Business Continuity Planning and Disaster Recovery Planning

Learning Objectives

- To understand the concept of Business Continuity Management;
- To understand the key phases and components of a Business Continuity Plan,
- To understand the key aspects of BCP Implementation;
- To learn about Back-up and Disaster Recovery Planning; and
- To learn how to audit a BCP.

Task Statements

- To design, develop, implement, test, maintain and audit all key phases and components of a Business Continuity Plan in an enterprise; and
- To conduct Risk assessment and Business Impact Assessment.

Knowledge Statements

- To know the concepts and components of Business Continuity Management;
- To know the development of Business Continuity Plans, Disaster Recovery Plans; Emergency Plans etc; and
- To know the different phases and components of BCP.

4.1 Introduction

Today, the networked society exceeds the boundaries of the nations with increased dependency on supply chain management demanding regulatory compliance, security and privacy of data and above all, improvement in performance and availability of services on 24 x 7 basis. Meeting their demands in global economy requires an enterprise to be able to meet the challenges of ever increasing threats and risks. They should be able to not only withstand but suitably adapt the sudden disruptions due to infrastructure outage or human error, else it might impact not only revenue but also the image and brand, ultimately leading to the survival of the enterprise of all types and sizes, public and private.

Business Continuity Management (BCM), over the years has emerged a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption of all kinds. With the BCM
4.2 Information Systems Control and Audit

Process in place, enterprises are able to assess the potential threats and manage the consequences of the disruption, which could reduce or eliminate the losses that would have resulted.

In order to ensure effective implementation of BCM, the enterprise should conduct regular internal audits at planned intervals to conform to the compliance of Business Continuity Process in line with the policy and regulatory requirements for the enterprise. The findings of the internal audit should be reported to the top management for necessary corrective action and improvements and the management to provide adequate resources to ensure that necessary corrections and corrective actions are taken without undue delay to eliminate nonconformities and their cause. The internal auditing activities should be taken up by the independent group within the enterprises such as internal audit functions managed by Chartered Accountants etc. This would ensure objectivity and impartiality of the audit process engaging the professionals for these key activities.

This chapter provides further insight into the BCM Policy, BCM Processes of management, assessment, strategy development and implementation, testing and maintenance and trainings. This facilitates the understanding of the concept, planning, implementation and continuous improvements of BCPs.

4.2 Need of Business Continuity Management (BCM)

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 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. The purpose of BCP is to ensure that vital business functions (critical business operations) are recovered and operationalized within an acceptable timeframe. The purpose is to ensure continuity of business and not necessarily the continuity of all systems, computers or networks. The BCP identifies the critical functions of the enterprise and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and incident response so as to ensure that the proper procedures will be carried out to ensure the timely restoration of services.

- **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with least impact. It is imperative that every
enterprise whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the enterprise. It is not enough that enterprise has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the enterprise.

4.2.1 BCP Manual

An incident or disaster affecting critical business operations can strike at anytime. Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. The BCP is expected to provide:

- 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, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise’s critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasoning teams between the functional area(s) affected and other departments providing support services.

BCM is business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- Proactively improves an enterprise’s resilience against the disruption of its ability to achieve its key objectives;
- Provides a rehearsed method of restoring an enterprise’s ability to supply its key products and services to an agreed level within an agreed time after a disruption; and
- Delivers a proven capability to manage a business disruption and protect the enterprise’s reputation and brand.

4.2.2 Scope of Business Continuity

Top management of the enterprise needs to define the scope of the BCM program by 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 case of 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.
4.2.3 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.

4.3 BCM Policy

The main objective of BCP is to minimize/eliminate the loss to enterprise’s business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction. This policy document is a high level document, which shall be the guide to make a systematic approach for disaster recovery, to bring about awareness among the persons in scope about the business continuity aspects and its importance and to test and review the business continuity planning for the enterprise in scope.

While developing the BCM policy, the enterprise should consider defining the scope, BCM principles, guidelines and minimum standards for the enterprise. They should refer any relevant standards, regulations or policies that have to be included or can be used as a benchmark. 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 be identified.
- 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 updation as required.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

The 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. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the enterprise, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process market, technology or organizational structure.
4.4 Business Continuity Planning

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. In fact, these consequences may be more severe because of the lost time that results from inadequate planning. After such an event, it is typical for senior management to become concerned with all aspects of the occurrence, including the measures taken to limit losses.

