

Summary of chapter 4- Business Continuity Plan

Q.1 What is BCP (Buss. Continuity Planning). (Ye BCM process ka output hota hai)

- Before disaster
 - Guide for action to be taken before during and after disaster
 - Either prevention or recovery in minimum time and losses
 - recovery of key resources
 - least impact on business continuity
 - reduce risk from unexpected disruption
 - provides reasonable assurance to senior mgt for business continuity
 - defines roles and responsibility
-
- So, Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.
 - The logistical plan is called a business continuity plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response.
 - The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience

So we can say... BCP is expected to provide :

- Provides reasonable assurance to senior mgt
- Anticipate threats
- Responsibility

Q.2 Business continuity covers the following areas ?

Business continuity covers the following **3** areas:

Business Resumption Planning: This is the operation's piece of business continuity planning.

Disaster Recovery Planning: This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and

ensure continuity of critical business functions of the organization in the event of disaster.

Crisis Management: This is the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

Q.3 **Objectives** of (BCP)business continuity planning ?

The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to reestablish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. **The key objectives of the contingency plan should be to:**

B C P ko SUCCESSFUL bnane aur COMPLEXITY REDUCE karne k liye Dilwale (i.e DURATION) Dulhaniya (jo ki hmesa DAMAGE hi krti hai) le jaenge CRITICAL LINE se.

- Critical **business** operations continuity
- Facilitate effective **co-ordination** of recovery tasks;
- Provide for the safety and well-being of **people** on the premises at the time of disaster;
- Establish **management succession** and emergency powers
- **Reduce the complexity** of the recovery effort;
- **Minimise the duration** of a serious disruption to operations and resources (both information processing and other resources);
- **Minimise immediate damage** and losses;
- **Identify critical lines** of business and supporting functions.

Q.4 **GOALS** of (BCP) business continuity planning ?

MT : WEAK CCD

Therefore, the goals of the Business Continuity Plan should be to:

- Id of weakness
- Co ordination
- Complexity
- Duration

Q.5 What is the methodology of develop a BCP (business continuity Plan)?

MT : **To PREVENT IMPACT on TEAM and UNDERSTAND OF TOTAL EFFORT of love,**
Hmesa 3 chijo ko RECOVER krne ki REQUIREMENT hoti hai :

1. Commitment
2. Understandable
3. Time

The methodology for developing a BCP can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organization. **The methodology emphasizes on the following:**

- Focusing appropriately on disaster **prevention** and impact minimization, as well as orderly recovery;
- Documenting the **impact** of an extended loss to operations and key business functions;
- Selecting business continuity **teams** that ensure the proper balance required for plan development;
- Providing management with a comprehensive **understanding of the total efforts** required to develop and maintain an effective recovery plan;
- Defining **recovery requirements** from the perspective of business functions;
- Obtaining **commitment** from appropriate management to support and participate in the effort;
- Developing a business continuity plan that is **understandable**, easy to use and maintain; and
- Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over **time**.

Q.6 Business continuity plan should be sub- divided into eight differentness ?

OR

Describe the phases of developing a Business Continuity Plan ?

- (i) Pre-Planning Activities (Business Continuity Plan Initiation),
- (ii) Vulnerability Assessment and General Definition of Requirements,
- (iii) Business Impact Analysis,
- (iv) Detailed Definition of Requirements,
- (v) Plan Development,
- (vi) Testing Program,
- (vii) Maintenance Program, and

(viii) Initial Plan Testing and Plan Implementation.

Phase 1 – Pre-Planning Activities (Project Initiation): This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. a Steering Committee should be established make all decisions related to the recovery planning effort.

Phase 2 – Vulnerability Assessment and General Definition of Requirements:

It include security assessment of System & communication environment physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security insurance; security planning and administration; application controls; and personal computers.

Phase 3 – Business Impact Assessment (BIA): A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:

- identify critical systems, processes and functions;
- Assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
- Assess the “pain threshold,” that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption.

