

1. Explain the maintenance tasks undertaken in development of BCP.

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise.
- Determine the maintenance regime to ensure the plan remains up to date.
- Determine the maintenance process to update the plan.
- Implement version control procedures to ensure that the plan is maintained up to date.
- Identify the BCP maintenance triggers to ensure that any – organisational
 - operational
 - structuralchanges are communicated to the personnel who are accountable.

2. Write a note on BCM Training Process.

An enterprise with BCM uses training as a tool to initiate a culture of BCM in all the stakeholders by:

- Developing a BCM program more efficiently.
- Providing confidence in its stakeholders in its ability to handle the business disruptions.
- Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels.
- Minimising the likelihood and impact of disruptions.

Development of a BCM culture is supported by:

- Leadership from senior personnel in the enterprise.
- Assignment of responsibilities.
- Awareness rising.
- Skill training.
- Exercising plans.

3. Explain the areas should be considered while reviewing the BCM Arrangements.

An audit or self assessment of the enterprise's BCM program should verify that:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprises BCM strategy.
- The enterprise's BCM policy, strategies, framework and plans are accurately reflects its objectives.
- The enterprises BCM competence and its BCM capability are effective.
- The enterprise's BCM solutions are effective, update and fit-for-purpose.
- The enterprise's BCM maintenance and exercising programs have been effectively implemented.
- The enterprise has an ongoing program for BCM training and awareness.
- BCM procedures have been effectively communicated to relevant staff.
- BCM strategies and plans incorporate improvements identified in the maintenance program.
- Change control processes are in place and operate effectively.

4. Explain the necessary competencies for personnel while developing the BCM.

- Actively listens to others, their ideas, views and opinions.
- Provides support in difficult or challenging circumstances.
- Responds constructively to difficult circumstances.
- Adopts leadership style appropriately to match the circumstances.
- Promotes a positive culture of health, safety and the environment.
- Recognises and acknowledges the contribution of colleagues.
- Encourage the taking of calculated risks.
- Encourage and actively responds to new ideas.
- Consults and involves team members to resolve problems.
- Demonstrates personal integrity.

5. **Explain briefly the types of plans with respect to Business Continuity and Disaster Recovery Plan.**

➤ **Emergency Plan:**

- It specifies the actions to be undertaken immediately when disaster occurs.
- Management must identify those situations that require the plan to be invoked.
Ex – major fire, major structural damage, terrorist attack etc.
- When the situations, that invoke the plan have been identified, four aspects of the emergency plan must be articulated they are:
 - ❖ The plan must show who is to be notified immediately when the disaster occurs.
 - ❖ The plan must show actions to be undertaken.
 - ❖ Any evacuation procedures required must be specified.
 - ❖ Return procedures must be defined.
- The actions to be initiated can vary depending on the nature of the disaster that occurs.

➤ **Backup Plan:** It specifies

- The type of backup to be kept.
- The frequency with which back up is to be undertaken.
- Procedures for making backup.
- Site where the resources can be assembled and operations re-started.
- Personnel who are responsible for gathering backup resources and re-starting operations.
- Priorities to be assigned to recovering the various systems and
- Time frame for recovery of each system.

➤ **Recovery Plan:**

- Recovery plans sets out the procedures to restore full information system capabilities.
- It should identify a recovery committee that will be responsible for working out that specifies of the recovery to be undertaken.
- The plan should specifies the responsibilities of the committee and provide guidelines on priorities to be followed.

➤ **Test Plan:**

- The final component of a disaster recovery plan is a test plan.
- The purpose of the test plan is to identify deficiencies in the emergency or back up or recovery plan.
- Periodically test plan must be invoked.
- To facilitate testing, a phased approach can be adopted.

6. **Explain briefly various types of Backups.**

➤ **Full Backup:**

- A complete backup of everything you want to backup is known as full backup.

Advantages:

- * Restores are fast and easy to manage.
- * Easy to maintain and restore different versions

Disadvantages:

- * Backup can take very long time.
- * Consumes more storage space.

