

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING.

Business continuity means maintaining the uninterrupted availability of all key business resources to support essential business activities.

DEFINITIONS :-

BUSINESS CONTINUITY :- An event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions.

→ If event is very destructive, it's often called a disaster.

BCP Process

:- 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

megzway

* may be invoked in whole / part and at any stage of the response to incident under BCM D and IP, they may be termed :-

(1) Business :- logistics, HR, etc

(2) Technical :- IT.

Date :

Page No.

critical operations.

- Ensure that the vital business functions (critical business operations) are recovered and operationalised within an acceptable timeframe.
- Ensure continuity of business and not necessarily the continuity of all systems, computers or networks.
- Identify the critical functions of the enterprise and the resources required to support them.

*

BC Planning (BCP) :- The ability of enterprises to recover from a disaster and continue operations with

creation and validation least impact.

of a practical
logistical plan

→ Imperative that whether profit oriented or service oriented enterprises have this plan.

recovery & restoration

→ There should be an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the enterprise.

partially or
completely

interrupted critical functions → within predetermined time

after a disaster or extended
disruption.

Areas covered by Business Continuity :-

1. Business Resumption Planning : This is the operational phase of BCP.
2. Disaster recovery Planning : This is the technological aspect of BCP.
3. Crisis management : This is the overall co-ordination of an organisations response to a crisis in an effective timely manner, with goal of avoiding or minimising damage to the organisations profitability, reputation or ability to operate.

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.

- * BCP is expected to provide :-

megzway

Reasonable assurance to senior management of enterprise about the capability of enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.

Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring "continuous availability of all key services/clients".

- * BCP manual is expected to specify the responsibilities of the BCM team whose mission is to establish appropriate BCP procedure to ensure the continuity of enterprise's critical business function.



In the event of an incident or disaster affecting any of the functional areas, BCM team serves as a liaising team between the functional areas affected and other departments providing support services.

BCM

→ Business owned, business - driven process that established a fit-for-purpose strategic and operational framework.

Proactively improve 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 product and services to an agreed level within an agreed time after a disruption.

Delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

Scope of Business Continuity → Defined by Top Management

Defined by identifying the key products & services that support the enterprise's obj, goals & statutory duties in line with the threat scenario and business impact analysis

In case of outsourced service/activity, risk accountability remains with the enterprise and necessary controls and process should be in place to manage the risk from an outsourced service.

megzway

Advantages of Business

Continuity

#

1

Enterprise is able to proactively assess the threat scenario and potential risks.

#

2

Enterprise has planned response to disruptions which can contain the damage and minimise the impact on the enterprise.

3

#

Enterprise is able to demonstrate a response through a process of regular testing and trainings.

- * Planning and management responsibility are assigned to a member of the relevant senior management team.

Date :

Page No.

BCM Policy

- * main objective of it is "to minimize/eliminate" the loss to an enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction.

- * It is a high level document, which shall be the guide to make a systematic approach for disaster recovery.

- * 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.

- * The set-up activities incorporate the specification, end to end design build, implementation and initial exercising of the Business continuity capability.

- * Points to be considered when developing the BCM policy.

(1) Defining the scope.

(2) BCM principles, guidelines and minimum standards for the enterprise.

(3) Relevant standards, regulations or policies that have to be included or can be used as a benchmark.

- * 15 Objective 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.

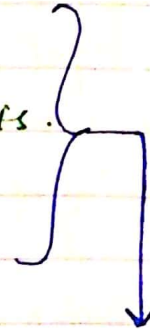
→ Innovation of incident management and business continuity plans can be managed.

→ Incident management & BC plans are subject to ongoing testing, revision and updation as required.

BUSINESS CONTINUITY LIFE CYCLE

4 Broad and sequential sections :-

1. RISK ASSESSMENT.
2. DETERMINATION OF RECOVERY ALTERNATIVES.
3. RECOVERY PLAN IMPLEMENTATION.
4. RECOVERY PLAN VALIDATION.



within each of these lifecycle sections, the applicable resource

- sets are manipulated to provide
- | | | |
|--------------------------|---------|--|
| (i) Information | ← — — — | Resources are manipulated to provide |
| (ii) Technology | | Resources are manipulated to provide the best mix. |
| (iii) People | | be broken or critical resource quantities |
| (iv) Process | | down into at optimum costs with minimum |
| (v) facilities. | | the following. Irrecoverable and recoverable losses. |
| (vi) Telecomm-unication. | | components |

megzway

BUSINESS CONTINUITY PLANNING

megzway

OBJECTIVES.