Their concerns range from the initiating event and contributing factors, to the response plans, effective contingency planning and disaster recovery coordination. Rather than delegating disaster avoidance to the facilities or building security organizations, it is preferable for a firm’s disaster recovery planner(s) to understand fully the risks to operations and the measures that can minimize the probabilities and consequences, and to formulate their disaster recovery plan accordingly.

When a risk manifests itself through disruptive events, the business continuity plan 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:** 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.

The Business Continuity Life Cycle is broken down into four broad and sequential sections:

- Risk assessment,
- Determination of recovery alternatives,
- Recovery plan implementation, and
- Recovery plan validation.

Within each of these lifecycle sections, the applicable resource sets are manipulated to provide the organization with the best mix or critical resource quantities at optimum costs with minimum tangible and intangible losses. These resource sets can be broken down into the
4.6 Information Systems Control and Audit

following components: Information, Technology, Telecommunication, Process, People, and Facilities.

4.4.1 Objectives and Goals of 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 re-establish 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:

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

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

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

4.5 Developing a Business Continuity Plan

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:

- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- Obtaining commitment from appropriate management to support and participate in the effort;
- Defining recovery requirements from the perspective of business functions;
- Documenting the impact of an extended loss to operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
Selecting business continuity teams that ensure the proper balance required for plan development;
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.

The eight phases are given as follows:

(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
(viii) Initial Plan Testing and Plan Implementation

Each of these phases are described below:

- **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. This enables the project team to:
  - refine the scope of the project and the associated work program;
  - develop project schedules; and
  - identify and address any issues that could have an impact on the delivery and the success of the project.

  During this phase, a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis.

  Two other key deliverables of this phase are:
  - The development of a policy to support the recovery programs; and
  - An awareness program to educate management and senior individuals who will be required to participate in the project.

- **Phase 2 – Vulnerability Assessment and General Definition of Requirements:** Security and controls within an organization are continuing concern. It is preferable from
4.8 Information Systems Control and Audit

an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

This phase will include the following key tasks:

- A thorough Security Assessment of the computing and communications environment including personnel practices; 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.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- 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 following implementation.
- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.

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. 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 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 (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) 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 components are defined and plans 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. 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. 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. 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.

The approach taken to test the plans depends in large part, 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 and accurate.
### 4.6 Components of BCM Process

Components of BCM Process are given as follows (in Fig. 4.6.1):

<table>
<thead>
<tr>
<th>Stage</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1</td>
<td><strong>Information Collection</strong></td>
</tr>
<tr>
<td>Stage 2</td>
<td><strong>BCM Strategies</strong></td>
</tr>
<tr>
<td>Stage 3</td>
<td><strong>Development &amp; Implementation</strong></td>
</tr>
<tr>
<td>Stage 4</td>
<td><strong>Testing and Maintenance</strong></td>
</tr>
<tr>
<td>Stage 5</td>
<td><strong>BCM Training</strong></td>
</tr>
</tbody>
</table>

**BCM – Process**

The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.

**BCM – Information Collection Process**

The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
Business Continuity Planning and Disaster Recovery Planning

- **BCM – Strategy Process**
  Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.

- **BCM – Development and Implementation Process**
  Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

- **BCM – Testing and Maintenance Process**
  BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.

- **BCM – Training Process**
  Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise’s core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

These components are explained below in detail.

### 4.7 Business Continuity Management Process

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:

#### 4.7.1 Organization Structure

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.

#### 4.7.2 Implementing Business Continuity in the Enterprise and Maintenance

In establishing and implementing the BCM system in the organization, managers from each function on site represent their areas of the operation. These people are also responsible for the ongoing operation and maintenance of the system within their area of responsibility. Where training is required to enable as a colleague to effectively carry out their BCM responsibilities, this will be identified as part of the ongoing staff appraisal and training process.
Top management should appoint the Manager (BCM) role as being the role that is responsible for the BCM policy and its implementation. The Resource Planning Manager is supported by the Shift Leaders and Team Captains from each function, who are responsible for the ongoing implementation and maintenance of the BCM. The program should be communicated to all the stakeholders with appropriate training and testing. The enterprise may adopt any project management model for effective output.

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

- Defining the scope & context;
- Defining roles and responsibilities;
- Engaging and involving all stakeholders;
- Testing of program on regular basis;
- Maintaining the currency & appropriateness of business continuity program;
- 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.

