

Business Continuity Planning and Disaster Recovery Planning
[Exam importance- 12 marks; Cash marks; LBH]

➤ Types of Plans that need to be designed:

1. Emergency Plan: specifies actions to be undertaken when a disaster occurs:
 - 4 aspects of an emergency plan:
 - a. Who should be contacted?
 - b. What actions to be taken?
 - c. Evacuation procedures?
 - d. Return procedures?
2. Back-up Plan: specifies type, frequency, procedures, location of backups and ensuring that all critical resources are backed up.
3. Recovery Plan: sets out the procedures to restore full information system capabilities.
4. Test Plan:
 - ✓ Final component of DRP.
 - ✓ Identifies deficiencies in the emergency, backup and recovery plans.
 - ✓ For the above it must simulate a range of disasters and specify the criteria based on which the emergency, backup and recovery plans can be deemed satisfactory.

➤ Types of Back Ups: (draw diagram in exam)

1. Full Backup (captures all files on the disk):
 - Advantages:
 - a) Restores very fast
 - b) Easy maintain & restore
 - Disadvantages:
 - a) Back up is time consuming
 - b) Consumes more storage space
2. Incremental Backup (captures files that were created/ modified *since last backup, regardless of backup type*):
 - Advantages:
 - a) Much faster backups
 - b) Efficient use of storage space
 - Disadvantages:
 - a) Restores are slower than other backups
 - b) Restores are complicated as each incremental backup needs to be restored
3. Differential Backup (captures files that were created/ modified *since last full backup*):
 - Advantages:
 - a) Faster to backup compared to full backups
 - b) More efficient use of storage space
 - c) Faster restore than incremental backups
 - Disadvantages:
 - a) Backup is slower than incremental backup
 - b) Not as efficient use of storage space as incremental backup; as it includes files that are already included in the previous differential backups
 - c) Restore little more complicated than full backups, but easier compared to incremental backup

4. Mirror Backup (a mirror of the source being backed up; no compression of files; cant be protected with a password)
 - Advantages:
 - a) The backup is clean and does not contain old and obsolete files
 - Disadvantages:
 - a) There is a chance that files in the source get deleted accidentally or by sabotage or through virus, thereby also deleting the corresponding file in mirror backup

➤ Alternate Processing Facility Arrangements:

1. Cold Site
 - ✓ If org can tolerate some downtime
 - ✓ Here minimum facilities are made available at the alternative site
 2. Hot Site
 - ✓ If fast recovery is critical; no downtime permissible
 - ✓ All facilities are made available at the alternative site
 - ✓ Expensive to maintain
 3. Warm Site
 - ✓ When org requires only essential facilities at alternative site
 - ✓ Provide intermediate level of backup facilities; Cold site + little more
 4. Reciprocal Agreement
 - ✓ 2 or more organizations agree to provide backup facilities to each other in event of one facing a disaster.
 - ✓ Relative cheaper, but each participant must maintain sufficient capacity to operate another's critical system
- ❖ If 3rd party site is used for backup & recovery purpose, then the contract must cover issues such as:
1. How soon the site will be made available subsequent to a disaster
 2. Facilities & services the site provider agrees to make available
 3. No. of orgs. that will be allowed to use the site concurrently in the event of a disaster
 4. The priority to be given to concurrent users of the site in event of a common disaster
 5. Period during which the site can be used
 6. Conditions under which the site can be used
 7. What controls will be in place at the offsite facility?

➤ Disaster Recovery Procedural Plan: disaster recovery and planning document may include the following areas: (Components of DRP):

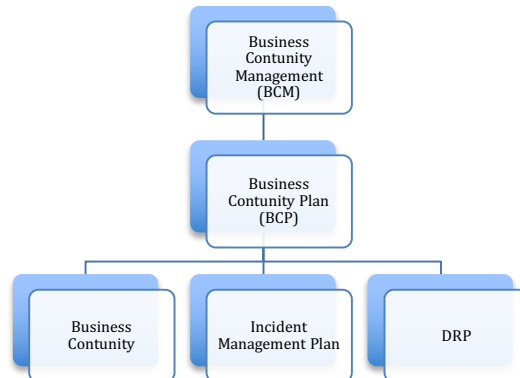
1. Conditions for activating the plans describing the process to be followed before activation.
2. Emergency procedures to be taken following the incident
3. Fallback procedures
4. Resumption procedures
5. Responsibilities of individuals describing who is responsible for executing the plan.
6. Emergency phone list of fire, police, suppliers, etc.
7. Medical procedures to be followed
8. Insurance papers and claim forms
9. Schedule for testing and maintaining the plan
10. Description of purpose and scope of the plan

