CHAPTER 4

Business Continuity Planning and Disaster Recovery Planning

1. Need of Business Continuity Management(BCM)

- To meet the enterprise business objectives and
- To 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 a quick and efficient transition to the backup arrangement for business systems and services.

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:** A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.
- **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.
- **Business Continuity Planning (BCP)**: It refers to the ability of enterprises to SurviveRecover& Restartits normal business operationsfrom adisaster with least impact. The purpose of BCP is to ensurethat vital & critical business operations are recovered and operationalized within an acceptable timeframe. The purpose is to ensure continuity of business and not necessarily the continuityof all systems, computers or networks.

2. BCP MANUAL:

- An incident or disaster can strike at anytime. Therefore organizations should have a comprehensive BCP Manual, whichensures process readiness, data and system availability to ensure business continuity.
- A BCP manual is a documented descriptionof **A**ctions to be taken, **R**esources to be used and **P**rocedures to be followed before, during and after an event that severely disrupts all or part of the business operations.
- The BCP is expected toprovide:
  - Reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.
  - Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients'.
- The BCP Manual is expected to specify the responsibilities of the BCM team, to ensure the continuity of enterprise'scriticalbusiness functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioningteams between the functional area(s) affected and other departments providing supportservices.

3. SCOPE OF BUSINESSCONTINUITY:

Top management of the enterprise needs to define the scope of the BCM programby identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis.

In caseof an outsourced service or activity, the risk accountability remains with the enterprise and necessary controls and process should be in place to manage the risk from an outsourced service.

Advantages of Business Continuity

The 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.

4. BCM POLICY:

- The main objective of BCP is tominimize/eliminate the loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction.
- This policy is a high level document, which acts as aguide to make a systematic approach for disaster recovery, to bring about awareness among the personsabout the business continuity aspects and its importance.
- 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:
  - **Critical services and activities** undertaken by the enterprise operation for the customer will beidentified.
  - **Plans will be developed**to ensure continuity of key service delivery following 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.
  - **Incident Management Plans &Business Continuity Plans** are subject to ongoing testing, revision and updationasrequired.
  - **Planning and management responsibility** are assigned to a member of the relevant senior managementteam.

5. BUSINESS CONTINUITY PLANNING (BCP):

- BCP refers to the ability of enterprises to Survive Recover & Restart its normal business operations from a disaster with least impact.
- The purpose of BCP is
  - To ensurethat vital & critical business operations are recovered and operationalized within an acceptable timeframe.
  - To ensure continuity of business and not necessarily the continuityof all systems, computers or networks.
- BCP is 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.
- BCP is a **guiding document** that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations including the quantification of the resources needed to support the operational commitments.
- Business continuity covers the following areas:
  - **Business Resumption Planning:** To resume business operation even at the time of disaster
  - **Disaster Recovery Planning:** Advance planning and preparations which are 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.
- The Business Continuity Life Cycle is broken down into four broad and sequential sections:
  - Riskassessment,
  - Determination of recovery alternatives,
  - Recovery plan implementation,and
  - Recovery planvalidation.

6. OBJECTIVES OF BCP:

Primary Objective: **Survive Recover Re-start.**

Secondary Objective:

- **Identify** critical lines of business and supporting functions;
- **Resume**/Continue critical businessoperations immediately;
- **Minimize** the duration of disruption to operations and resources.
- **Minimize** losses& damages
- **Provide** the safety to people on the premises at the time of disaster;
- **Reduce** the complexity of the recovery effort;
- **Ensure** effective co-ordination of recovery tasks
- **Establish** management succession and emergency powers and

7. GOALS OF THE BCP:

- **Identify** weaknesses and
- **Implement**a disaster prevention program;
- **Minimize** the duration of a serious disruption to business operations;
- **Reduce** the complexity of the recovery effort
- **Ensure** effective co-ordination of recovery tasks; and

8. METHODOLOGY OF DEVELOPING A BCP:

The methodology for developing a BCP can be sub-divided into eight different phases.

