TRUE/FALSE

1. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object.

   ANS: T PTS: 1 REF: 4

2. Once intellectual property (IP) has been defined and properly identified, breaches in the controls that have been placed around the IP constitute a threat to the security of this information.

   ANS: T PTS: 1 REF: 5

3. IRP focuses more on preparations completed before and actions taken after the incident, whereas DRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

   ANS: F PTS: 1 REF: 25

4. The vision of an organization is a written statement of an organization's purpose.

   ANS: F PTS: 1 REF: 31

5. An information security policy provides rules for the protection of the information assets of the organization.

   ANS: T PTS: 1 REF: 31

MULTIPLE CHOICE

1. The ____ has been the industry standard for computer security since the development of the mainframe.
   a. disaster recovery plan
   b. C.I.A. triangle
   c. strategic plan
   d. asset classification

   ANS: B PTS: 1 REF: 3

2. ____ ensures that only those with the rights and privileges to access information are able to do so.
   a. Confidentiality
   b. Availability
   c. Integrity
   d. Risk assessment

   ANS: A PTS: 1 REF: 3

3. The threat of corruption can occur while information is being stored or transmitted. ____ is the prevention of that corruption.
   a. Risk assessment
   b. Availability
   c. Integrity
   d. Confidentiality

   ANS: C PTS: 1 REF: 3

4. ____ enables authorized users - persons or computer systems - to access information without interference or obstruction, and to receive it in the required format.

a. Integrity
b. Availability
c. Confidentiality
d. Risk assessment

ANS: B PTS: 1 REF: 3

5. A(n) ____ is a category of objects, persons, or other entities that pose a potential risk of loss to an asset.
a. payload
b. intellectual property
c. Trojan horse
d. threat

ANS: D PTS: 1 REF: 4

6. ____ is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas".
a. Avoidance
b. Trojan horse
c. Malware
d. Intellectual property

ANS: D PTS: 1 REF: 5

7. ____ hack systems to conduct terrorist activities through network or Internet pathways.
a. Cyberterrorists
b. Script kiddies
c. Programmers
d. Social engineers

ANS: A PTS: 1 REF: 6

8. A ____ attack seeks to deny legitimate users access to services by either tying up a server's available resources or causing it to shut down.
a. Trojan horse
b. DoS
c. social engineering
d. spyware

ANS: B PTS: 1 REF: 7

9. ____ is the process of examining and documenting the security posture of an organization's information technology and the risks it faces.
a. Risk identification
b. Data classification
c. Security clearance
d. DR

ANS: A PTS: 1 REF: 11

10. ____ assigns a risk rating or score to each information asset. While this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process.
a. BC
b. Risk assessment
c. DR
d. Avoidance

ANS: B PTS: 1 REF: 18

11. ____ is the risk control strategy that attempts to prevent the exploitation of the vulnerability.
a. Acceptance
b. Transference
c. Avoidance
d. Mitigation

ANS: C PTS: 1 REF: 21

12. ____ is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.
a. Transference
c. Acceptance

b. Mitigation
d. Avoidance

ANS: A PTS: 1 REF: 22

13. ____ is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
a. Avoidance
c. Acceptance
b. Transference
d. Mitigation

ANS: D PTS: 1 REF: 22

14. ____ of risk is the choice to do nothing to protect a vulnerability, and to accept the outcome of its exploitation.
a. Inheritance
c. Avoidance
b. Acceptance
d. Mitigation

ANS: B PTS: 1 REF: 23

15. A(n) ____ is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization, and, subsequently, to restore the organization to normal modes of business operations.
a. threat
c. contingency plan
b. social plan
d. asset

ANS: C PTS: 1 REF: 23

16. A(n) ____ is an investigation and assessment of the impact that various attacks can have on the organization.
a. BIA
c. incident
b. intellectual property
d. threat

ANS: A PTS: 1 REF: 24

17. A(n) ____ is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability.
a. threat
c. worm
b. Trojan horse
d. incident

ANS: D PTS: 1 REF: 24

18. A ____ deals with the preparation for and recovery from a disaster, whether natural or man-made.
a. mitigation plan
c. risk management
b. disaster recovery plan
d. risk assessment

ANS: B PTS: 1 REF: 25

19. A ____ is a document that expresses how an organization ensures that critical business functions continue at an alternate location while the organization recovers its ability to function at the primary site if a catastrophic incident or disaster occurs.
a. risk assessment plan
c. Trojan horse
b. business continuity plan
d. worm

ANS: B PTS: 1 REF: 25

20. A(n) ____ is a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization.
    a. policy
    b. assessment
    c. asset
    d. residual risk

    ANS: A PTS: 1 REF: 30

21. ____ is the process of moving the organization toward its vision.
    a. Transference
    b. Avoidance
    c. Strategic planning
    d. Mitigation

    ANS: C PTS: 1 REF: 31

COMPLETION

1. _____ is defined by the Committee on National Security Systems (CNSS) as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

   ANS: Information security

   PTS: 1 REF: 3

2. Information has the characteristic of _____ when disclosure or exposure to unauthorized individuals or systems is prevented.

