

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.1. 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.

- 1) **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.
- 2) **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.
- 3) **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with least impact. It is implied 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. 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:

- 1) **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.
- 2) **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.

4.3. 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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.4. Advantage of Business Continuity

The advantages of BCM are that the enterprise:

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

4.5. 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 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. 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:

- 1) Critical services and activities undertaken by the enterprise operation for the customer will be identified.
- 2) 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.
- 3) Invocation of incident management and business continuity plans can be managed.
- 4) Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updation as required.
- 5) Planning and management responsibility are assigned to a member of the relevant senior management team.

4.6. 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.

Business continuity covers the following areas:

- 1) **Business Resumption Planning:** This is the operation's piece of business continuity planning.
- 2) **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.
- 3) **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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

The business continuity life cycle is broken down into four broad and sequential sections:

- 1) Risk assessment,
- 2) Determination of recovery alternatives,
- 3) Recovery plan implementation, and
- 4) Recovery plan validation.

4.7. 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:

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

Therefore, the goals of the business continuity plan should be to:

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

4.8. 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:

- 1) **Providing management** with a **comprehensive understanding** of the total **efforts required** to develop and maintain an effective recovery plan;
- 2) **Obtaining commitment** from appropriate management to support and participate in the effort;
- 3) **Defining recovery requirements** from the perspective of business functions;
- 4) **Documenting the impact** of an extended loss to operations and key business functions;
- 5) **Focusing** appropriately **on disaster prevention and impact minimization**, as well as orderly recovery;
- 6) **Selecting** business continuity **teams** that ensure the proper balance required for plan development;
- 7) **Developing a business continuity plan** that is understandable, easy to use and maintain; and
- 8) 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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

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

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:

- a) refine the scope of the project and the associated work program;
- b) develop project schedules; and
- c) 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.

Two other key deliverables of this phase are:

- a) The development of a policy to support the recovery programs; and
- b) 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 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) 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.
- b) 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.
- c) 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.
- d) Define the scope of the planning effort.
- e) 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.
- f) Develop a Plan Framework.
- g) Assemble Project Team and conduct awareness sessions.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

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:

- a) identify critical systems, processes and functions;
- b) assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
- c) 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:

- a) Defining the test purpose/approach;
- b) Identifying test teams;
- c) Structuring the test;
- d) Conducting the test;
- e) Analyzing test results; and
- f) Modifying the plans as appropriate.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.9. Components of BCM Process

- 1) **BCM - Management 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.
- 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. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- 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. The selection of strategy will take into account the processes and technology already present within the enterprise.
- 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 and accurate; and Identifies opportunities for improvement.
- 6) **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.

4.10. BCM 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:

- 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.
- 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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

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

- a) Defining the scope & context;
 - b) Defining roles and responsibilities;
 - c) Engaging and involving all stakeholders;
 - d) Testing of program on regular basis;
 - e) Maintaining the currency & appropriateness of business continuity program;
 - f) Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and business impact analysis (BIAs);
 - g) Managing costs and benefits associated; and
 - h) Convert policies and strategies into action.
- 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.
- a) The business continuity policy;
 - b) The business continuity management system;
 - c) The business impact analysis report;
 - d) The risk assessment report;
 - e) The aims and objectives of each function;
 - f) The activities undertaken by each function;
 - g) The business continuity strategies;
 - h) The overall and specific incident management plans;
 - i) The business continuity plans;
 - j) Change control, preventative action, corrective action, document control and record control processes;
 - k) Local Authority Risk Register;
 - l) Exercise schedule and results;
 - m) Incident log; and
 - n) Training program.

To provide evidence 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.

4.11. 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:

- 1) enterprise's objectives, stakeholder obligations, statutory duties and the environment in which the enterprise operates;
- 2) activities, assets and resources, including those outside the enterprise, that support the delivery of these products and services.
- 3) impact and consequences over time of the failure of these activities, assets and resources; and
- 4) Perceived threats that could disrupt the enterprise's key products and services and the critical activities, assets and resources that support them.
- 5) 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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.12. 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 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:

- 1) assess the impacts that would occur if the activity was disrupted over a period of time;
- 2) identify the maximum time period after the start of a disruption within which the activity needs to be resumed.
- 3) Identify critical business processes;
- 4) assess the minimum level at which the activity needs to be performed on its resumption;
- 5) identify the length of time within which normal levels of operation need to be resumed; and
- 6) 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.

4.13. 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. For ready reference

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.

As a result of the BIA and the risk assessment, the enterprise should identify measures that:

- 1) reduce the likelihood of a disruption;
- 2) shorten the period of disruption; and
- 3) 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.

4.14. BCM Development and Implementation Process

- 1) 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:
- 2) confirm Impact of incident (nature and extent),
- 3) control of the situation,
- 4) contain the incident,
- 5) communicate with stakeholders, and
- 6) coordinate appropriate response.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.15. 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.

4.16. BCM Testing and Maintenance Process

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

- 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.

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:

- a) Practicing the enterprise's ability to recover from an incident;
- b) Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities;
- c) Highlighting assumptions, which need to be questioned;
- d) Instilling confidence amongst exercise participants;
- e) Raising awareness of business continuity throughout the enterprise by publicizing the exercise;
- f) Validating the effectiveness and timeliness of restoration of critical activities; and
- g) 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 objectives of performing BCP tests are to ensure that:

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

- 2) **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:

- a) Defining the test purpose/approach;
- b) Identifying test teams;
- c) Structuring the test;
- d) Conducting the test;
- e) Analyzing test results; and
- f) Modifying the plans as appropriate.
- g) The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

- 3) **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 business continuity and incident management plans.