- **Providing** management with a complete &comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- **Obtaining** commitment from management to support and participate in the effort;
- **Defining** recovery requirements from the perspective of business functions;
- **Documenting** possiblelosses, recovery tasks & procedures
- **Developing**a business continuity plan that is understandable, easy to implement, use and maintain
- **Integrate** BCP with other business planning process.
- **Selecting** proper business continuity teams to ensure the proper balance required for plan development
- **Focusing on** – Prevention of disaster/ minimizing the impact of disaster/ Timely recovery of disaster

9. THE 8 PHASES OF DEVELOPING A BCP:

Phase 1 - Pre-Planning Activities (Business Continuity PlanInitiation)

Phase 2 - Vulnerability Assessment and General Definition of Requirements

Phase 3 - Business ImpactAnalysis

Phase 4 - Detailed Definition of Requirements

Phase 5 - PlanDevelopment

Phase 6 - TestingProgram

Phase 7 - MaintenanceProgram

Phase 8 - Initial Plan Testing and Plan

Phase 1 – Pre-Planning Activities (Project Initiation):

- Understandthe existing and projected computing environment of the organization.
- Establish a steering committee - The committee should have the overall responsibility for providing direction and guidance to the Project Team
- Employ BC Manager who will work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the BIA.
- Develop a policy to support the recovery programs
- Provide Training &awareness to educate management and senior individuals who will be required to participate in the project.

Phase 2 – Vulnerability Assessment and General Definition ofRequirements:

Vulnerability Assessment is done to know the weakness in the existing system. This phase will include the following key tasks:

- A thorough Security Assessment of the computing andcommunications environment.
- The above Security Assessment will enable the project team to improve any existing emergency plans and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessmentto the Steering Committee so that corrective actions can be initiated in a timelymanner.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current followingimplementation.
- Develop a PlanFramework.
- Assemble Project Team and
- Conductawareness sessions.

Phase 3 –Business Impact Assessment (BIA):

- A BIA is an analysis which is conducted to determine various disasters which may cause big loss to business & potential impacts of those various other disasters.
- Tasks to be undertaken in BIA:
  - Identify overall threats/disasters such as fire flood etc
  - Identify critical business process
  - Identify possible threats/disaster events
  - Determine maximum allowable downtime of these process
  - Identify the type & quantity of the resources required for recovery
  - Determine the impact to organization in the event of disaster.
- 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. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Phase 4 – Detailed Definition of Requirements:

- During this phase, a profile of recovery requirementsisdeveloped.Thisprofileistobeusedasabasisforanalyzingalternativerecovery strategies.
- The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include **hardware, software** (vendor supplied, in - house developed, etc.), **documentation, outside support**, **facilities** and **personnel** for each business unit.
- Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

Phase 5 – Plan Development:

- During this phase, recovery plans are defined, developed and are documented.
- This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities.

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. The plans 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.

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 testpurpose/approach;
- Identifying testteams;
- Structuring thetest;
- Conducting thetest;
- Analyzing test results;and
- Modifying the plans as appropriate.