   ANS: confidentiality

   PTS: 1 REF: 3

3. _____ is the process of applying controls to reduce the risks to an organization's data and information systems.

   ANS: Risk control

   PTS: 1 REF: 11

4. _____ is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components in the organization's information system.

   ANS: Risk management

   PTS: 1 REF: 12

5. For the purpose of relative risk assessment, _____ *equals* likelihood of vulnerability occurrence *times* value (or impact) *minus* percentage risk already controlled *plus* an element of uncertainty.

   ANS: risk

   PTS: 1 REF: 20

MATCHING

Match each item with a statement below.

a. Threat agent
b. Intellectual property
c. Hacker
d. Computer viruses
e. Trojan
f. Risk management
g. Likelihood
h. Residual risk
i. Standards

1. A specific and identifiable instance of a general threat.
2. Detailed statements of what must be done to comply with policy.
3. A person who uses and creates computer software to gain access to information illegally.
4. Something that looks like a desirable program or tool, but that is in fact a malicious entity.
5. The probability that a specific vulnerability within an organization will be successfully attacked.
6. The risk that remains to the information asset even after the existing control has been applied.
7. Includes trade secrets, copyrights, trademarks, and patents.
8. The process used to identify and then control risks to an organization's information assets.
9. Segments of code that perform malicious actions.

1. ANS: A PTS: 1 REF: 4
2. ANS: I PTS: 1 REF: 30
3. ANS: C PTS: 1 REF: 6
4. ANS: E PTS: 1 REF: 8
5. ANS: G PTS: 1 REF: 18
6. ANS: H PTS: 1 REF: 20
7. ANS: B PTS: 1 REF: 5
8. ANS: F PTS: 1 REF: 11
9. ANS: D PTS: 1 REF: 7

SHORT ANSWER

1. What are some of the criteria to be considered when conducting an information asset valuation?

   ANS:
   Among the criteria to be considered are:

   Which information asset is the most critical to the success of the organization?
   Which information asset generates the most revenue?
   Which information asset generates the most profitability?
   Which information asset would be the most expensive to replace?
   Which information asset would be the most expensive to protect?
   Which information asset would be the most embarrassing or cause the greatest liability if revealed?

   PTS: 1 REF: 15

2. Once the project team for information security development creates a ranked vulnerability worksheet, the team must choose one of four basic strategies to control each of the risks that result from these vulnerabilities. List the four strategies.

   ANS:

The four strategies are as follows:

Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability (avoidance).
Transfer the risk to other areas or to outside entities (transference).
Reduce the impact should the vulnerability be exploited (mitigation).
Understand the consequences and accept the risk without control or mitigation (acceptance).

PTS: 1 REF: 21

3. What are the subordinate functions of contingency planning?

ANS:
Contingency planning involves four subordinate functions:

Business impact assessment
Incident response planning
Disaster recovery planning
Business continuity planning

PTS: 1 REF: 23

4. What are the steps in contingency planning?

ANS:
1. The IR plan focuses on immediate response, but if the attack escalates or is disastrous (such as a fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and business continuity.

2. The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan.

3. The BC plan runs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

PTS: 1 REF: 26

5. What is difference between access control lists and configuration rules?

ANS:
Access control lists (ACLs): Lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.

Configuration rules: The specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

PTS: 1 REF: 34

6. What are some of the key elements that a security policy should have in order to remain viable?

ANS:

An individual (like a policy administrator) responsible for the creation, revision, distribution, and storage of the policy; this individual should solicit input from all communities of interest in policy development

A schedule of reviews to ensure currency and accuracy, and to demonstrate due diligence

A mechanism by which individuals can comfortably make recommendations for revisions, preferably anonymously

A policy and revision date and possibly a "sunset" expiration date

Optionally, policy management software to streamline the steps of writing policy, tracking the workflow of policy approvals, publishing policy once it is written and approved, and tracking when individuals have read the policy

PTS: 1 REF: 35

7. What is a polymorphic threat?

ANS:
A polymorphic threat is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and appearance to elude detection by antivirus software programs. This means that an e-mail generated by the virus may not match previous examples, making detection more of a challenge.

PTS: 1 REF: 8

8. What is the difference between transference and mitigation?

ANS:
Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations. Mitigation is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

PTS: 1 REF: 22

9. What is the difference between a disaster recovery plan and a business continuity plan?

ANS:
A disaster recovery (DR) plan deals with the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan is a document that expresses how an organization ensures that critical business functions continue at an alternate location while the organization recovers its ability to function at the primary site if a catastrophic incident or disaster occurs.

PTS: 1 REF: 25

10. What is the difference between avoidance of risk and acceptance of risk?

ANS:
Avoidance is the risk control strategy that attempts to prevent the exploitation of the vulnerability. This is the preferred approach, and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. Acceptance of risk is the choice to do nothing to protect a vulnerability, and to accept the outcome of its exploitation.

PTS: 1 REF: 21 | 23