CHAPTER 4 : BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

BCP MANUAL

It 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

BCM POLICY

- It defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability
- Set-up activities incorporate the specification, end-to-end design, build, and implementation
- Ongoing maintenance and management activities include embedding business continuity within the enterprise, exercising plans, updating and communicating them.

OBJECTIVES

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,
3. Invocation of incident management and BCP.
4. Incident Management Plans & BCP 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.

Components of BCM Process

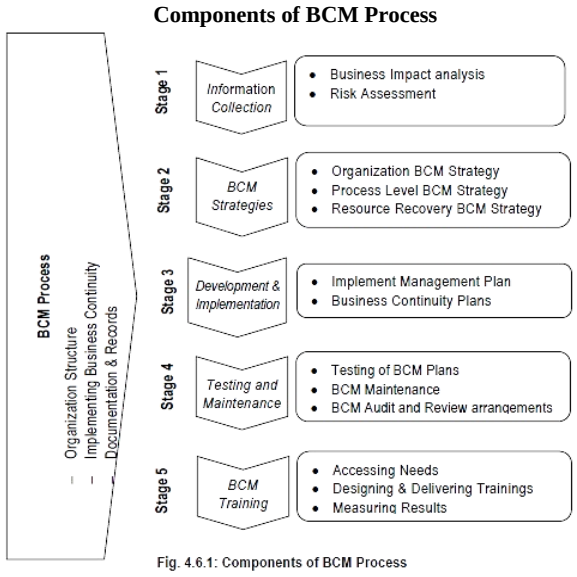

Fig. 4.6.1: Components of BCM Process

Reviewing BCM Arrangements (or) Audit / self-assessment of enterprise BCM program

1. All key products and services and their supporting critical activities & resources are included in BCM strategy
2. The enterprise BCM
- policy, strategies, framework & plans reflects its requirement
- competent & its capability are effective
- solutions are effective & up to date
- maintainence programs are effectively implemented

3. BCM strategies and plans incorporate improvements
4. BCM procedures are effectively communicated to staff
5. Enterprise has an ongoing program for BCM training
6. Change control processes are in place and operate effectively

Major documents that should be part of Business Continuity Management System

1. Business continuity Policy
2. Business continuity Strategies
3. Business continuity Plan
4. Business continuity Management plan
5. Business impact analysis report
6. Risk assessment report
7. Incident log
8. Training program
9. Exercise schedule and results

BUSINESS CONTINUITY PLANNING (BCP)

It is the creation and validation of a practical logistical plan for how an enterprise will recover & restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

OBJECTIVES & GOALS

1. Provide for the safety and well-being of people on the premises at the time of disaster
2. Establish management succession and emergency powers
3. Identify critical lines of business and supporting functions
4. Continue critical business operations
5. Minimize the duration of a serious disruption to operations and resources
6. Minimize immediate damage and losses
7. Facilitate effective co-ordination of recovery tasks
8. Reduce the complexity of the recovery effort
→Identify weakness & implement a disaster recovery program. (+5, 7, 8—goals)

METHODOLOGY OF DEVELOPING A BCP

1. Defining recovery requirements from the perspective of business functions
2. Defining how business continuity considerations must be integrated in to ongoing business planning & system development process
3. Developing a business continuity plan that is understandable, easy to use and maintain
4. Selecting business continuity teams that ensure the proper balance required for plan development
5. Documenting the impact of an extended loss to operations and key business functions
6. Obtaining commitment from appropriate management
7. Focusing appropriately on disaster prevention

8 PHASES OF BCP

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.

Phase 2 – Vulnerability Assessment and General Definition of Requirements:
This phase addresses measures to reduce probability of occurrence of disaster.

Phase 3 – Business Impact Assessment (BIA):

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. 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.

Phase 6 – Testing/Exercising Program:
Testing/ exercising goals are established and alternative testing strategies are evaluated.

Phase 7 – Maintenance Program:
It is critical that existing change management processes are revised to take recovery plan maintenance into account.

Key task performed in 'Vulnerability Assessment and General Definition of Requirement

1. A thorough Security Assessment of the computing and communications environment including personnel practices; physical security etc.
2. The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures
3. 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.
4. Define the scope of the planning effort.
5. Develop a Plan Framework
6. Assemble Project Team and conduct awareness sessions

BUSINESS IMPACT ANALYSIS (BIA)

- It 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.
- For each activity supporting the delivery of key products & services, the enterprise should:

1. Assess the impacts
2. Identify maximum time period for resumption
3. Identify critical business processes
4. Assess Minimum level of activity
5. Identify length of time
6. Identify any interdependent activities, assets etc.