10. Components of BCMProcess

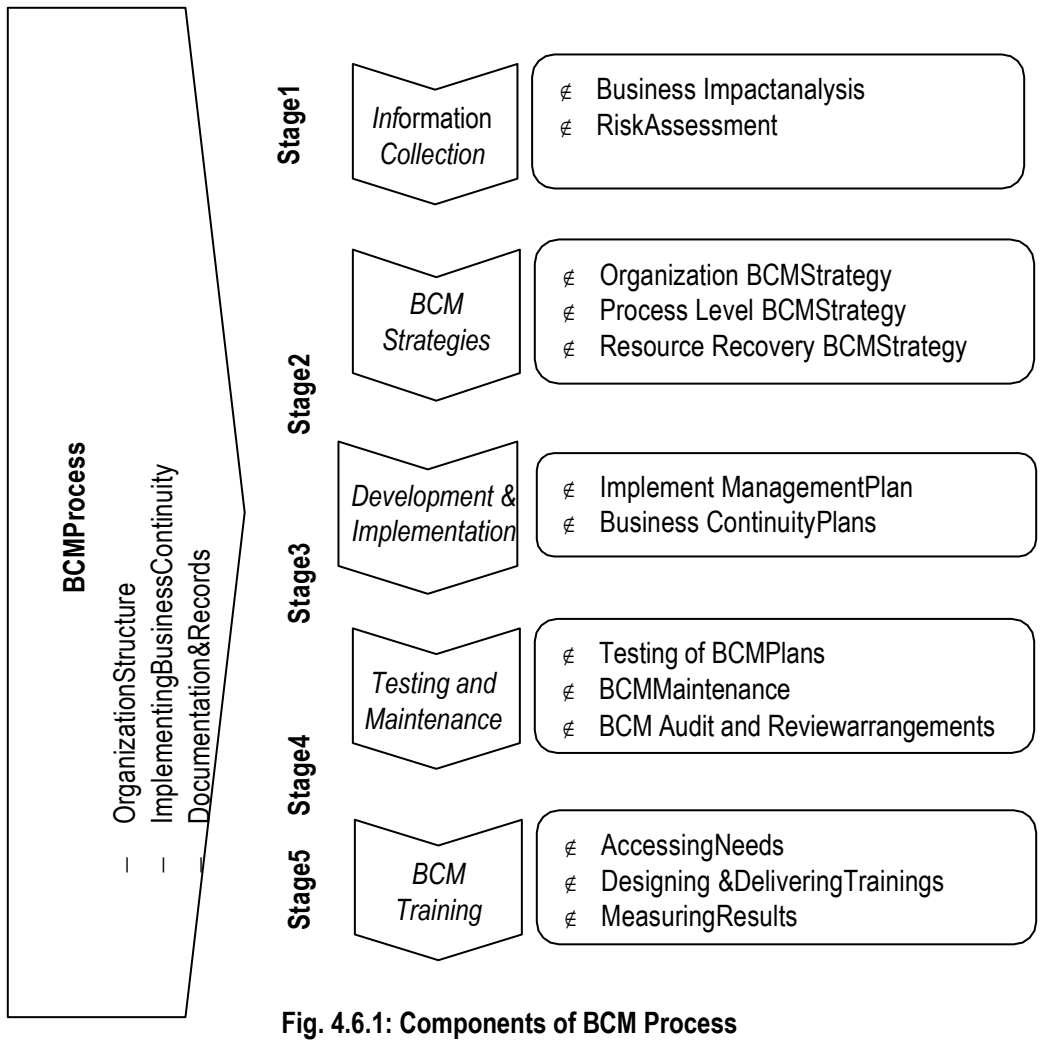

Fig. 4.6.1: Components of BCM Process

11. Business Continuity ManagementProcess

A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management. The BCM Processes are mapped as follows:

A. OrganizationStructure

The organization should nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance. It should clearly define the persons responsible for business continuity within the enterprise and responsibility.

B. Implementing Business Continuity in the Enterprise and Maintenance

In implementation, the major activities that should be carried out include:

- Defining the scope &context;
- Defining roles andresponsibilities;
- Engaging and involving allstakeholders;
- Testing of program on regularbasis;
- Maintaining the currency & appropriateness of business continuityprogram;
- Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and business impact analysis(BIAs);
- Managing costs and benefits associated;and
- Convert policies and strategies into action.

C. BCM Documentation and Records

All documents that form the BCM are subject to the document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:

- BCP- business continuitypolicy;
- BCMS- business continuity managementsystem;
- BC strategies
- BIA- business impact analysisreport;
- RA- risk assessment report;
- IMP & BCP - overall and specific incident managementplans & BCP
- LARR- Local Authority RiskRegister
- Incident log
- Training program
- The aims and objectives of eachfunction;
- The activities undertaken by eachfunction;
- Change control, preventative action, corrective action, document control and record control processes;
- Exercise schedule andresults;

12. BCM Information Collection Process

In order to design an effective BCM, it is pertinent to understand the enterprise from all perspectives of interdependencies of its activities, external enterprises and including:

- enterprise's objectives, stakeholder obligations, statutory duties and the environment in which the enterpriseoperates;
- activities, assets and resources, including those outside the enterprise, that support the delivery of these products and services;
- impact and consequences over time of the failure of these activities, assets andresources;and
- Perceived threats that could disrupt the enterprise's key products and services and the critical activities, assets and resources that support them.

