

Chapter – 4

Business Continuity Planning and Disaster recovery planning

Business Continuity Management: Business Continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Key terms relating to BCM are:

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.

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 the business operations.

Advantage of Business Continuity The advantages of BCM are that the enterprise:

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

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. **Objectives of BCP**

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.

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

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.
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.

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

- A. Risk assessment,
- B. Determination of recovery alternatives,
- C. Recovery plan implementation, and
- D. Recovery plan validation.

Objectives of business continuity PLA:

- i. Minimize immediate damage and losses;
- ii. Continue critical business operations
- iii. Establish management succession and emergency powers
- iv. Facilitate effective co-ordination of recovery tasks
- v. Reduce the complexity of the recovery effort

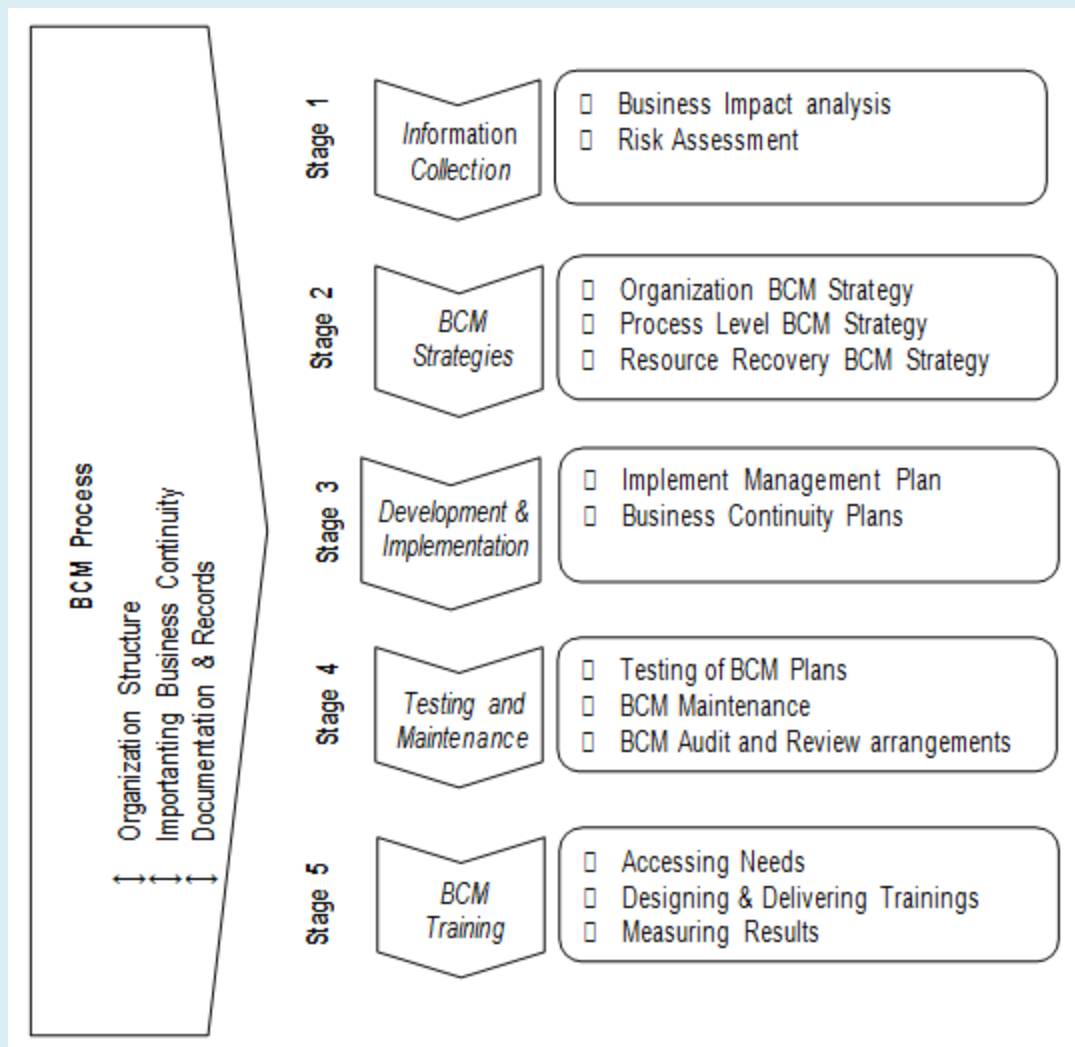
Goals of business continuity

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.