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

- a) Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- b) 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
- c) Determine the maintenance regime to ensure the plan remains up-to-date;
- d) Determine the maintenance processes to update the plan; and
- e) Implement version control procedures to ensure that the plan is maintained up-to-date.

4) **Reviewing BCM Arrangements**

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

- a) All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- b) The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives);
- c) 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;
- d) 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;
- e) The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- f) BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- g) The enterprise has an ongoing program for BCM training and awareness;
- h) BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- i) Change control processes are in place and operate effectively.

4.17. **BCM Training Process**

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

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

Development of a BCM culture is supported by:

- 1) Leadership from senior personnel in the enterprise;
- 2) Assignment of responsibilities;
- 3) Awareness raising;
- 4) Skills training; and
- 5) Exercising plans.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.18. Types of Plans

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

- 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 (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.
- 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.
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.
- 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.
- 4) **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.

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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

4.19. 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 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.
- 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

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. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.
- 3) **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
- 4) **Reciprocal agreement:** Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system
- 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
 - a) how soon the site will be made available subsequent to a disaster;
 - b) the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
 - c) the priority to be given to concurrent users of the site in the event of a common disaster;

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

- d) the period during which the site can be used;
- e) the conditions under which the site can be used;
- f) the facilities and services the site provider agrees to make available; and
- g) what controls will be in place and working at the off-site facility.
- h) 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.

Disaster Recovery Procedural Plan

The disaster recovery planning document may include the following areas:

- 1) **The conditions for activating** the plans, which describe the process to be followed before each plan, are activated.
- 2) **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.
- 3) **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.
- 4) **Resumption procedures**, which describe the actions to be taken to return to normal business operations.
- 5) **A maintenance schedule**, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- 6) **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.
- 7) **The responsibilities of individuals** describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- 8) **Contingency plan document distribution list**.
- 9) Detailed **description** of the **purpose** and scope of the plan.
- 10) **Contingency plan testing** and recovery procedure.
- 11) **List of vendors** doing business with the organization, their contact numbers and address for emergency purposes.
- 12) **Checklist for inventory** taking and updating the contingency plan on a regular basis.
- 13) List of **phone numbers** of employees in the event of an emergency.
- 14) **Emergency phone** list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- 15) **Medical procedure** to be followed in case of injury.
- 16) **Back-up location** contractual agreement, correspondences.
- 17) **Insurance papers** and claim forms.
- 18) Primary computer center hardware, software, peripheral equipment and software configuration.
- 19) **Location of data and program files**, data dictionary, documentation manuals, source and object codes and back-up media.
- 20) **Alternate manual procedures** to be followed such as preparation of invoices.
- 21) **Names of employees trained for emergency situation**, first aid and life saving techniques.
- 22) Details of airlines, hotels and transport arrangements.

4.18. 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.

CHAPTER-4

BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

Sample list of BCP Audit steps are given below:

- 1) **Determine that disaster recovery/business is exists** and was **developed using a sound methodology** that includes the following elements:
 - a) **Identification** and **prioritization** of the activities, which are essential to continue functioning.
 - b) The plan is **based upon a business impact analysis** that considers the impact of the loss of essential functions.
 - c) **Operations managers** and key employees **participated** in the development of the plan.
 - d) The plan **identifies the resources** that will likely be **needed for recovery** and the location of their availability.
 - e) The **plan is simple and easily** understood so that it will be effective when it is needed.
 - f) The plan **is realistic in its assumptions**.
- 2) Determine if information **backup procedures**, sufficient to allow for recovery of critical data.
- 3) Determine if a **test plan exists** and to what extent the disaster recovery/business resumption plan has been tested.
- 4) Determine if resources have been made available to maintain the disaster recovery/ business resumption plan and keep it current.
- 5) Obtain and review the existing disaster recovery/ business resumption plan.
- 6) Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests
- 7) Obtain and review the existing business impact analysis.
- 8) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.
- 9) Determine if copies of the plan are safeguarded by off-site storage.
- 10) Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?
- 11) Gain an understanding of the methodology used to develop the existing business impact analysis.
- 12) Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.
- 13) Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?
- 14) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.
- 15) Determine if the plan has been updated within past 12 months.
- 16) 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?
- 17) Review information backup procedures in general. The availability of backup data could be critical in minimizing the time needed for recovery.

CHAPTER-4
BUSINESS CONTINUITY PLANNING AND RECOVERY PLANNING

- 18)** 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?
- a) Does the disaster recovery/ business resumption plan include provisions for Personnel
 - b) Have key employees seen the plan and are all employees aware that there is such a plan?
 - c) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
 - d) Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
 - e) Does the disaster recovery/ business resumption plan include provisions for people with special needs?
 - f) Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?
- 19)** Building, Utilities and Transportation
- a) 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?
 - b) 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.
 - c) Review any agreements for use of backup facilities.
 - d) Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
 - e) Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
 - f) Are building safety features regularly inspected and tested?
 - g) 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.
- 20)** Information Technology
- a) Determine if the plan reflects the current IT environment.
 - b) Determine if the plan includes prioritization of critical applications and systems.
 - c) Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
 - d) Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?
 - e) Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
 - f) 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.