Chapter 2: Planning for Organizational Readiness

TRUE/FALSE

1. Team leaders from the subordinate teams, including the IR, DR, and BC teams, should not be included in the CPMT.

   ANS: F PTS: 1 REF: 50

2. Effective contingency planning begins with effective policy.

   ANS: T PTS: 1 REF: 54

3. A business impact analysis (BIA) identifies threats, vulnerabilities, and potential attacks to determine what controls can protect the information.

   ANS: F PTS: 1 REF: 57

4. A weighted analysis table can be useful in resolving the issue of which business function is the most critical to the organization.

   ANS: T PTS: 1 REF: 58

5. The recovery time objective (RTO) downtime metric is the defined as the point in time to which lost systems and data can be recovered after an outage as determined by the business unit.

   ANS: F PTS: 1 REF: 61

MULTIPLE CHOICE

1. In a CPMT, a(n) ____ should be a high-level manager with influence and resources that can be used to support the project team, promote the objectives of the CP project, and endorse the results that come from the combined effort.
   a. incident manager
   b. champion
   c. crisis manager
   d. project manager

   ANS: B PTS: 1 REF: 50

2. In a CPMT, a(n) ____ leads the project to make sure a sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed.
   a. incident manager
   b. champion
   c. crisis manager
   d. project manager

   ANS: D PTS: 1 REF: 50

3. A CPMT should include _____ who can oversee the security planning of the project and provide information on threats, vulnerabilities, and recovery requirements needed in the planning process.
   a. business managers
   b. human resource managers
   c. physical plant managers
   d. information security managers

   ANS: D PTS: 1 REF: 50

4. Within an organization, a(n) ____ is a group of individuals who are united by shared interests or values and who have a common goal of making the organization function to meet its objectives.
   a. database community
   b. network community
   c. community of interest
   d. incident response community

   ANS: C PTS: 1 REF: 51

5. The ____ job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks.
   a. information technology management and professionals
   b. organizational management and professionals
   c. information security management and professionals
   d. human resource management and professional

   ANS: C PTS: 1 REF: 52

6. The ____ job functions and organizational roles focus on costs of system creation and operation, ease of use for system users, timeliness of system creation, and transaction response time.
   a. information technology management and professionals
   b. organizational management and professionals
   c. information security management and professionals
   d. human resource management and professional

   ANS: A PTS: 1 REF: 52

7. The elements required to begin the ____ process are a planning methodology; a policy environment to enable the planning process; an understanding of the causes and effects of core precursor activities, and access to financial and other resources.
   a. human resource planning
   b. information security planning
   c. relocation planning
   d. contingency planning

   ANS: D PTS: 1 REF: 52

8. The purpose of the ____ is to define the scope of the CP operations and establish managerial intent with regard to timetables for response to incidents, recovery from disasters, and reestablishment of operations for continuity.
   a. incident response policy
   b. contingency planning policy
   c. disaster recovery policy
   d. cross-training policy

   ANS: B PTS: 1 REF: 54

9. The ____ is an investigation and assessment of the impact that various events or incidents can have on the organization.
   a. business impact analysis
   b. threat of attack analysis
   c. forensic analysis
   d. cross-training analysis

   ANS: A PTS: 1 REF: 57

10. The first major business impact analysis task is to analyze and prioritize the organization's business processes based on their relationships to the organization's ____.
    a. mission
    b. budget
    c. downtime metrics
    d. information assets

    ANS: A PTS: 1 REF: 58

11. The ____ is the point in time by which systems and data must be recovered after an outage as determined by the business unit.
    a. recovery point objective
    b. dependency objective
    c. recovery time objective
    d. training objective

    ANS: A PTS: 1 REF: 61

12. The ____ is the period of time within which systems, applications, or functions must be recovered after an outage.
    a. recovery point objective
    b. dependency objective
    c. recovery time objective
    d. training objective

    ANS: C PTS: 1 REF: 61

13. The last stage of a business impact analysis is prioritizing the resources associated with the ____, which brings a better understanding of what must be recovered first.
    a. contingency planning
    b. information assets
    c. mission/business processes
    d. insurance costs

    ANS: C PTS: 1 REF: 63

14. An manual alternative to the normal way of accomplishing an IT task might be employed in the event that IT is unavailable. This is called a ____.
    a. workload shift
    b. business disruption experience
    c. work outflow
    d. work-around procedure

