Cyber Security and Privacy, IIT Madras
Prof. Saji K Mathew

Week 4 Quiz
(All questions carry 1 point each)

1. A facility that provides only rudimentary services, with no computer hardware or peripherals is known as:

a. Cold site
b. Hot site
c. Warm site
d. Service bureau

Ans: a. Cold Site

Explanation: A cold site is a backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place.

2. The amount of effort necessary to make the business function operational after the technology element is recovered is known as:

a. Recovery Time Objective
b. Work Recovery Time
c. Maximum Tolerable Downtime
d. Recovery Point Objective

Ans: b. Work Recovery Time

Explanation: The Work Recovery Time (WRT) is the remainder of the Maximum Tolerable Downtime (MTD) used to restore all business operations.

3. Contingency Planning includes:

a. Incident response plan
b. Disaster recovery plan
c. Business continuity plan
d. All the above

Ans: d. All the above

Explanation: Contingency Planning includes incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP), in preparation for adverse events that become incidents or disasters.

4. An investigation and assessment of the various adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization's core processes and recovery priorities is known as:

a. Risk assessment
b. Business impact analysis
c. Crisis management
d. Incident damage assessment

Ans: b. Business impact analysis

Explanation: BIA helps determine which business functions and information systems are the most critical to the success of the organization.

5. The process that prepares an organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site is known as:
a. Business continuity planning
b. Disaster recovery planning
c. Strategic Planning
d. Operational planning

Ans: a. Business continuity planning

Explanation: The BC plan establishes critical business functions at an alternate site.

6. Which level of Organizational Planning typically addresses day-to-day activities and tasks?
a. Strategic Planning
b. Tactical Planning
c. Operational Planning
d. Top Management Planning

Ans: c. Operational Planning

Explanation: Operational Planning, the bottom level of Organizational Planning, typically addresses day-to-day activities and operational tasks within the organization.

7. The job function of the Chief Information Security Officer includes:

a. Creating a strategic information security plan with a vision for the future of information security.
b. Understanding fundamental business activities performed by the company and suggesting appropriate information security solutions that uniquely protect these activities.
c. Improving the status of information security by developing action plans, schedules, budgets, status reports and top management communications
d. All the above

Ans: d. All the above

Explanation: CISO is typically considered the top information security officer in an organization and has primary responsibility for the assessment, management, and implementation of information security in the organization.

8. What is the unit of analysis in the contingency planning approach?

a. Business Assets
b. Risk Assets
c. Business Processes
d. Risk Factors

Ans: c. Business Processes

Explanation: Unit of Analysis in Contingency Planning Approach is Business Processes whereas its Assets in Risk Management Approach

9. Which of the following is not a possible incident indicator?

a. Presence of unfamiliar files
b. Unusual consumption of computing resources
c. Unusual system crashes
d. Activities at unexpected times

Ans: d. Activities at unexpected times

Explanation: Activities at unexpected times are a probable indicator of an incident

10. What is the purpose of conducting an After Action Review (AAR) in incident response?

a. To review and improve the effectiveness of the DRP
b. To review and improve the effectiveness of the BCP
c. To review and improve the effectiveness of the IRP
d. To notify law enforcement agencies

Ans: c. To review and improve the effectiveness of the IRP

Explanation: AAR is conducted to assess the effectiveness of the Incident Response Plan (IRP) by examining actions taken during the incident, identifying areas for improvement, and refining response procedures for future incidents.