Cyber Security

1) Which one of the following exposures associated with the spooling of sensitive reports for offline printing could be considered the most serious?
    a. other unauthorized copies of reports could be printed
    b. sensitive data may be read by operators
    c. data cannot be altered without authorization
    d. output would be lost in case of system failure

    Competency: Defend and attack

2) Which one of the following is **not** a common integrity goal?
    a. maintain internal and external consistency
    b. prevent unauthorized users from making modifications
    c. prevent paths that could lead to inappropriate disclosure
    d. prevent authorized users from making improper modifications

    Competency: Network security

3) What is the Biba security model concerned with?
    a. confidentiality
    b. integrity
    c. reliability
    d. availability

    Competency: Public key

4) Attributable data should be:
    a. often traced to individuals responsible for observing and recording the data
    b. sometimes traced to individuals responsible for observing and recording the data
    c. never traced to individuals responsible for observing and recording the data
    d. always traced to individuals responsible for observing and recording the data

    Competency: Public key

5) Which one of the following is **not** a method to protect objects and the data within the objects?
    a. data mining
    b. layering
    c. abstraction
    d. data hiding

Competency: Authentication

6) What does it mean if a system uses "Trusted Recovery"?
    a. A failure or crash of the system cannot be used to breach security.
    b. A single account on the system has the administrative rights to recover or reboot the system after a crash.
    c. The recovery process is done from media that have been locked in a safe.
    d. There is no such principle as "Trusted Recovery" in security.

Competency: Disaster recovery

7) Which one of the following questions is less likely to help in assessing controls covering audit trails?
    a. Is access to online logs strictly controlled?
    b. Does the audit trail provide a trace of user actions?
    c. Are incidents monitored and tracked until resolved?
    d. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Competency: Disaster recovery

8) What is a locking device that prevents unauthorized unplugging of cables from computer devices called?
    a. cable trap
    b. door delay
    c. slot locks
    d. preset locks

Competency: Physical security

9) When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
    a. They both involve rewriting the media
    b. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
    c. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
    d. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Competency: Forensics security

10) The Information Technology Security Evaluation Criteria (ITSEC) was written to address which one of the following that the Orange Book did **not** address?
    a. integrity and availability
    b. integrity and confidentiality
    c. confidentiality and availability
    d. accessibility and confidentiality

Competency: Cyber security policy

ANSWER KEY

1. A
2. C
3. B
4. D
5. A
6. A
7. C
8. A
9. C
10. A