Phase 4 – Detailed Definition of Requirements:

- During this phase, a profile of recovery requirements is developed.
- This profile is to be used as a basis for analyzing alternative recovery strategies.
- The profile is developed by identifying resources required to support critical functions identified in Phase 3.
- This profile should include hardware, software, documentation, facilities etc.
- Recovery Strategies will be based on short term intermediate term and long term outages.

Phase 5 – Plan Development:

- During this phase, recovery plans components are Defined (i.e determine available options) and plans are documented.
- This phase also define of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

Phase 6 – Testing/Exercising Program:

- The plan Testing/Exercising Program is developed during this phase.
- Testing/exercising goals are established and alternative testing strategies are evaluated.
- Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

Phase 7 – Maintenance Program:

- Maintenance of the plans is critical to the success of an actual recovery.
- Plan must reflect changes to the environments that are supported by the plans.
- It is critical that existing change management processes are revised to take recovery plan maintenance into account.
- In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.

Phase 8 – Initial Plan Testing and Implementation: Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following :

- Defining the test purpose/approach;
- Identifying test teams;
- Structuring the test;
- Conducting the test;
- Analyzing test results; and
- Modifying the plans as appropriate.

BCM (Buss Continuity Mgt) = BCP + Execution/Implementation of BCP

We can say that “ The primary Output of BCM process is *BCP i.e Bus.Continuity Plan*

Q.6 What is Business continuity Management (BCM). Explain its Scope advantage also ?

To meet the enterprise business objectives and ensure continuity of services and operations, an enterprise shall adapt and follow well-defined and time-tested plans and procedures, build redundancy in teams and infrastructure, manage backup arrangement for business systems and services.

- Where **Business continuity means** maintaining the uninterrupted availability of all key business resources required to support essential business activities.

Let us understand some **key terms related to BCM** :-

- Business Contingency
- BCP Process
- Business Continuity Planning (BCP)

❖ **Advantages of BCM:**

- Top mgt. need to define the Scope of the BCM program by identifying the key products & services that support the enterprise's objectives, obligations, and statutory duties in line with the threat scenario and Bus. Impact Analysis (BIA).
- Also in case of an outsourced service or activity, the risk accountability remains with the enterprise.

❖ **Advantages of BCM are that the enterprise:**

- is able to proactively assess the threat scenario and potential risks;
 - has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
 - is able to demonstrate a response through a process of regular testing and trainings.
-

Q. 8 What is BCM Policy. What are the Objective of BCM Policy ?

BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability.

While developing the BCM policy, the enterprise should consider defining the scope, BCM principles, guidelines and minimum standards for the enterprise.