The pre-planning phase of Developing the BCP also involves collection of information. It enablesus to refine the scope of BCP and the associated work program; develop schedules;and identify and address issues that could have an impact on the delivery and the success of the plan.

The process used for the development of both Business Impact Analysis and the Risk Assessment is detailed below. The outputs from these processes are reviewed by top management and signed off as being anaccurate representation of the operation at the time of their completion. Both the BIA and Risk Assessment will be reviewed as part of the annual BCM management review or following a change to the operation, its processes or associate risks.

A. Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is essentially a means systematically assessing the potential impacts resulting from various events or incidents. A BIA is an analysis which is conducted to determine various disasters which may cause big loss to business & potential impacts of those various other disasters. The process of BIA determines anddocumentstheimpactofadisruptionoftheactivitiesthatsupportitskeyproductsand services.

It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the length of time business units that can survive without access to the system, services and facilities.

The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management .This report identifies critical service functions and the time frame in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

B. Classification of Critical Activities

BCP leader and BCP team leaders in consultation with respective function owner shall carryout BIA for infrastructure and business transactions. BIA will result in categorization (like Vital, Desirable and Essential) of infrastructure and business function following by disaster scenarios (Catastrophic, major, minor trivial) for various disaster causes (fire, flood, system failure etc.), which is given as follows:

- **Business Categorization (Vital/Essential/Desirable):** The parameters considered in deciding whether a function/service is Vital/Essential/Desirable are:
  a. Loss ofrevenue;
  b. Loss ofreputation;
  c. Decrease in customer satisfaction;and
  d. Loss of productivity (man-hours).

- **Disaster Scenarios (Major/Minor/Trivial/Catastrophic):** The scenario of disaster shall be decided with the matrix given below:

The X-axis represents the Business impact of the infrastructure and business transaction as desirable (value=1), essential (value=2) or vital (value=3). The Y-axis represents the likelihood of occurrence of the disaster on a three point scale (1 -3).

3 (minor)	6 (Major)	9 (Catastrophic)
2 (Trivial)	4 (Major)	6 (Major)
1 (Trivial)	2 (Trivial)	3 (Minor)

Fig :Business Impact Matrix (1)

The Business Impact Analysis matrix is also used to assess Risk and is thusalso referred as Risk Assessment Matrix. The interpretation of the above Fig can be drawn like this.

In a risk assessment matrix, risks are placed on the matrix based on two criteria:

1. ***Likelihood:*** *the probability of a risk or the occurrence of the disaster – On Y Axis*
2. ***Consequences:*** *the severity of the impact or the extent of damage caused by the risk - On XAxis*

Likelihood of Occurrence

Based on the likelihood of the occurrence of arisk, the risks can be classified under one of the following categories:

1. ***Definite (scaled 3):*** *A risk that is almost certain to show-up during project execution. If you're looking at percentages a risk that is more than 80% likely to cause problems will fall under this category.*
2. ***Likely (scaled 2):*** *Risks that have 60-80% chances of occurrence can be grouped as likely.*
3. ***Unlikely (scaled 1):*** *Rare and exceptional risks which have a less than 10% chance ofoccurrence.*

Consequences

The consequences of a risk can again be ranked and classified into one of the following categories, based on how severe the damage can be.

1. ***Trivial/Insignificant (scaled 1):*** *Risks that will cause a near negligible amount of damage to the overall progress of the project.*
2. ***Minor (scaled 2):*** *If a risk will result in some damage, but the extent of damage is not toosignificant.*
3. ***Major (scaled 3):*** *Risks with significantly large consequences which can lead to a great amount of loss are classified as critical.*
4. ***Catastrophic (scaled 4):*** *These are the risks which can make the project completely unproductive and unfruitful, and must be a top priority during risk management.*

3 x 1 = 3	*3 x 2 = 6*	*3 x 3 = 9*	*3 x 4 = 12*
2 x 1 = 2	*2 x 2 = 4*	*2 x 3 = 6*	*2 x 4 = 8*
1 x 1 = 1	*1 x 2 = 2*	*1 x 3 =3*	*1 x 4 = 4*

Like-wise the grid can be extended depending upon the criteria one chooses. Depending upon the grid value, the risk can be assessed.