- Provide the safety and well being of people on the premises at the time of disaster
- Continue critical business operations
- Minimise the duration of a serious disruption to operations and resources
- Minimise immediate damages and losses.
- Establish management succession and emergency powers.

GOALS.

- Identify weaknesses and implement a disaster prevention program.
- Minimise the duration of a serious disruption to business operations.
- Facilitate effective co-ordination of recovery work.
- Reduce the complexity of recovery effort.

METHODOLOGY OF DEVELOPING A BUSINESS CONTINUITY PLAN.

megzway

EMPHASISES:-

- 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 of operations on key business functions.
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery.

PHASES :-

PHASE I :

PRE - PLANNING ACTIVITIES (PROJECT INITIATION)

This phase is used to obtain an understanding of the existing and projected computing environment of the organization.



Enables the project team to :-

- Define the scope of the project and associated work program.
- Develop project schedules and
- Identify and address any issues that could have an impact on the delivery and the success of the project.



During this phase, a steering committee should be established, it should have overall responsibility for providing direction and guidance to the project team, to make all decisions related to the recovery planning effort.



Project manager should work with steering committee in finalizing the detailed work plan and developing intervention schedules for conducting the security assessment and the Business Impact Analysis.



2 other key deliverables of this phase are :-

1. development of a policy to support the recovery programs, and
2. 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.



Concentrates on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster from an economic and business strategy perspective. rather than concentrating on minimizing impact of an actual disaster.



This phase addresses measures to reduce the probability of occurrence.



Key tasks included are as follows :-

- (1) A thorough Security Assessment of the computing and communications environment including personal practices ; physical security etc.
- (2) 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.
- (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 scope of the planning effort.
- (5) Analyse, recommend development of plans.
- (6) Assemble project team and conduct awareness sessions.

megzway

PHASE 3:

BUSINESS IMPACT ASSESSMENT (BIA)

BIA of all business units that are part of the business environment enables the project team to :-

- (1) Identify critical systems, processes and functions.
- (2) Assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
- (3) assess the "pain threshold" that is, the length of time business units can survive without access to systems, services and facilities.



BIA Report should be presented to steering committee



Used as basis for identifying systems and resources required to support the critical services.

PHASE 4:

DETAILED DEFINITION OR 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.



It should include hardware, software, documentation, 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

Recovery plans components are defined and plans are documented



Includes the implementation of changes to user procedures, vendor contract negotiations and definition of recovery teams, their roles and responsibilities



Recovery standards are also developed during this phase

megzway

PHASE 6 :

TESTING / EXECUTION PROGRAM

Plan for testing / executing program is developed during this phase.



Testing / executing goals are established and alternate testing strategies are evaluated



Strategies tailored to the environment should be selected and an ongoing testing program should be established.

PHASE 7 :

MAINTENANCE PROGRAM

Maintenance of the plans is critical to the success of an actual recovery



Plans must reflect changes to the environments that are supported by the plans.



Existing management processes for change are revised to take recovery plan maintenance into account, where such change management does not exist, they will be recommended and implemented

PHASE 8 :

INITIAL PLAN TESTING AND IMPLEMENTATION

once plans are developed, initial tests of the plans are conducted and necessary modifications to the plans are made based on an analysis of the test results



specific activities of this phase include .

- (i) Defining the test purpose / approach
- (ii) Identifying test teams
- (iii) Structuring the test
- (iv) Conducting the test
- (v) Analyzing test results
- (vi) modifying the plans as appropriate.



Approach Taken to test the plans depends in large part on the recovery strategies selected to meet the recovery requirements of the organization.



Recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

Date :
Page No.

BUSINESS CONTINUITY MANAGEMENT PROCESS.

megzway

1. ORGANIZATION STRUCTURE :-

The organization should nominate a person or a team with appropriate seniority and authority to be accountable for BCP policy implementation and maintenance.

2. IMPLEMENTING BUSINESS CONTINUITY IN THE ENTERPRISE AND MAINTENANCE :-

In establishing and implementing the BCP system in the organization, managers from each function on site represent their areas of the operation. These people are also responsible for ongoing operation and maintenance of the system within their area of responsibility.



Top management should appoint (BCP) manager role as being the role that is responsible for the BCP policy and its implementation.



Resource planning manager is supported by the shift leaders and Team captains from each function, who are responsible for ongoing

Implementation and maintenance of the BCM.



The programs should be communicated to all the Stakeholders with appropriate training and testing.