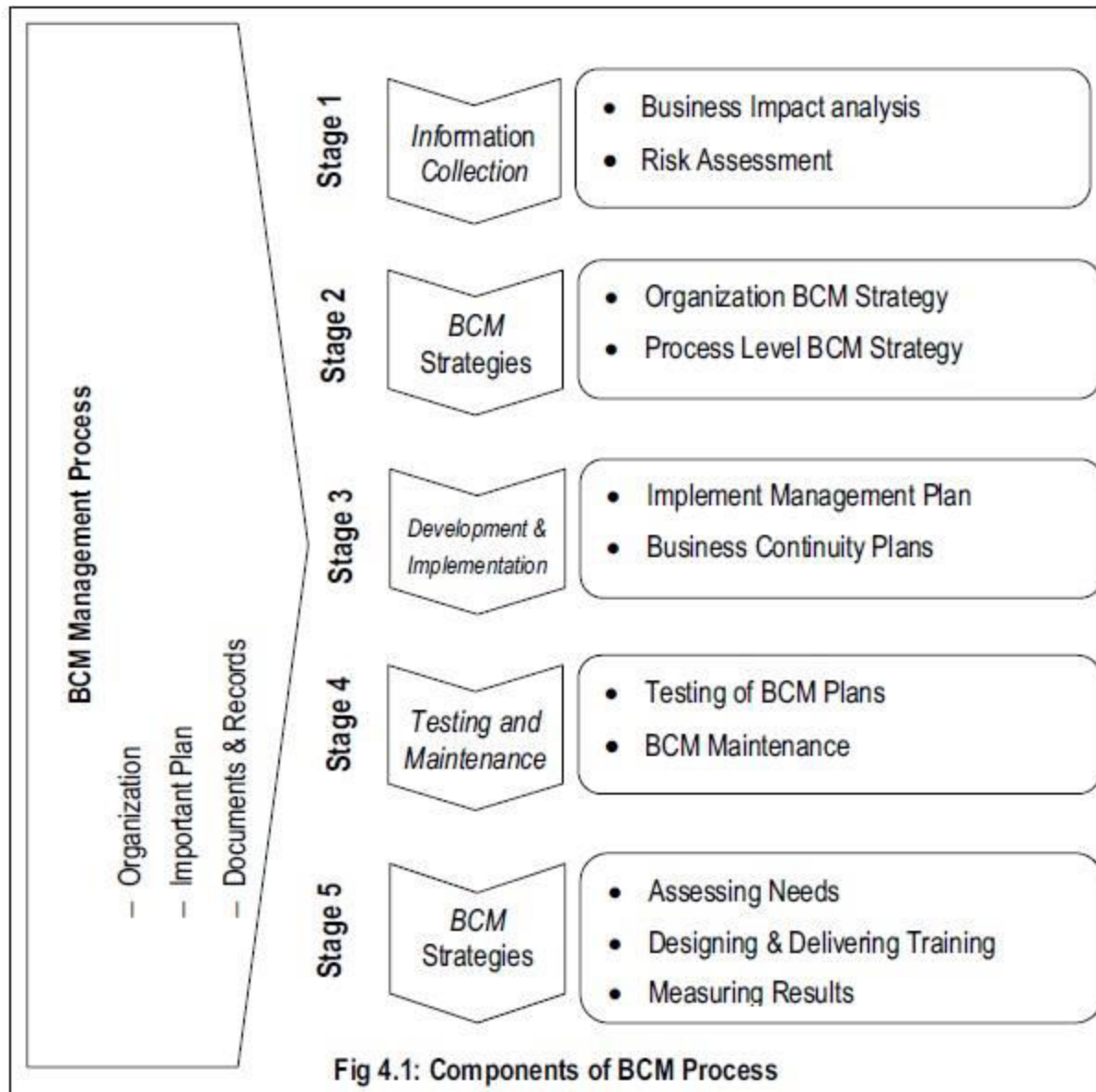
The objective of this policy is to provide a structure through which:

MT : To TEST the INCEDENT , CRITICAL RESOURCES are RESPONSIBLE

- **Critical services** and activities undertaken by the enterprise operation for the customer will be identified.
 - Plans will be developed to **ensure continuity of key service** delivery after a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
 - **Invocation of incident management** and business continuity plans can be managed.
 - **Ongoing testing, revision and updation** of Incident Management Plans & Business Continuity Plans.
 - Planning and management **responsibility are assigned** to a member of the senior management team.
 - The loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction is minimized.
-

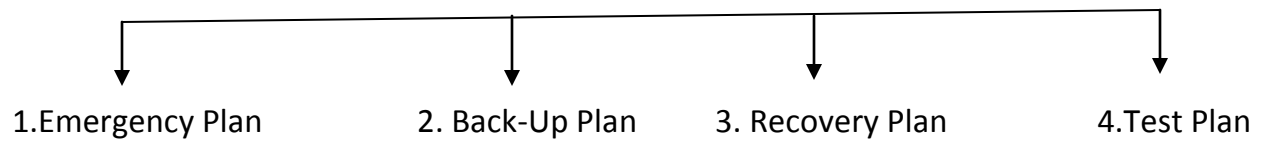
COMPONENT OF BCM PROCESS (5 Process)

- **BCM – Information Collection Process**
- **BCM – Strategy Process**
- **BCM – Development and Implementation Process**
- **BCM – Testing and Maintenance Process**
- **BCM – Training Process**



Pending : Above detail

Q.9 What are the difference **TYPES OF PLANS ?**



1) **Emergency Plan :**

- Emergency plan specifies the actions to be undertaken immediately when a disaster occurs.
- Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack.
- The actions to be initiated can vary depending on the nature of the disaster that occurs.