- ***Like values 8 to 12 can be categorized into Catastrophic.***
- ***Values 4 to 6 can be denoted as Major.***
- ***Value 3 can be given as Minor.***
- ***Values 1 and 2 can be denoted as Trivial.***

In some books, the values can be classified into High, Medium, Low, and Very Low.

C. Risk Assessment

- It is assessment of the disruption to critical activities, which are supportedby resources such as people, process, technology, information, infrastructure supplies and stakeholders.
- The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality. It is the decision of the enterprise to select a risk assessment approach, but it is important that it is suitable and appropriate to address all of the enterprise's requirements.
- Specific **Threats** may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.
- **Vulnerabilities**might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience. The Security Assessment willenable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist. This is similar to vulnerability assessment phase of developing aBCP.

Impacts might result from the exploitation of vulnerabilities by threats. As a result of the BIA and the risk assessment, the enterprise should identify measuresthat:

- reduce the likelihood of adisruption;
- shorten the period of disruption;and
- limit the impact of a disruption on the enterprise's key products andservices.

These measures are known as loss mitigation and risk treatment.

13. BCM STRATEGYPROCESS:

Much preparation is needed to implement the strategies for protecting critical functions andtheir supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundantcapability.

The enterprise develops and documents a series of plans, which enable them to effectively manage an incident and subsequently recover its critical activities and their supporting resources, within the timescales agreed with the customer. While some activities have been defined as non-critical, the actions required to recover these are also included in the business continuity plans as they assist in allowing the critical activities to operate in a more efficient and effective manner. The enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and/ or reduce the potential impact of those incidents and mitigation measures for both critical and non criticalactivities.

14. BCM DEVELOPMENT AND IMPLEMENTATION PROCESS:

The enterprise should have an exclusive organization structure, Incident Management Team / Crisis management team for an effective response and recovery from disruptions. In the event ofany incident, there should be a structure to enable the enterprise to:

- **confirm** Impact of incident (nature and extent),
- **control**of thesituation,
- **contain** theincident,
- **communicate** with stakeholders,and
- **coordinate** appropriateresponse.

A. The Incident Management Plan(IMP)

To manage the initial phase of an incident, the crisis is handled by IMP. The IMP should have top management support with appropriate budget for development, maintenance and training. They should be flexible, feasible and relevant; be easy to read and understand; and provide the basis for managing all possible issues, including the stakeholder and external issues, facing the enterprise during an incidents.

B. The Business Continuity Plan(BCP)

To recover or maintain its activities in the event of a disruption to a normal business operation, the BCP are invoked to support the critical activities required to deliver the enterprise's objectives. They may be invoked in whole or part and at any stage of the response to incident.

The recovery strategies may be two-tiered:

- Business: Logistics, accounting, human resources, etc; and
- Technical: Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voicenetworks).

15. BCM TESTING AND MAINTENANCEPROCESS:

Various aspects of BCM Testing and Maintenance Process are given as follows:

A. BCM Testing

A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to beclearly defined in the BCP. A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation. Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovativesolutions.

The BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.) and technology and telecommunications recovery, including the availability and relocation of staff.

In addition, it might lead to the improvement of BCM capability by:

- Practicing the enterprise's ability to recover from an incident;
- Verifying that BCP incorporates all enterprise critical activities &their dependencies &priorities;
- Highlighting assumptions, which need to be questioned;
- Instilling confidence amongst exercise participants;
- Raising awareness of business continuity throughout the enterprise by publicizing the exercise;
- Validating the effectiveness and timeliness of restoration of critical activities; and
- Demonstrating competence of the primary response teams and their alternatives.

