

4. Business Continuity Planning and Disaster Recovery Planning

4.1 Types of Plans

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.
- 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 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.

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 systems and a time frame for recovery of each system.
- The backup plan needs continuous updating as changes occur.

3. Recovery Plan

- Recovery plans set out procedures to restore full information system capabilities. The plan might also indicate which applications are to be recovered first.
- 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.
- 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. 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.
- Periodically, test plans must be invoked. Unfortunately, top managers are 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. 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.

4.2 Types of Back-ups

- When the back-ups are taken of the system and data together, they are called total system's back-up. Various types of back-ups are given as follows:

1. Full Backup –

- ✦ 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.
- ✦ However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

2. Incremental Backup –

- ✦ An incremental backup captures files that were created or changed since the last backup, regardless of backup type.
- ✦ This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
- ✦ Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup and then recovering from every incremental backup taken since

3. Differential Backup –

- ✦ A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete.
- ✦ 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.

4. Mirror back-up –

- ✦ 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.

4.3 Alternate Processing Facility Arrangements

- Security administrators should consider the following backup options:

1. Cold site –

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

2. Hot site –

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

3. Warm site –

- ✦ A warm site provides an intermediate level of backup.
- ✦ It has all cold-site facilities in addition to hardware that might be difficult to obtain or install.
- ✦ For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

4. Reciprocal agreement –

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

5. 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 organization that will be allowed to use the site concurrently in event of 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.

4.4 Disaster Recovery Procedural Plan

- The disaster recovery planning document may include the following areas:
 - ✦ The conditions for activating the plans.
 - ✦ Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life.
 - ✦ Fallback procedures, which describe the actions to be taken to move essential business activities to alternate temporary locations, to bring business process back into operation in required time-scale.
 - ✦ Resumption procedures, which describe actions to be taken to return to normal operation.
 - ✦ 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.
 - ✦ 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, supplier, customer, backup location etc.
 - ✦ Medical procedure to be followed in case of injury.
 - ✦ Back-up location contractual agreement, correspondences.
 - ✦ Insurance papers and claim forms.
 - ✦ 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.

4.5 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 interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.
- 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.
- Business continuity covers the following areas:
 - i). Business Resumption Planning:**
 - ✦ This is the operation's piece of business continuity planning.
 - ii). 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.
 - iii). 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.

4.5.1 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 disruption and enable an organization to survive a disaster and to reestablish business operations.
- **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;
 - ✦ 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.

- **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.

4.6 Developing a Business Continuity Plan

- The methodology for developing a BCP can be sub-divided into eight different phases. 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 & impact minimization as well as orderly recovery;
 - ✦ Selecting business continuity teams that ensure 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:
 - 1) Pre-Planning Activities (Business Continuity Plan Initiation)
 - 2) Vulnerability Assessment and General Definition of Requirements
 - 3) Business Impact Analysis
 - 4) Detailed Definition of Requirements
 - 5) Plan Development
 - 6) Testing Program
 - 7) Maintenance Program
 - 8) Initial Plan Testing and Plan Implementation

4.6.1 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 delivery and 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 Project Manager should work with the Steering Committee in finalizing the detailed work plan.
- 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. 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.

Phase 4 – Detailed Definition of Requirements:

- During this phase, a profile of recovery requirements is developed and used as a basis for analyzing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3.
- This profile should include hardware, software, and 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 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 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. 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.

4.7 Components of BCM Process

Components of BCM Process are given as follows:

1) BCM – Process

- The management process enables the business continuity, capacity and capability to be established and maintained.

2) 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.

3) 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.

4) BCM – Development and Implementation Process

- Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

5) 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, accurate and Identifies opportunities for improvement.

6) BCM – Training Process

- Extensive training in BCM framework, incident management, business continuity, business recovery and restoration plans enable it to become part of the enterprises core value and provide confidence in all stakeholders in the ability of enterprise to cope with minimum disruptions and loss of service.

4.8 Business Continuity Management – Process:

- A BCM process should be in place to address the policy and objectives as defined in the business continuity policy. The BCM Processes are mapped as follows:

4.8.1 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.

4.8.2 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.

- Top management should appoint the Manager (BCM), responsible for implementation of BCM policy. The Resource Planning Manager is supported by the Shift Leaders and Team Captains from each function. The program should be communicated to all stakeholders with appropriate training & testing.
- 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.

4.8.3 BCM Documentation and Records

- All document that form the BCM are subject to the document control and record control processes.
- The following documents 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 and record control process;
 - ✦ 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.
- This also includes general and detailed definition of requirements as described in developing a BCP.

4.9 BCM Information Collection Process

- The pre-planning phase of Developing the BCP also involves collection of information.
- 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, 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.
- 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.

4.9.1 Business Impact Analysis (BIA)

- Business Impact Analysis (BIA) is a means of systematically assessing the potential impacts resulting from various events or incidents. The enterprise should have a documented approach to conduct BIA.
- 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.
- 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.
- 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.

4.9.2 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:

1. Business Categorization (Vital/essential/desirable):

- ✦ The parameter 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)

2. 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 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 [Desirable (1), Essential (2), Vital (3)]

4.9.3 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 & stakeholders.
- 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.
- The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist.

- 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.
- 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.

4.10 BCM Strategy Process

- Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources.
- 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.
- The enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and reduce the potential impact of those incidents and resilience and mitigation measures for both critical and non-critical activities.

4.11 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,
 - ✦ communicate with stakeholders, and
 - ✦ Coordinate appropriate response.

4.11.1 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.

4.11.2 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.

- The recovery strategies may be two-tiered:
 - ✦ Business: Logistics, accounting, human resources, etc.; and
 - ✦ Technical: Information Technology (e.g. desktop, server, mainframe computers, data & voice networks).
- Recovery standards are developed during this phase.

4.12 BCM Testing and Maintenance Process

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

4.12.1 BCM Testing

- A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation.
- The BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure and technology and telecommunications recovery, including the availability and relocation of staff.
- The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements.
- **In addition, it might lead to the improvement of BCM capability by:**
 - ✦ Practicing the enterprise's ability to recover from an incident;
 - ✦ Verifying that the 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.
- **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 systems 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.

4.12.2 BCM Maintenance

- 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 BCP and IMP.
- 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 organizational, 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.

4.12.3 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 BCM maintenance and exercising programs have been effectively implemented;
 - ✦ 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;
- ✦ 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.

4.13 BCM Training Process

- An enterprise with BCM uses training as a tool to initiate a culture of BCM in all stakeholders by:
 - ✦ Developing a BCM program more efficiently;
 - ✦ Providing confidence in its stakeholders 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.

4.13.1 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.

4.14 Business Continuity Management (BCM)

- Business Continuity Management (BCM), 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.
- In order to ensure effective implementation of BCM, the enterprise should conduct regular internal audits to conform to the compliance of Business Continuity Process. The findings of the internal audit should be reported to top management for necessary corrective action and improvements.
- 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.

4.14.1 Key Terms related to Business Continuity Management (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 and assure continuity of minimum level of services necessary for critical operation.
 - ✦ The purpose is to ensure continuity of business and not necessarily the continuity of all systems.
 - ✦ 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.

4.15 BCP Manual

- 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 business operation.
- 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 function.
- Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity.
- 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.

4.17 Advantage of Business Continuity

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

4.18 BCM Policy

- 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 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.
- BCM 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.

- 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.