When the situations that evoke the plan have been identified, 4 aspects of the emergency plan must be articulated : **MT: emergency me NEAR wale kam aate hai**

1. **Who is to be Notified immediately when the disaster occurs**(E.g. Management, police, fire department, media and so on)
2. **Evacuation procedures** (i.e removal of individuals from a dangerous place)
- 3.
4. **Actions to be undertaken**(Such as shutdown of equipment, removal of files, and termination of power.
5. **Return procedures** (e.g. conditions that must be met before the site is considered safe)

Emergency plan also identified personnel with key responsibility and protocols to be followed must be specified clearly.

2) **Back-up Plan**

The backup plan specifies the :

- Type of backup to be kept,
- Frequency with which backup is to be undertaken,
- Procedures for making backup,
- Location of backup resources,
- Site where these resources can be assembled and operations restarted,

- Personnel who are responsible for gathering backup resources and restarting operations.
- Priorities to recovering various resources.
- Time frame for recovery of each system.

❖ ***Features for Effective backup Plan :***

1. The backup plan needs **continuous updating** as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly.
2. It is prudent to have **more than one person knowledgeable in a backup task** in case someone is injured when a disaster occurs.
3. Lists of **hardware and software must be updated** to reflect acquisitions and disposals.

3) **Recovery Plan** : It set out procedures to recover Hardware, Software and other IT facility.

It Should contain following key elements :

- Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken.
- Plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed.
- Plan also indicate which applications are to be recovered first
- Members of a recovery committee must understand their responsibilities
- Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur.
- If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

Test Plan

This plan identify deficiencies in the

- ✓ emergency, backup, or recovery plans and/or
- ✓ In the preparedness of an organization/personnel in the event of a disaster.

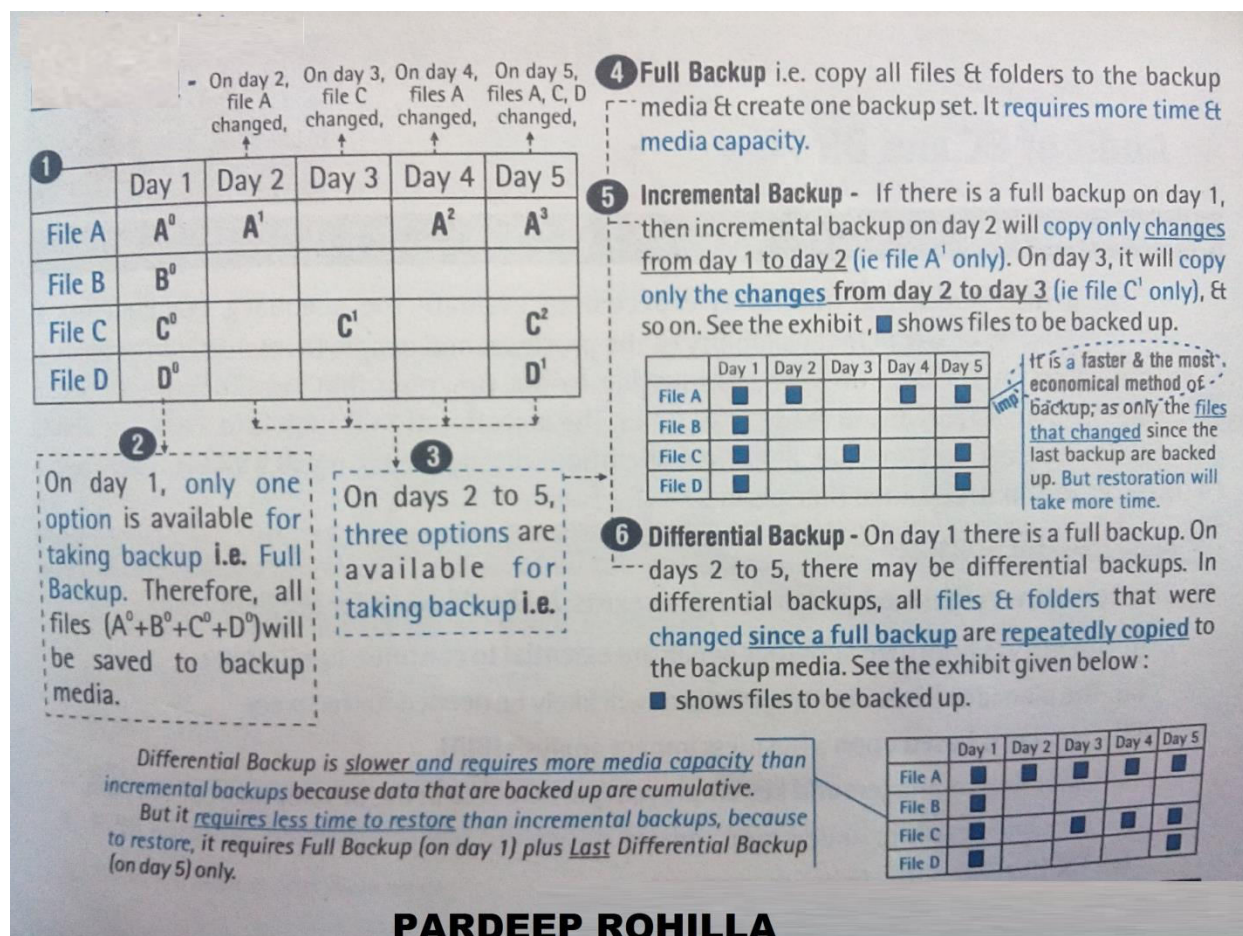
Periodically, test plans must be invoked (**that means a disasters to be simulated**) to ensure the quality working of emergency, backup, and recovery plans.