The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements. However, the testing program should be flexible, taking into account the rate of change within the enterprise, and the outcomeof previous one. The above exercise methods can be employed for individual plan components, and single and multiple plans. In case of Development of BCP, the objectives of performingBCP tests are to ensure that:

- The recovery procedures are complete and workable.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- The manual recovery procedures and IT backup system/s are current and can either be operational orrestored.
- The success or failure of the business continuity training program is monitored.

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 testpurpose/approach;
- Identifying testteams;
- Structuring thetest;
- Conducting thetest;
- Analyzing test results;and
- Modifying the plans asappropriate.

The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive andaccurate.

B. BCM Maintenance

It is important to keep preparations including documentation, up-to-date. Contracts and agreements may also need to reflect the changes. If additional equipmentis needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

Similarly, the maintenance tasks undertaken in Development of BCP are to:

- Determine **the ownership and responsibility**for maintaining the various BCP strategies within theenterprise;
- Identify the **BCP maintenance triggers**to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remainsup-to-date;
- Determine the **maintenance regime**to ensure the plan remains up-to-date;
- Determine the **maintenance processes**to update the plan; and
- Implement **version control procedures**to ensure that the plan is maintained up-to-date.

C. Reviewing BCMArrangements

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 enterprise's BCM strategy;
- The **enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities** and requirements (the enterprise's objectives);
- 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;
- 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;
- The **enterprise's BCM maintenance and exercising programs have been effectively implemented**;
- **BCM strategies and plans incorporate improvements** identified during incidents and exercises and in the maintenance program;
- The **enterprise has an ongoing program** for BCM training and awareness;
- BCM procedures have been **effectively communicated to relevant staff**, and that those staff understand their roles and responsibilities; and
- **Change control processes**are in place and operate effectively.

16. BCM TRAININGPROCESS:

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

- Developing a BCM program more efficiently;
- Providing confidence in its stakeholders (especially staff and customers) in its ability to handle businessdisruptions;
- Increasing its resilience over time by ensuring BCM implications are considered indecisions at all levels;and
- Minimizing the likelihood and impact of disruptions

Development of a BCM culture is supported by:

- **Leadership**from senior personnel in the enterprise;
- **Assignment**ofresponsibilities;
- **Awareness**raising;
- **Skills training**;and
- **Exercisingplans**.

A. Training, Awareness and Competency

While developing the BCM, the competencies necessary for personnel within the system have been determined. These are given asfollows:

- Actively listens to others, their ideas, views and opinions;
- Provides support in difficult or challenging circumstances;
- Responds constructively to difficult circumstances;
- Adapts leadership style appropriately to match the circumstances;
- Promotes a positive culture of health, safety and the environment;
- Recognizes and acknowledges the contribution of colleagues;
- Encourages the taking of calculated risks;
- Encourages and actively responds to new ideas;
- Consults and involves team members to resolve problems;
- Demonstrates personal integrity;and
- Challenges established ways of doing things to identify improvement opportunities.

17. TYPES OF PLANS:

There are various kinds of plans that need to be designed. They include the following:

A. EmergencyPlan-

The emergency plan specifies the **actions to be undertaken** immediately when adisaster 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.

- The plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'.
- Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files ,and termination of power.
- Third, any evacuation procedures required must be specified.
- Fourth, return procedures (e.g., conditions that must bemet before the site is considered safe) mustbe designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

B. Back-upPlan

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,
- prioritiesto be assigned to recovering the various systems, and a time frame for recovery of each system.

For some resources, the procedures specified in the backup plan might be straightforward. In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain. For example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire.

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. Indeed, it is prudent to have more than one person knowledgeable in a backup task incase someone is injured when a disaster occurs. Similarly, lists of hardware and software must be updated to reflect acquisitions and disposals.

C. RecoveryPlan-

The backup plan is intended to restore operations quickly so that information system functioncan continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities.

Recovery plan should identify a recovery committee that willbe responsible for working out the specifics of the recovery to be undertaken.

- The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed.
- The plan might also indicate which applications are to be recovered first.

