1. The key attribute in security analysis is the identification of assets. While all of the following definitions are technically correct, when discussing information assurance an asset is BEST defined as:

a. A useful resource in an organization other than your own.

*b. Anyone or anything requiring protection within a respective organization.

c. Items of monetary value.

d. Computer hardware.

2. The original acronym for computer security in the 1980s (before INFOSEC, now information assurance) was _____, which was based off of the acronym _____.

a. COMSEC, INFOSEC

b. IA, COMSEC

*c. COMPUSEC, COMSEC

d. OSINT, COMPUSEC

3. In what step of the disaster recovery plan are the executives in an organization briefed on the plan and their roles in it?

a. Step 5

b. Step 4

c. Step 3

*d. Step 6

4. The value brought to the field of information assurance by the McCumber Cube is:

a. A security-based approach that is technology-specific.

*b. An information-based approach that applies regardless of the technology employed.

c. A systems-oriented approach that evolves with current technology.

d. A science-based approach that re-evaluates the model with every new

technological discoveries.

5. The McCumber cube constitutes a comprehensive risk assessment process.

a. True
*b. False

6. McCumber (2005) repudiates previous models such as the Bell-LaPadula model and the Rainbow Series (beginning with "the Orange Book"), and the Common Criteria as being insufficient for information assurance.

*a. True
b. False

7. The McCumber Cube methodology is an alternative to the risk assessment process.

a. True
*b. False

8. Which of these is NOT an element of the risk management process according to McCumber 2005 ?

*a. Non-repudiation

b. Threat

c. Vulnerability

d. Asset

9. According to McCumber (2005), security is a binary notion. That is, a system is either secure or it is not secure.

a. True
*b. False

1. Five out of every ten organizations surveyed have been through a disaster.

a. true
*b. false

2. A good public image is an asset that takes years to achieve and considerable diligence to maintain.

*a. true
b. false

3. Developing a solid disaster recovery plan only

requires the support of an organization's upper managers.

a. true
*b. false

4. Planners must continually evaluate new threats and business conditions as they develop.

*a. true
b. false

5. Disaster recovery planning can be broken down into 10 major steps.

a. true
*b. false

6. In general, three major groups staff an organization's disaster recovery function.

*a. true
b. false

7. In organizations of 250 or fewer employees, a centralized office of disaster recovery is probably not necessary.

a. true
*b. false

8. All business processes must be identified and analyzed during a business impact analysis.

*a. true
b. false

9. Most managers surveyed think that testing and rehearsing recovery plans are not beneficial.

a. true
*b. false

10. IT and network managers help develop and deliver training to department managers and employees who will assist in recovery procedures for computer systems and networks.

*a. true
b. false

11. In which step of disaster recovery planning should the team be trained in disaster recovery planning?

*a. Organizing the team
b. Developing policies and procedures
c. Preparing to handle disasters
d. Ongoing management

12. In which step of disaster recovery planning are all business processes identified and analyzed?

*a. Assessing risks in the enterprise
b. Developing policies and procedures
c. Preparing to handle disasters
d. Ongoing management

13. In which step of disaster recovery planning does the planning team determine the contribution that each department can make to the plan and disaster recovery?

a. Organizing the team
b. Developing policies and procedures
*c. Establishing roles across departments and organizations
d. Ongoing management

14. In which step of disaster recovery planning does the planning team determine the interdependency of each department and organization involved?

a. Organizing the team
b. Establishing roles across departments and organizations
*c. Developing policies and procedures
d. Documenting disaster recovery procedures

15. In which step of disaster recovery planning is each policy and procedure drafted, reviewed, and approved by management and all of the departments and organizations responsible for its implementation?

a. Organizing the team
b. Assessing risks in the enterprise
*c. Documenting disaster recovery procedures
d. Preparing to handle disasters

16. In which step of disaster recovery planning is the final plan distributed to all of the departments, organizations, and employees involved in disaster response and recovery?

a. Organizing the team

b. Developing policies and procedures
c. Documenting disaster recovery procedures
*d. Preparing to handle disasters

17. In which step of disaster recovery planning do all departments and support organizations run through the entire disaster recovery process?

a. Organizing the team
b. Developing policies and procedures
c. Preparing to handle disasters
*d. Training, testing, and rehearsal

18. In which step of disaster recovery planning does the planning team assess the emergence of new threats, adjust for changes in organizational structure, and determine the impact of new technology on recovery procedures?

*a. Ongoing management
b. Organizing the team
c. Assessing risks in the enterprise
d. Training, testing, and rehearsal

19. What do IT and network managers do during risk assessment and business impact analysis?

a. Determine how many IT staff need to be on the team
*b. Help answer questions about potential consequences from system downtime
c. Help develop and deliver training to department managers and employees
d. Support and manage the ongoing disaster recovery plan

20. During a business impact analysis, how are business processes ranked?

a. Necessary, critical, essential, desirable
*b. Critical, essential, necessary, desirable
c. Essential, critical, necessary, desirable
d. Desirable, necessary, essential, critical

21. In which step of disaster recovery planning should legal and contractual requirements be reviewed?

a. Organizing the team
b. Developing policies and procedures
*c. Assessing risks in the enterprise

d. Preparing to handle disasters

22. The planning team must establish procedures for communicating with which of the following?

*a. Employees
b. Media
c. Law enforcement
d. Emergency services
e. All of the above