Certified in Cybersecurity Practice Quiz

1. Is it possible to avoid risk?

   A. Yes

   B. No

   C. Sometimes

   D. Never

The correct answer is A. To avoid an identified risk, stop doing what you have identified as being too risky or dangerous and not acceptable to the organization.

2. What is meant by non-repudiation?

   A. If a user does something, they can't later claim that they didn't do it.

   B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.

   C. It is part of the rules set by administrative controls.

   D. It is a security feature that prevents session replay attacks.

The correct answer is A. To repudiate means to attempt to deny after the fact, to lie about one's actions.

3. Which of the following is very likely to be used in a disaster recovery effort?

   A. Guard dogs

   B. Data backups

   C. Contract personnel

   D. Antimalware solutions

The correct answer is B. Restoring from backups is often very useful during a DR effort.

4. Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

   A. Routers

   B. Laptops

C. Firewalls

D. Backups

The correct answer is D. Backups are often crucial in DR efforts, so that the normal production environment can be restored.

5. Derrick logs on to a system in order to read a file. In this example, Derrick is the _______.

   A. Subject

   B. Object

   C. Process

   D. Predicate

The correct answer is A. Subjects are entities that access objects.

6. Which of the following is a subject?

   A. A file

   B. A fence

   C. A filename

   D. A user

The correct answer is D. A user is a subject; something trying to get access to objects.

7. Common network device used to connect networks.

   A. Server

   B. Endpoint

   C. Router

   D. Switch

The correct answer is C. Routers are used to connect networks.

8. A common network device used to filter traffic.

   A. Server

   B. Endpoint

   C. Ethernet

D**. Firewall**

The correct answer is D. This is the purpose of a firewall.

9. Who is responsible for publishing and signing the organization’s policies?
   A. The security office
   B. Human resources
   C. Senior management
   D. The legal department

The correct answer is C. Policies are direct organizational mandates from senior management.

10. A set of security controls or system settings used to ensure uniformity of configuration through the IT environment.
    A. Patches
    B. Inventory
    C. Baseline
    D. Policy

The correct answer is C. This is the definition of a baseline.