Members of a recovery committee must understand their responsibilities. Again, the problem is thatthey will be required to undertake unfamiliar tasks. 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 theirresponsibilities.

D. TestPlan-

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, backup, or recovery plans or in the preparedness of anorganization and its personnel for facing a disaster.

It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can bedeemed satisfactory.

Periodically, test plans must be invoked. 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, the disaster recovery plan can be tested by **desk checking and inspection and walkthroughs**, much like the validation procedures adopted for programs.
- Next, a **disaster can be simulated at a convenient time**-for example, during a slow period in the day. Anyone, who will be affected by the test (e.g. personnel and 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 testsof the organization's ability to recover from a catastrophe.

18. 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:

(i) **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 incrementalor 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 thatdo not occupy too much storage space. The Windows operating system lets us to copy a full backupon several DVD disks. Any good backup plan has at least one full backup of aserver.

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. The cycle continues thisway.

Advantages

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

Disadvantages

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

(ii) **Incremental Backup:**

An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. ***The last backup can be afullbackupor 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 backupon Wednesday will include only the changes and new files since Tuesday'sbackup. The cycle continues this way.

Advantages:

- ***Much fasterbackups.***
- ***Efficient use of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.***

Disadvantages:

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

(iii) 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 andsubsequent 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.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files thatwere already included in earlier differential backups.

For example - Suppose a differential backup job or task is to be doneevery 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 willonly 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 incrementalbackups.***

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 differentialbackup.***
- ***Restores are slower than with full backups.***
- ***Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the lastdifferential backup are needed to perform a restore.***

(iv) **Mirror back-up:** ***Mirror backups are, as the 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 orthrough a virus may also cause that same file in mirror to be deleted as well. Some donot 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 apassword. A mirrorbackup 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 kepton the storage server for at least 30 days before it is eventually deleted. This helpsstrike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software 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.***

19. ALTERNATE PROCESSING FACILITY ARRANGEMENTS:

Security administrators should consider the following backup options:

- **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 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 organisationto provide a cold-sitefacility.

- **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-siteneeds.

- **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 orinstall. 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.

- **Reciprocal Agreement:** Two or more organisationsmight 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 tooperate another's criticalsystem.

20. 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:

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

21. DISASTER RECOVERY PROCEDURALPLAN:

The disaster recovery planning document may include the following areas:

- The **conditions for activating the plans**, which describe the process to be followed before each plan, areactivated.
- **Various procedures to be undertaken:**
  - **Emergency procedures**, which describe the actions to be taken followingan incident which jeopardizes business operations and/or human life. e.g. police, fire, services and local government.
  - **Fallback procedures**, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
  - **Resumption procedures**, which describe the actions to be taken to return to normal businessoperations.
- **A maintenance schedule**, which specifies 'how and when the plan will be tested', and the process for maintaining theplan.
- **Awareness and education activities**, which are designed to createan understanding of the business continuity, process and ensure that the business continues to be effective.
- The **responsibilities of individuals**describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- **Contingency plan** document distributionlist.
- **Contingency plan testing** and **recovery**procedure and **updating** the contingency plan on a regular basis
- Detailed description of the **purpose and scope of the plan**.
- **List of vendors doing business with the organization**, their contact numbers and address for emergencypurposes.
- **List of phone numbers of employees**in the event of an emergency.
- **Emergency phone list for fire, police, hardware, software, suppliers, customers, back -up location,etc.**
- **Medical procedure**to be followed in case of injury.
- **Insurance papers and claimforms**.
- **Names of employees trained for emergency situation**, first aid and life saving techniques.
- **Details of airlines, hotels and transport arrangements**.
- **Alternate manual procedures**to be followed such as preparation of invoices.
- **Back-up location** contractual agreement, correspondences.
- Primary **computer centre hardware, software, peripheral equipment &software**configuration.
- **Location of** data and program files, data dictionary, documentation manuals, source and object codes and back-upmedia.

22. AUDIT OF THE 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 a disruption.
- The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period.
- BCP Auditor is expected to identify residual risks, which are not identified 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 steps are given below:

(i) Determine if a **disaster recovery/business resumption plan exists**and was developed using a sound methodology ?