➤ AUDIT of the Business Continuity Plan/ Disaster Recovery Plan:

- ✓ Objective of BCP Audit is to assess the ability of an entity to continue all critical operations during a contingency and recover from a disaster within the defined critical recovery time period.
- ✓ Auditor is expected to evaluate the processes of developing and maintaining documented, communicated and tested plans for continuity of business operations and IS processing in the event of disruption.
- ✓ Sample list of BCP Audit STEPS:

1. Obtain and review existing BCP/ DRP.
2. Obtain and review the existing business impact analysis.
3. Determine if BCP/ DRP plan Exists and was developed using sound methodology that includes the following elements:
 - a. Identification and prioritization of the activities, which are essential to continue functioning.
 - b. The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
 - c. Operations managers and key employees participated in the development of the plan.
 - d. The plan identifies the resources that will likely be needed for recovery and the location of their availability.
 - e. The plan is simple and easily understood so that it will be effective when it is needed.
 - f. Plan is realistic in its assumptions.
4. Determine if Backup procedures are sufficient to allow for recovery of critical data.
5. Interview managers & employees to determine their understanding of BCP/ DRP.
6. Building, utilities and transportation
 - a. Does the DR/BR plan have a provision for having a building engineer to inspect the building soon after a disaster so that damage can be identified and repaired to make the premises safe for the return, a.s.a.p.?
 - b. Does the DR/BR consider the need for alternative location, if needed?
 - c. Review any arrangements for use of back-up facilities
 - d. Are building safety features regularly inspected and tested?
7. Information Technology
 - a. Determine if plan reflects current IT environment.
 - b. “ “ “ includes prioritization of critical applications.
 - c. Does BCP/ DRP include arrangements for emergency telecommunications?
 - d. Is there a plan for alternate means of data transmission if the computer network is interrupted?
8. Administrative Procedures
 - a. Does DR/BR plan cover administrative & management aspects?
 - b. Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
 - c. Determine if DR/BR plan cover procedures for disaster declaration, general shutdown and migration of operations to backup facility.
 - d. To facilitate retrieval, are essential records separated from those that will not be needed immediately?
9. Have resources allocated for BCP/ DRP prevented from becoming outdated and ineffective.
10. Determine if the plan has been updated in last 12 months.

➤ Need for Business Continuity Management (BCM):



- BCP is expected to provide:
 1. Reasonable assurance to senior management to recover from any unexpected incident and continue to provide services with minimal impact.
 2. Anticipate various types of incident and outline action plan accordingly, to recover from such incident if it occurs, with minimum impact and ensuring continuous availability of all key services to client.
 3. BCP Manual: is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business function.
- Advantage of Business Continuity MANAGEMENT: Enterprise is:
 1. Able to proactively assess the threat scenario and potential risks;
 2. Has planned response to disruptions and minimize the impact on the enterprise; and
 3. Is able to demonstrate a response through regular testing and trainings.
- Methodology Developing a Business Continuity Plan: (divided into 8 phases):
 - The methodology emphasizes on the following:
 1. Providing mgt. with a comprehensive understanding of the total efforts required developing and maintaining an effective recovery plan.
 2. Obtaining commitment from appropriate management to support and participate in the effort.
 3. Defining recovery requirements from the perspective of business functions.
 4. Documenting the impact of an extended loss to operations and key business functions.
 5. Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery.
 6. Selecting business continuity teams that ensure the proper balance required for plan development
 7. Developing a business continuity plan that is understandable, easy to use and maintain; and
 8. Defining how business continuity considerations must be integrated into ongoing business planning and system development process in order that the plan remains viable over time.

