ANS: A PTS: 1 REF: 58

20. ____ planning prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
    a. Business continuity
    b. Incident response
    c. Attack
    d. Crisis management

    ANS: A PTS: 1 REF: 58

21. Establishing a contact number of hot line is an aspect of ____ planning.
    a. business continuity
    b. incident response
    c. attack
    d. crisis management

    ANS: D PTS: 1 REF: 59-60

COMPLETION

1. A(n) _____ is also known as a general security policy, an IT security policy, or an information security policy.

   ANS:
   enterprise information security policy
   EISP
   enterprise information security policy (EISP)

   PTS: 1 REF: 37

2. A(n) _____ is a set of specifications that identifies a piece of technology's authorized users and includes details on the rights and privileges those users have on that technology.

   ANS:
   access control list
   ACL
   access control list (ACL)

   PTS: 1 REF: 40

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

   ANS: framework

   PTS: 1 REF: 41

4. The identification of critical business functions and the resources needed to support them is the cornerstone of the _____ plan.

   ANS:
   business continuity
   BC
   business continuity (BC)

   PTS: 1 REF: 58

5. _____ management differs dramatically from incident response, as it focuses first and foremost on the people involved.

   ANS: Crisis

   PTS: 1 REF: 59

MATCHING

Match each item with a statement below.

a. managerial guidance SysSP document
b. security training
c. incident response
d. business continuity plan
e. information security policy
f. de jure
g. de facto
h. security blueprint
i. business impact analysis

1. Basis for the design, selection, and implementation of all security program elements, including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program.
2. Investigation and assessment of the impact that various attacks can have on the organization.
3. Set of rules for the protection of an organization's information assets.
4. Provides detailed information and hands-on instruction to employees to prepare them to perform their duties securely.
5. Ensures that critical business functions continue if a catastrophic incident or disaster occurs.
6. Informal part of an organization's culture.
7. Created by management to guide the implementation and configuration of a specific technology so as to direct the way a technology is to be used to control the behavior of people in the organization.
8. The set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
9. Published, scrutinized, and ratified by a group.

1. ANS: H PTS: 1 REF: 41
2. ANS: I PTS: 1 REF: 53
3. ANS: E PTS: 1 REF: 37
4. ANS: B PTS: 1 REF: 50
5. ANS: D PTS: 1 REF: 51-52
6. ANS: G PTS: 1 REF: 35
7. ANS: A PTS: 1 REF: 40
8. ANS: C PTS: 1 REF: 57
9. ANS: F PTS: 1 REF: 35

SHORT ANSWER

1. Explain the difference between a policy and a standard.

   ANS:

A policy is a set of guidelines or instructions that an organization's senior management implements to regulate the activities of the organization members who make decisions, take actions, and perform other duties. Policies are the organizational equivalent of public laws in that they dictate acceptable and unacceptable behavior within an organization. Like laws, policies define what is right and what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, although they have the same compliance requirement as policies, are more detailed descriptions of what must be done to comply with policy.

PTS: 1 REF: 35

2. What criteria must a policy meet to be considered effective and legally enforceable?

ANS:
Dissemination (distribution)
Review (reading)
Comprehension (understanding)
Compliance (agreement)
Uniform enforcement

PTS: 1 REF: 36

3. How does an EISP address an organization's need to comply with laws and regulations?

ANS:
1. General compliance by ensuring the organization establishes suitable programs and assigns responsibilities to identified organizational units
2. Identification of specific penalties and disciplinary actions for deviations from policy

PTS: 1 REF: 37

4. What topics might an ISSP cover?

ANS:
Use of company-owned networks and the Internet
Use of telecommunications technologies (fax and phone)
Use of electronic mail
Specific minimum configurations of computers to defend against worms and viruses
Prohibitions against hacking or testing organization security controls
Home use of company-owned computer equipment
Use of personal equipment on company networks
Use of photocopy equipment

PTS: 1 REF: 38

5. Explain what might happen if managerial guidance SysSP documents have not been written or provided to technical staff.

ANS:

Imagine that management fails to convey to the firewall technicians its intent with respect to the firewall's technical configuration. In the absence of such guidance, the technicians will rely on their own experiences and training to select rules they feel are appropriate. The organization will then experience numerous problems if and when business needs conflict with the technicians' perception of the security function of a firewall. If this were an organization with a need for ultra-high security, such as a Department of Defense contractor, and if the technicians developed a set of firewall rules with an intermediate degree of control, the organization might find itself underprotected, having a need for a high degree of control. On the other hand, with the same set of intermediate-level rules, an organization with an open environment, such as an academic institution, might find itself overly restricted, with the flow of information stifled. This wide range of possible needs is why it's necessary to carefully direct the development, implementation, and configuration of all technologies in the organization, especially security technologies

PTS: 1 REF: 40

6. Explain how access control lists might be implemented.

ANS:
A capability table specifies the subjects and objects that users or groups can access; in some systems, capability tables are called user profiles or user policies. These specifications frequently take the form of complex matrices, rather than simple lists or tables. The access control matrix combines capability tables and ACLs, so that organizational assets are listed along the vertical axis while users are listed along the horizontal axis. The resulting matrix contains ACLs in columns for a particular device or asset, while a row contains the capability table for a particular user.

PTS: 1 REF: 40-41

7. List the sections of the ISO/IEC 27002.

ANS:
1. Risk Assessment and Treatment
2. Security Policy
3. Organization of Information Security
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations
8. Access Control
9. Information Systems Acquisition, Development, and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

PTS: 1 REF: 42

8. What are spheres of security? Provide examples illustrating the different components.

ANS:

Spheres of security are the generalized foundation of a good security framework and can be considered a type of best practice recommendation. Generally speaking, they illustrate how information is under attack from a variety of sources. The sphere of use, illustrates the ways in which people access information. For example, systems users are intended to access information through systems. Information, the most important asset, is at the center of the sphere. It is always at risk from the people and computer systems that have access to it. Networks and the Internet represent indirect threats, because a person attempting to access information from the Internet must first go through the local networks and then access systems that contain the information. The sphere of protection, shows that between each layer of the sphere of use there must exist a layer of protection to prevent the outer layer from accessing the inner layer. Each shaded band is a layer of protection and control. For example, the items labeled "Policy & law" and "Education & training" are located between people and the information.

PTS: 1 REF: 48

9. Describe the benefits of a security newsletter.

ANS:
The security newsletter is the most cost-effective method of disseminating security information and news to the employee. Newsletters can be distributed via hard copy, e-mail, or intranet. Newsletter topics can include information about new threats to the organization's information assets, the schedule for upcoming security classes, and security personnel updates. The goal is to keep the idea of information security in users' minds and to stimulate users to care about security. If a security awareness program is not actively implemented, employees may begin to neglect security matters, and the risk of employee accidents and failures is likely to increase.

PTS: 1 REF: 51

10. List and describe the four phases of incident response.

ANS:
1. Planning—getting ready to handle incidents
2. Detection—identifying that an incident has occurred
3. Reaction—responding to the immediate threat of an incident and regaining control of information assets
4. Recovery—getting things "back to normal," resolving the damage done during the incident, and understanding what happened to prevent reoccurrence

PTS: 1 REF: 57