A **DRP/BRP** should includes the following elements:

- ∉ Identification and prioritization of the activities, which are essential to continue functioning.
- ∉ Is Theplan is based upon a BIA that considers the impact of the loss of essentialfunctions.
- ∉ Operations managers and key employees participated in the development of theplan.
- ∉ The plan identifies the resources that will likely be needed for recovery and the location of theiravailability.
- ∉ The plan is simple and easily understood so that it will be effective when it is needed.
- ∉ The plan is realistic in its assumption

(ii) Determine **if information backup procedures are sufficient**to allow for recovery of critical data.

(iii) Determine if **a test plan exists** and to what extent the disaster recovery/business resumption plan has beentested.

(iv) Determine if **resources have been made available**to maintain the disaster recovery/ business resumption plan and keep it current.

(v) Obtain and review the **existing disaster recovery/ business resumption plan**.

(vi) Obtain and review **plans for disaster recovery/ business resumption testing** and/or documentation of actualtests.

(vii) Obtain and review the **existing business impact analysis**.

(viii) **Gather background information**to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.

(ix) Determine if **copies of the plan**are safeguarded by off-site storage.

(x) Gain an understanding of the **methodology used to develop the existing disasterrecovery/ business resumption plan**. Who participated in the development effort?

(xi) Gain an understanding of the **methodology used to develop the existing business impact analysis.**

(xii) Determine if **recommendations made by the external firm**who produced the business impact analysis have been implemented or otherwise addressed.

(xiii) Have **resources been allocated**to prevent the disaster recovery/ business resumption plan from becoming outdated andineffective?

(xiv) Determine if the **plan is dated each time that it is revised**so that the most current version willbe used ifneeded.

(xv) Determine if the **plan has been updated within past 12 months**.

(xvi) Determine all the **locations where the DRP/BRP is stored.**Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?

(xvii) **Review information backup procedures**in general. The availability of backup data could be critical in minimizing the time needed for recovery.

(xviii)**Interview functional area managers**or key employees to determine their understanding of the disaster recovery/ business resumption plan.

- ∉ Does the disaster recovery/ business resumption plan include provisions for Personnel?
- ∉ Do they have a clear understanding of their role in working towards the resumption of normal operations?
- ∉ Have key employees seen the plan and are all employees aware that there is such a plan? Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
- ∉ Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
- ∉ Does the disaster recovery/ business resumption plan include provisions for people with specialneeds?
- ∉ Does the disaster recovery/ business resumption plan have a provision for replacement staff whennecessary

(xix) Building, Utilities andTransportation:

- ∉ Does the DRP/BRPhave a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- ∉ Does the DRP/BRPconsider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the samedisaster.
- ∉ Review any agreements for use of backup facilities.
- ∉ Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- ∉ Does the DRP/BRP consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- ∉ Are building safety features regularly inspected andtested?
- ∉ Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

(xx) InformationTechnology:

- ∉ Determine if the plan reflects the current IT environment.
- ∉ Determine if the plan includes prioritization of critical applications and systems.
- ∉ Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- ∉ Does the DRP/BRPinclude arrangements for emergencytelecommunications?
- ∉ Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- ∉ Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.

(xxi) AdministrativeProcedures:

- ∉ Does the **DRP/BRP** cover administrative and management aspects in addition to operations?
- ∉ Is there a management plan to maintain operations if the building is severely damaged or if access to the buildingis denied or limited for an extended period of time?
- ∉ Is there a designated emergency operations center where incident management teams can coordinate response andrecovery?
- ∉ Determine if the **DRP/BRP** covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.
- ∉ Have essential records been identified? Do we have a duplicate set of essential records stored in a securelocation?
- ∉ To facilitate retrieval, are essential records separated from those that will not be neededimmediately?

(xxii) Does the **DRP/BRP include the names and numbers of suppliers**of essential equipment and other material?

(xxiii) Does the **DRP/BRP**include **provisions for the approvalto expend funds** that were not budgeted for the period? Recovery may be costly.

(xxiv) Has **executive management assigned the necessary resources for plan development**, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the needarise.