Developing a Business Continuity Plan: The methodology for developing a business continuity plan can be sub-divided into eight different phases:

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
9. Plan Implementation.

Components of BCM Process: Components of BCM Process are shown in the following diagram



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 :

1. organization structure with responsibilities and authority,
2. implementation and maintenance of business continuity management.
3. BCM documentation and records

BCM Information Collection Process: The pre-planning phase of Developing the BCP also involves collection of information. It enables the organization to define the scope of BCP and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan. Two other key deliverables of that phase are:

the development of a policy to support the recovery programs; and

an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

Business Impact Analysis: Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the For each activity

supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

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

BCM Strategy Process: Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications.

The enterprise develops and documents a series of plans, which enable them to effectively manage an incident, which impacts on site operations and subsequently recover its critical activities and their supporting resources, within the timescales agreed with the customer.

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. there should be a structure to enable the enterprise to:

- a. Confirm Impact of incident (nature and extent),
- b. Control of the situation,
- c. Contain the incident,
- d. Communicate with stakeholders, and coordinate appropriate response.

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.

The Business Continuity Plan (BCP)

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

The recovery strategies may be two-tiered:

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

BCM Testing and Maintenance Process: 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.

the objectives of performing BCP tests are to ensure that:

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

The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the enterprise's business continuity program; that 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.

Reviewing BCM Arrangements

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

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

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

Types of Plans: Various plans are as under:

- I. **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.
- II. **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.
- III. **Recovery Plan:** The backup plan is intended to restore operations quickly so that information system functions can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first.
- IV. **Test Plan:** The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to assure that the DR plan will work and 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.

Types of Back-ups: Various types of back-ups are given as follows:

- a. **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.
- b. **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.
- c. **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.
- d. **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:

- I. **Cold site:** If an organization can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a system—raised floors, air conditioning, power, communication lines, and so on.
- II. **Hot site:** If fast recovery is critical, an organization 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.
- III. **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.
- IV. **Reciprocal agreement:** Two or more organizations 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.

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. List of phone numbers of employees in the event of an emergency.
13. Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
14. Medical procedure to be followed in case of injury.
15. Back-up location contractual agreement, correspondences. Insurance papers and claim forms. Primary

computer centre hardware, software, peripheral equipment and software configuration.

16. Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.

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 were not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.

Sample list of BCP Audit steps are given below:

- (i) Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:
 - 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.
- (ii) Determine if information backup procedures are sufficient to allow for recovery of critical data.
- (iii) Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested.
- (iv) Determine if resources have been made available to maintain the disaster recovery/ business resumption plan and keep it current.
- (v) Obtain and review the existing disaster recovery/ business resumption plan.
- (vi) Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests
- (vii) Obtain and review the existing business impact analysis.
- (viii) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.
- (ix) Determine if copies of the plan are safeguarded by off-site storage.
- (x) Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?
- (xi) Gain an understanding of the methodology used to develop the existing business impact analysis.
- (xii) Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.

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

(xiv) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.

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

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

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

(xviii) Interview functional area managers or key employees to determine their understanding of the disaster recovery/ business resumption plan. Do they have a clear understanding of their role in working towards the resumption of normal operations?

- 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?

(xix) *Building, Utilities and Transportation*

- ☐ Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?

(xx) *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.

(xxi) *Administrative Procedures*

- a. Does the disaster recovery/ business resumption plan cover administrative and

management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time?

- b. Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
- c. Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.
- d. Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?
- e. To facilitate retrieval, are essential records separated from those that will not be needed immediately?

Mohd. Afroz