Unfortunately, top managers are often unwilling to carry out a test because:

- daily operations are disrupted.
- They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a Phased Approach can be adopted :

First	Next	Finally
Desk checking and inspection and walkthroughs Note down all critical situations that may arise due to disaster & ensure that the plan cover all aspects.	Full operational test with proper/prior notice of test Create some conditions of disaster and test all plans. Anyone, who will be affected by the test. (e.g. Personnel & customers) also might be given prior notice of the test so they are prepared.	• Finally, disasters could be simulated without warning at any time. • These are the acid tests of the organization's ability to recover from a real disaster/catastrophe.



Q.9 What are you mean by Total System backup ? Explain the Types of Back-ups ?

When the back-ups are taken of the system and data together, they are called total system's back-up.

Various types of back-ups are given as follows:

1. Full Backup
2. Differential Backup
3. Incremental Backup
4. Mirror Backup

Q.10 Explain the Full backup ? Also its advantages and disadvantages ?

Full Backup: A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set.

- At each backup run, all files designated in the backup job will be backed up again.
- This includes files and folders that have not changed.
- It is commonly used as an initial or first backup followed with subsequent incremental or differential backups.
- After several incremental or differential backups, it is common to start over with a fresh full backup again.
- Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space.
- The Windows operating system lets us to copy a full backup on several DVD disks. Any good backup plan has at least one full backup of a server.

For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not.

❖ Advantages of Full backup :

- Restores are fast and easy to manage as the entire list of files and folders are in one backup set.
- Easy to maintain and restore different versions.

❖ Disadvantages of Full backup :

- Backups **can take very long** as each file is backed up again every time the full backup is run.
- **Consumes the most storage space** compared to incremental and differential backups.
- The exact **same files are stored repeatedly** resulting in inefficient use of storage.

Q.11 What is Incremental Backup ? Also its advantages and disadvantages ?

- An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type.
- The last backup can be a full backup or simply the last incremental backup.
- With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Advantages

1. Much faster backups.
2. Efficient use of storage space as files are not duplicated.
3. Much less storage space used compared to running full backups and even differential backups.

Disadvantages

1. Restores are slower than with a full backup and differential backups.
2. Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

Q.12 What is Differential Backup ? Also its advantages and disadvantages ?