### 4.7.3 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:

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.
To provide evident of the effective operation of the BCM, records demonstrating the operation should be retained for a minimum period of 1 year, in line with enterprise’s policy. The nature of the record means that the retention is a statutory, regulatory or customer requirement, it will be retained for the amount of time dictated. These records include reference to all business interruptions and incidents, irrespective of the nature and length of disruption. This also includes general and detailed definition of requirements as described in developing a BCP. In this, a profile is developed by identifying resources required to support critical functions, which include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipments, etc.) and personnel for each business unit.

4.8 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 enterprise operates;
- 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 and resources; 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 enables us 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. Two other key deliverables of that phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

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 an accurate 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. This review will ensure that the findings and the decisions made as a result of the findings are still accurate and relevant to the needs of the operation and its stakeholders.

4.8.1 Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and
4.14 Information Systems Control and Audit

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 “pain threshold,” that is, the length of time business units can survive without access to the system, services and facilities. For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

- assess the impacts that would occur if the activity was disrupted over a period of time;
- identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;
- assess the minimum level at which the activity needs to be performed on its resumption;
- identify the length of time within which normal levels of operation need to be resumed; and
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

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. Developing the BCP also takes into account the BIA process.

4.8.2 Classification of Critical Activities

BCP leader and BCP team leaders in consultation with respective function owner shall carry out Business Impact Analysis 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:
  - Loss of revenue;
  - Loss of reputation;
  - Decrease in customer satisfaction; and
  - Loss of productivity (man-hours).

These parameters shall be graded in a three-point scale 1-3 where,

1 = Low (L)
2 = Medium (M)
3 = High (H)
- **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).

<table>
<thead>
<tr>
<th>3 (minor)</th>
<th>6 (Major)</th>
<th>9 (Catastrophic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (Trivial)</td>
<td>4 (Major)</td>
<td>6 (Major)</td>
</tr>
<tr>
<td>1 (Trivial)</td>
<td>2 (Trivial)</td>
<td>3 (Minor)</td>
</tr>
</tbody>
</table>

  **Fig. 4.8.1: Business Impact Matrix (1)**

  Identify all the mission critical processes for categorizing into Vital, Essential and Desirable and looking for the probable disasters as per the list attached.

  The Business Impact Analysis matrix is also used to assess Risk and is thus also referred as Risk Assessment Matrix. The interpretation of Fig. 4.8.1 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 X Axis

  **Likelihood of Occurrence**

  Based on the likelihood of the occurrence of a risk, 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 of occurrence.

  **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 too significant.

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.

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.

### 4.8.3 Risk Assessment

The risk assessment is assessment of the disruption to critical activities, which are supported by 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 will enable 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 a BCP.

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

- reduce the likelihood of a disruption;
- shorten the period of disruption; and
- limit the impact of a disruption on the enterprise’s key products and services.

These measures are known as loss mitigation and risk treatment. Loss mitigation strategies can be used in conjunction with other options, as not all risks can be prevented or reduced to an acceptable level. The enterprise might include one or more or all of the strategies for each critical activity.

### 4.9 BCM Strategy Process

Much preparation is needed to implement the strategies for protecting critical functions and their 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 redundant capability.

The enterprise develops and documents a series of plans, which enable them to effectively manage an incident with impacts on the site operations 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 resilience and mitigation measures for both critical and non-critical activities.

### 4.10 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 of any incident, there should be a structure to enable the enterprise to:

- confirm Impact of incident (nature and extent),
- control of the situation,
- contain the incident,
4.18 Information Systems Control and Audit

- communicate with stakeholders, and
- coordinate appropriate response.

4.10.1 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.

4.10.2 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 voice networks).

The plan development phase also includes the implementation of changes to use 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. Recovery standards are also developed during this phase. The organization’s recovery strategy needs to be developed for the recovery of the many business processes.

4.11 BCM Testing and Maintenance Process

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

4.11.1 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 be clearly 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 innovative solutions.

An exercise program should leads to objective assurance that the BCP will work as anticipated when required. 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:
Business Continuity Planning and Disaster Recovery Planning

- Practicing the enterprise’s ability to recover from an incident;
- Verifying that the BCP incorporates all enterprise critical activities and their dependencies and 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 outcome of 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 performing BCP 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 or restored.
- 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 test purpose/approach;
- Identifying test teams;
- Structuring the test;
- Conducting the test;
- Analyzing test results; and
- Modifying the plans as appropriate.