➤ **Incremental Backup:**

- An incremental backup captures files that were created or changed since last backup regardless of backup type.

Advantages:

- * Much faster backups.
- * Efficient use of storage space.

Disadvantages:

- * Restores are slower than with full and differential backup.
- * Restores are little more complicated.

➤ **Differential Backups:**

- It falls in the middle between full and incremental backups.
- It stores files that have changed since the last full backup.

Advantages:

- * Much faster backup than full backup.
- * More efficient use of storage space.
- * Faster restore than incremental backup.

Disadvantages:

- * Backups are slower than the incremental backups.
- * Restores are slower than with full backups.
- * Restores are little more complicated than full backups.

➤ **Mirror Backup:**

- They are the mirror of the source being backed up.
- With this when a file in the source is deleted, that file is eventually also deleted in the mirror backup.

Advantages:

- * The backup is clean and does not contain old and obsolete files.

Disadvantages:

- * There is a chance that files in the source deleted accidentally by sabotage or through virus.

7. What are the issues to be considered by the Security Administrator, if the third party site is used for backup and recovery purpose?

- How soon the site will be made available subsequent to a disaster.
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster.
- The priority to be given to concurrent users of the site in the event of common disaster.
- The period during which the site can be used.
- The facilities and services the site provider agrees to make available.
- The conditions under which the site can be used.
- What controls will be in place and working at the offsite facility.

8. Explain briefly the terms with respect to alternate processing facility arrangements.

➤ **Cold site:**

- If an organization can tolerate some downtime, cold site backup might be appropriate.
- A cold site has all the facilities needed to install – a system –raised floors
 - air conditioning
 - power
 - communication line etc.
- An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.

➤ **Hot Site:**

- If fast recovery is critical, an organization might need hot site backup.
- All hardware and operation facilities will be available at the hot site.
- They are usually shared with other organisation.
- A hot site is expensive to maintain but worth.

➤ **Warm Site:**

- A warm site provides an intermediate level of backup.
- It has all cold site facilities in addition to the hardware that might be difficult to obtain or install.

➤ **Reciprocal Arrangements:**

- Two or more organizations might agree to provide facilities to each other in the event of disaster.
- This option is relatively cheap.

9. Explain the areas which should be included in the Disaster Recovery Planning Document.

- The conditions for activating the plan.
- Emergency procedures.
- Fall back procedures.
- Resumption Procedures.
- A maintenance schedule.
- Awareness and education activities.
- The responsibilities of individuals.
- Contingency plan testing and recovery procedures.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- List of vendors doing business with the organisation.
- Emergency phone list for fire, police etc.
- Check list for inventory taking and updating the contingency plan on a regular basis.
- Medical procedures to be followed in case of injury.
- Backup location, contractual agreements, correspondence.
- Insurance papers and claim forms.
- Alternate manual procedures to be followed.
- Names of trained employees for emergency situations.
- Details of airlines, hotels, and transport arrangements.
- List of phone numbers of employees in the event of emergency.

10. Briefly explain the audit of BCP/DRP.

- In a BCP Audit, the 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 disruptions.
- The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during contingency and recover from a disaster within the defined critical recover time period.
- BCP auditor is expected to identify residual risks and provide recommendations to mitigate them.
- The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.
- Sample list of BCP audit are :
 - Determine if a DRP/BRP exists and was developed using a sound methodology.
 - Determine if information backup procedures are sufficient to allow for recovery of critical data.
 - Determine if a test plan exists and to what extent DRP/BRP has been tested.
 - Determine if resources have been made available to maintain the DRP/BRP.
 - Obtain and overview the existing DRP/BRP.
 - Obtain and review the existing BIA.
 - Determine if copies of the plan are safeguarded by off-site storage.
 - Determine if the plans has been updated within past 12 months.
 - Determine all the locations where the DRP/BRP is stored.
 - Determine if the plan is dated each time that it is revised.
 - Gain an understanding of the methodology used to develop the existing DRP/BRP.
 - Gain an understanding of the methodology used to develop the existing BIA.