- Differential Backup: Differential backups fall in the middle between full backups and incremental backup.
- A Differential Backup stores files that have changed since the last full backup.
- With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.
- Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up.
- Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Advantages :

- Much faster backups then full backups.
- More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run.
- Faster restores than incremental backups.

Disadvantages:

- Backups are slower then incremental backups.
- Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.
- Restores are slower than with full backups.
- Restores are a little more complicated than full backups.

Q.13 Explain Mirror back-up ? Also its advantages and disadvantages ?

- Mirror backups are, as name suggests, a mirror of the source being backed up.
- With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup.
- Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.
- Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep utilities do provide support for mirror backups.

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 a virus may also be deleted from the backup mirror.
-

Q.14 Explain the alternate processing facility arrangements in business continuity and disaster recovery planning.

1. Cold Site:

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

2. Hot Site:

- If fast recovery is critical, an organisation might need hot site backup.
- All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there.
- A hot site is expensive to maintain.
- They are usually shared with other organisations that have hot-site needs.

3. 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.
- For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

4. Reciprocal Agreement:

- Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster.
- This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

Q.15 Explain third-party site backup ? or

A company has decided to outsource its recovery process to a third party site. What are the issues that should be considered by the security administrators while drafting the contract?

If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as :

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

Q.16 Describe contents of a Disaster Recovery and Planning Document. ?

Taj me **Emergency** bomb blast hua, sara business dusri **Location** pe move kiya. Kaunsi **Inventory** kahape rakhi hain iska **Documentation** kiya. Blast honese pahale hi sabko **Aware aur Train** kiya tha. Is plan ko already **Test** kiya gaya tha. Sabhiko **Plan** ke **Purpose** aur **Responsibility** pata thi. disaster ho gaya ab **Resumption** karna tha isiliye **Phone list** me dekhkar **Police, Medical, Insurance, Airlines** ko call kiya. **Hardware** aur **Software** jo jalgaye the wo **Vendors** se firse kharide. **Back up** honese jyada data ka loss nahi hua tha. **Recovery** pura hone tak **Manual system** se **Maintain** kiya.

1. The conditions for activating the plans, which describe the process to be followed before each **plan**, is activated.
2. **Emergency procedures**, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life.
3. **Location** of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
4. Checklist for **inventory** taking and updating the contingency plan on a regular basis.

5. Contingency plan **documentation** distribution list.
 6. **Awareness** and education activities, which are designed to create an understanding of the disaster recovery process.
 7. Contingency plan **test** and recovery procedure.
 8. Names of employees **trained** for emergency situation, first aid and life saving techniques.
 9. Detailed description of the **purpose and scope of the plan**.
 10. **Responsibilities** of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
 11. **Resumption** procedures, which describe the actions to be taken to return to normal business operations.
 12. **List of phone** numbers of employees in the event of an emergency.
 13. Emergency phone list for **fire, police, hardware, software, suppliers, customers, back-up location**, etc.
 14. **Medical** procedure to be followed in case of injury.
 15. **Insurance** papers and claim forms
 16. Details of **airlines**, hotels, supplies and transport arrangements.
 17. Primary computer center **hardware, software**, peripheral equipment and software configuration.
 18. **Vendors** list who doing business with the organization, their contact numbers and address for emergency purposes.
 19. **Back-up** location contractual agreement, correspondences.
 20. **Recovery procedures**, which describe the actions to be taken to move essential business activities.
 21. Alternate **manual procedures** to be followed during the period of disruption such as manual preparation of invoices.
 22. A **maintenance schedule**, which specifies the process for **maintaining** the plan.
-

Q. 17 As an IS auditor, what are the key areas you would verify during review of BCM arrangements of an enterprise. OR

While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified.

An audit or self-assessment of the enterprise's BCM (Business Continuity Management) program should verify that:

1. All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
2. The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements;
3. The enterprise' BCM competence and its BCM capability are effective and fit-for purpose and will permit management, command, control and coordination of an incident;
4. The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
5. The enterprise's BCM maintenance and exercising programs have been effectively implemented;
6. BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
7. The enterprise has an ongoing program for BCM training and awareness;