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 and accurate.
4.11.2 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 equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization’s architecture. The BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise’s business continuity program; the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise’s structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise’s business continuity and incident management plans.

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

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- 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 remains up-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.

4.11.3 Reviewing 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 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.
4.12 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 (especially staff and customers) in its ability to handle business disruptions;
- Increasing its resilience over time by ensuring BCM implications are considered in decisions 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 of responsibilities;
- Awareness raising;
- Skills training; and
- Exercising plans.

4.12.1 Training, Awareness and Competency

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined. These are consistent with the competencies required by the organization of the relevant role and are given as follows:

- 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.
4.13 Types of Plans

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

4.13.1 Emergency Plan

The 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. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated. First, 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 be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

4.13.2 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 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. For example, microcomputer users might be admonished to make backup copies of critical files and store them off site. 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 in case someone is injured when a disaster occurs. Similarly, lists of hardware and software must be updated to reflect acquisitions and disposals.

4.13.3 Recovery Plan

The backup plan is intended to restore operations quickly so that information system function can 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 will be 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 that they 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 their responsibilities.

### 4.13.4 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, backup, or recovery plans or in the preparedness of an organization 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 be deemed 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 tests of the organization's ability to recover from a catastrophe.

### 4.14 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 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. The cycle continues this way.*
Advantages
- 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
- 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.

(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 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
- Much faster backups.
- 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 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.
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 that were already included in earlier differential backups.

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 than full backups.
- More efficient use of storage space than 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 than 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 but simpler than incremental backups. Only the full backup set and the last differential 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 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...
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.

4.15 Alternate Processing Facility Arrangements

Security administrators should consider the following backup options:

- **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.

- **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.

- **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.

- **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.

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 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 a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- 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.
These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

4.16 Disaster Recovery Procedural Plan

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, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities 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 business operations.
- A maintenance schedule, which specifies ‘how and when the plan will be tested’, and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an 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 distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- 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.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
4.28 Information Systems Control and Audit

- Primary computer centre hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

4.17 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 that includes the following elements:
   - Identification and prioritization of the activities, which are essential to continue functioning.
   - The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
   - Operations managers and key employees participated in the development of the plan.
   - The plan identifies the resources that will likely be needed for recovery and the location of their availability.
   - The plan is simple and easily understood so that it will be effective when it is needed.
   - The plan is realistic in its assumptions.

(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 been tested.

(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 actual tests.
(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 disaster recovery/ 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 and ineffective?
(xiv) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.
(xv) Determine if the plan has been updated within past 12 months.
(xvi) Determine all the locations where the disaster recovery/ business resumption plan 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. Do they have a clear understanding of their role in working towards the resumption of normal operations?
  • Does the disaster recovery/ business resumption plan include provisions for Personnel?
  • 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 special needs?
  • Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?
(xix) Building, Utilities and Transportation

- Does the disaster recovery/business resumption plan have 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 disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- 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 disaster recovery/business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?
- 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) Information Technology

- 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 disaster recovery/business resumption plan include arrangements for emergency telecommunications?
- 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) Administrative Procedures

- Does the disaster recovery/business resumption plan 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 building is denied or limited for an extended period of time?
- Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
Business Continuity Planning and Disaster Recovery Planning

- Determine if the disaster recovery/business resumption plan 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 secure location?

- To facilitate retrieval, are essential records separated from those that will not be needed immediately?

(xxii) Does the disaster recovery/business resumption plan include the names and numbers of suppliers of essential equipment and other material?

(xxiii) Does the disaster recovery/business resumption plan include provisions for the approval to 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 need arise.

4.18 Summary

In order to demonstrate responsiveness to business requirements and addressing the needs of all the stakeholders, it is imperative to establish the BCM process in any enterprise. The advantages of having an effective business continuity process are numerous but the most important factor is the brand value and the reputation of the enterprise. Therefore, the management has to have adequate resource provision in terms of budget, skilled manpower, technology etc. to establish BCM process and lead the industry sector by providing uninterrupted continuous 24 x 7 operations to the external as well as internal customers.

BCM identifies itself as a management approach by focusing on aligning an enterprise with its customers through the execution of processes. It enables the enterprises to be more efficient and effective by becoming a process-based enterprise.