    ANS: D PTS: 1 REF: 65

15. The ____ is used to collect information directly from the end users and business managers.
    a. facilitated data-gathering session
    b. data management session
    c. system log session
    d. forensic analysis

    ANS: A PTS: 1 REF: 71

16. What is a common approach used in the discipline of systems analysis and design to understand the ways systems operate and to chart process flows and interdependency studies?
    a. database diagramming
    b. network diagramming
    c. application diagramming
    d. systems diagramming

    ANS: D PTS: 1 REF: 72

17. One modeling technique drawn from systems analysis and design that can provide an excellent way to illustrate how a business functions is a(n) ____.:
    a. focus group
    b. IT application log
    c. production schedule
    d. collaboration diagram

    ANS: D PTS: 1 REF: 73

18. Which of the following collects and provides reports on failed login attempts, probes, scans, denial-of-service attacks, and detected malware?
    a. departmental reports
    b. financial reports
    c. scheduled reports
    d. system logs

    ANS: D PTS: 1 REF: 75

19. The final component to the CPMT planning process is to deal with ____.

a. BIA data collection
b. prioritizing mission/business processes
c. budgeting for contingency operations
d. identifying recovery priorities

ANS: C PTS: 1 REF: 76

20. To a large extent, incident response capabilities are part of a normal IT budget. The only area in which additional budgeting is absolutely required for incident response is the maintenance of ____.
a. audit documentation
b. redundant equipment
c. BIA questionnaires
d. local area networks

ANS: B PTS: 1 REF: 77

21. Companies may want to consider budgeting for contributions to employee loss expenses (such as funerals) as well as for counseling services for employees and loved ones as part of ____.
a. crisis management budgeting
b. incident response budgeting
c. risk assessment budgeting
d. recovery criticality budgeting

ANS: A PTS: 1 REF: 79

COMPLETION

1. A(n) _____ is the collection of individuals responsible for the overall planning and development of the contingency planning process.

ANS:
contingency planning management team
CPMT
contingency planning management team (CPMT)

PTS: 1 REF: 49

2. The _____ adds insight into what the organization must do to respond to adverse events, minimize the damage from such events, recover from the effects, and return to normal operations.

ANS:
business impact analysis
business impact analysis (BIA)
BIA

PTS: 1 REF: 57

3. A task performed by an organization or organizational subunit in support of the organization's overall mission is referred to as a mission or _____.

ANS: business process

PTS: 1 REF: 58

4. _____ are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

ANS:

Recovery time objectives
Recovery time objectives (RTOs)
RTOs

PTS: 1 REF: 61

5. The downtime metric, _____, is also referred to as maximum acceptable data loss.

ANS:
recovery point objective
RPO
recovery point objective (RPO)

PTS: 1 REF: 61

MATCHING

Match each item with a statement below.

a. Review financial reports and budgets
b. BIA questionnaire
c. Focus group
d. Maximum tolerable downtime
e. Use case diagram
f. System logs
g. Insurance
h. Employee overtime
i. Paid employee leave

1. Includes a function description, impact assessment, work backlog and other items
2. The total amount of time acceptable for process outage or disruption
3. Can provide a description of the attack environment the organization faces
4. Also known as a facilitated data-gathering session
5. Potential crisis management expense
6. A common business continuity expense
7. Modeling technique used to help understand the interactions between entities and business functions
8. Most common method of calculating business impact
9. The number one budgetary expense for disaster recovery

1. ANS: B PTS: 1 REF: 64
2. ANS: D PTS: 1 REF: 60-61
3. ANS: F PTS: 1 REF: 75
4. ANS: C PTS: 1 REF: 71
5. ANS: I PTS: 1 REF: 79
6. ANS: H PTS: 1 REF: 79
7. ANS: E PTS: 1 REF: 72
8. ANS: A PTS: 1 REF: 76
9. ANS: G PTS: 1 REF: 78

SHORT ANSWER

1. Briefly describe the functions of the contingency planning management team.

ANS:
- Obtaining commitment and support from senior management
- Managing and conducting the overall CP process