- The enterprise should have documented approach to conduct BIA

Objectives of performing BCP tests in developing a BCP

1. The recovery procedures are complete and workable
2. The competence of personnel in their performance of recovery procedures can be Evaluated
3. The manual recovery procedures and IT backup systems are operational or restored.
4. Business processes, systems, personnel, facilities and data are obtained and perform recovery processes
5. The success or failure of the business continuity training program is monitored.

Maintenance tasks undertaken in the development of a BCP

1. Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
2. Determine the maintenance regime to ensure the plan remains up-to-date;
3. Determine the maintenance processes to update the plan
4. Implement version control procedures to ensure that the plan is maintained up-to-date
5. Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel & ensure that plan remains up-to-date

TYPES OF PLANS

EMERGENCY PLAN
It specifies the actions to be undertaken immediately when a disaster occurs. It identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack.

BACKUP LAN
It specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup.

RECOVERY PLAN
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.

TEST PLAN
To identify deficiencies in the emergency, backup / recovery plan

Alternate Processing Facility Arrangements

COLD SITE
If an organization can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system –raised floors, air conditioning, power, communication lines, and so on.

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.

WARM SITE
A warm site provides an interme diate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.

REIPROCAL AGREEMENT
Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster.

Considerations in contract of 3rd party site

1. How soon the site will be made available subsequent to a disaster
2. No of org. that will be allowed to use the site concurrently
3. The period during which the site can be used
4. The conditions under which the site can be used;
5. The facilities and services the site provider agrees to make available
6. The priority to be given to concurrent users

TYPES OF BACKUPS

FULL BACKUP
All files on disk / folder is backed up. At each backup run, all files designated in the backup job will be backed up again.
It is commonly used as an initial or first backup followed with subsequent incremental / differential backup.

Example
Suppose a full backup is done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not.

Advantages
►Restores are fast and easy to manage as the entire list is backed up
►Easy to maintain and restore different versions.

Disadvantages
►Backups can take very long as each file is backed up again ►Consumes the most storage space compared to incremental & differential backups.

INCREMENTAL BACKUP
An incremental backup captures files that were created or changed since the last backup, regardless the type of backup – Full / Incremental.

Example
Suppose an Incremental backup is done every night from Monday to Friday. This first backup on Monday will be a full back up as no prior backup is done.
However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup

Advantages
►Much faster backups.
►Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.

Disadvantages
►Restores are slower than with a full back-up and differential backups
►Restores are a little more complicated. All backup sets (first full backup and all Incremental backups) are needed to perform a restore.

DIFFERENTIAL BACKUP
Differential backups fall in the middle between full backup & incremental backup.
With differential backups, one full backup is done first & subsequent backup runs are the changes made since the last full backup.

Example
A differential backup is done every night from Monday to Friday. On Monday a full back will be first done since no prior backups. On Tuesday, the differential backup will only backup the files that have changed since Monday & any new files added to the backup folders. On Wednesday, the files changed & files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on tuesday.

Advantages
►Much faster backups than full backups.
►More efficient use of storage space than full backups
►Faster restores than incremental backups

Disadvantages
►Backups are slower than incremental backups.
►Not efficient as storage as compared to incremental backups.
►Restores are slower than with full backups.

DISASTER RECOVERY PROCEDURAL PLAN

- Emergency procedures
- Fall-back procedure
- Resumption procedure
- Maintenance schedule
- List of phone no of employees in even of emergency
- Responsibility of individual for executing the plan
- Awareness Activities
- Medical procedure
- Insurance paper
- Backup location
- Emergency phone list is for hardware, software, fire etc.
- Details of airline, hotels & transport arrangement

AUDIT OF BCP / DRP

Building, Utilities and Transportation

1. Does the Disaster recovery / Business Resumption plan
- has provision to inspect the building & facilities soon after a disaster, identify damages & repair the premises for safe return of employees
- consider the need for alternative shelter
- consider the failure of electrical power, natural gas, toxic chemical containers, and pipes
- consider the disruption of transportation systems as it could affect the ability of employees to report to work or return home

2. Review any agreements for use of backup facilities
3. Verify that the backup facilities are adequate based on projected needs
4. Are building safety features regularly inspected and tested?

AUDIT OF BCP / DRP

Administrative Procedures

1. Determine if the Disaster recovery / Business Resumption plan
- cover administrative and management aspects
- covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.

2. Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
3. Have essential records been identified? Whether duplicate set of essential records stored in a secure location?
4. To facilitate retrieval, are essential records separated from those that will not be needed immediately?

AUDIT OF BCP / DRP

Information Technology

1. Determine if the Disaster recovery / Business Resumption plan
- reflects the current IT environment
- includes prioritization of critical applications and systems
- includes time requirements for recovery
- include arrangements for emergency telecommunications

2. In case of interruption, is there alternate means of data transmission?
3. Verify that the backup facilities are adequate based on projected needs
4. Determine whether testing schedule exists and is adequate