- Writing the master CP document
- Conducting the business impact analysis (BIA), which includes:
  - Assisting in identifying and prioritizing threats and attacks
  - Assisting in identifying and prioritizing business functions
- Organizing and staffing the leadership for the subordinate teams:
  - Incident response
  - Disaster recovery
  - Business continuity
  - Crisis management
- Providing guidance to and integrating the work of the subordinate teams

PTS: 1 REF: 49-50

2. What are three communities of interest with roles and responsibilities in information security?

ANS:
1. Managers and professionals in the field of information security
2. Managers and professionals in the field of information technology
3. Managers and professionals from general management

PTS: 1 REF: 52

3. What are the elements required to begin contingency planning?

ANS:
The elements required to begin the CP process are a planning methodology; a policy environment to enable the planning process; an understanding of the causes and effects of core precursor activities, known as the business impact analysis (BIA); and access to financial and other resources, as articulated and outlined by the planning budget.

PTS: 1 REF: 52

4. What is the purpose of formal contingency planning policy?

ANS:
The purpose of policy is to define the scope of CP operations and establish managerial intent with regard to timetables for response to incidents, recovery from disasters, and reestablishment of operations for continuity. This policy also establishes responsibility for the development and operations of the CPMT in general, and it may provide specifics on the constituencies of all CP-related teams.

PTS: 1 REF: 54

5. In one or two sentences, define business impact analysis (BIA).

ANS:
Business impact analysis (BIA) is an investigation and assessment of the impact that various events or incidents can have on the organization. A crucial component of the initial planning stages, it also provides a detailed identification and prioritization of critical business functions, which would require protection and continuity in an adverse event.

PTS: 1 REF: 57

6. What are the five “Keys to BIA success” noted by Zawada and Evans that contribute to a successful business impact analysis?

   ANS:
   1. Set the scope for the project carefully. Be sure to consider the functional and administrative units to include, the categories of risks to be addressed, and the range of impacts to be considered.
   2. Initiate a data-gathering process that will find the information senior managers need to make informed decisions.
   3. Seek out objective rather than subjective data. Subjective data can be useful when used by experienced analysts, but facts are important.
   4. Determine the needs of higher management prior to the data collection. The final reported risk assessment and BIA must address those needs to be of value.
   5. Gain validation of the results derived from the risk assessment and BIA from the owners of the business processes being examined, or else the final product many not have their support.

   PTS: 1 REF: 57

7. Briefly describe three key downtime metrics.

   ANS:
   Maximum tolerable downtime (MTD): The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

   Recovery time objective (RTO): The period of time within which systems, applications, or functions must be recovered after an outage. RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

   Recovery point objective (RPO): The point in time to which lost systems and data can be recovered after an outage as determined by the business unit.

   PTS: 1 REF: 60-61

8. How does the length of the recovery time objective (RTO) of a contingency plan affect the possible solutions that can be enacted to meet the RTO? Give an example.

   ANS:
   When plans require a short RTO, the solutions will usually be more expensive to design and use. For example, if a system must be recovered immediately, it will have an RTO of 0. These types of solutions will require fully redundant alternate processing sites, which will have much higher costs. However, a longer RTO would be able to make use of a less expensive recovery system.

   PTS: 1 REF: 62

9. What are some of the methods that can be used to collect data to support a business impact analysis (BIA)?

   ANS:
   - Online questionnaires
   - Facilitated data-gathering sessions
   - Process flows and interdependency studies
   - Risk assessment research

- IT application or system logs
- Financial reports and departmental budges
- BCP/DRP audit documentation
- Production schedules

PTS: 1 REF: 64

10. What expenses are normally associated with disaster recovery budgeting? What expenses might be incurred if a company is specifically worried about losses from cyber attacks such as denial-of-service events?

ANS:
The number one budgetary expense of disaster recovery (DR) is insurance. Insurance policies provide for the capabilities to rebuild and reestablish operations at the primary site. Should fire, flood, earthquake, or other natural disaster strike, the insurance carrier oversees the funding of replacement structures and services until the primary site is restored.

One problem with insurance is that much of the damage from electronic attacks is not covered in normal policies. Some forward-thinking insurance companies are starting to roll out data loss policies (hacker insurance). Natural disasters are familiar to insurance adjusters but losses from electronic attacks are not. Some companies are finding it difficult to estimate exactly how much they will need in order to cover expected losses.

PTS: 1 REF: 77-78