Enterprise may adopt any project management model for effective output.



major activities for implementation :-

- defining the scope and context.
- defining roles and responsibilities.
- Engaging and involving all stakeholders.
- Testing of programs on regular basis.
- managing costs and benefits associated, and
- 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.



Documents (representatively) are part of BCM system:-

1. BC Policy
2. BC management system.
3. BIA Report.
4. RA Report
5. Aims and objectives of each function.
6. Incident log.
7. Training programs.

↓
to provide evidence of the effective operation of the BSM.

↓
Such documents/records should be retained for min 1 year
in line with enterprise policy

↓
the nature of the record means that the retention is a statutory,
regulatory or customer requirement, it will be retained for
the amount of time dictated.

↓
These records include reference to all business interruptions
and incidents, irrespective of the nature and length of disruption.

Stage 1:

BCM ICP (Information collection process)

The pre planning phase of developing the BCP also involves *

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:

- Enterprises objectives, stakeholders obligations, statutory duties and the environment in which the enterprise operates;
- Activity, assets and resources, including those outside the enterprise that support the delivery of these products and services;
- Impact and consequences over time of the failure of 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.



Enables us to refine the scope of BCP and the associated risk program; develop schedules; and identify and address issues that could have an impact on delivery and the success of the plan.



2 key deliverables of it are :-

- (1) Development of a policy to support the recovery programme.

megzway

- (11) Awareness program to educate management and senior individuals who will be required to participate in BCP program.

BIA & RA are signed off by top management as representation of operation which is accurate and relevant to the needs of the operation and its stakeholders.

megzway

→ BIA

A means of systematically assessing the potential impacts resulting from various events or incidents

- 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.



Enterprise should have a documented approach to conduct BIA.



Presented by top management in form of report	it identifies critical service functions and the time frame in which they must be recovered after interruption.
--	---

Classification Of Critical Activities

megzway

BCP leader and BCP team leaders in consultation with respective function owners shall carry out BIA for infrastructure and business functions



BIA will result in categorization of infrastructure

- (i) vital
- (ii) desirable
- (iii) essential.

2.

Business function after a disaster

- (i) catastrophic
- (ii) major
- (iii) minor/ trivial.

for various causes

- (i) fire
- (ii) flood
- (iii) system failure.

1. BUSINESS CATEGORIZATION (VITAL/ESSENTIAL/DESIRABLE):

The parameters considered in deciding whether a function/service is vital/essential/desirable are:-

- (1) Loss of Revenue.
- (2) Loss of reputation.
- (3) ↓ in customer satisfaction; and
- (4) Loss of productivity (man-hours).



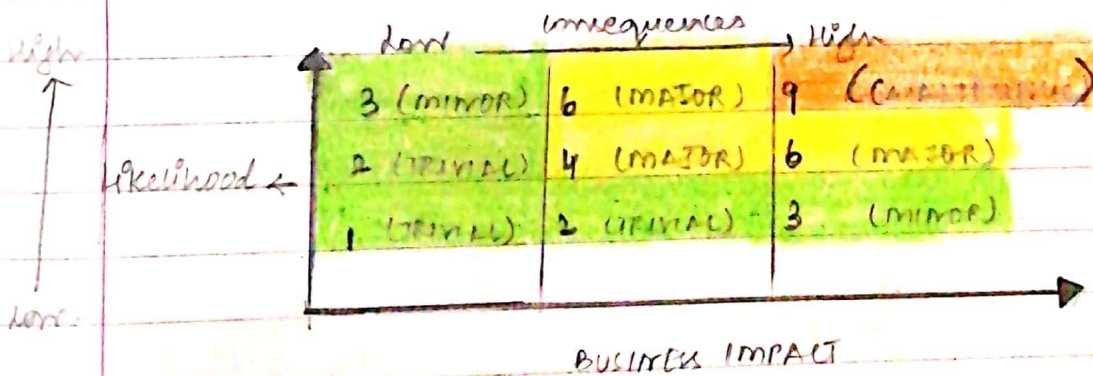
leading three-point scale 1-3 where, of these above parameters

1 = Low (L)

2 = medium (M)

3 = High (H)

2. DISASTER SCENARIOS (MAJOR/MINOR/TRIVIAL/CATASTROPHIC):



Low & very low

medium

High

(It is used to assess risk and

is thus also referred as RA matrix)

Likelihood: the probability of a risk or the occurrence of the disaster

consequences: the severity of the impact or the extent of damage caused by the risk.

Based on likelihood of the occurrence of risks, the risks can be classified under one of the following, categories

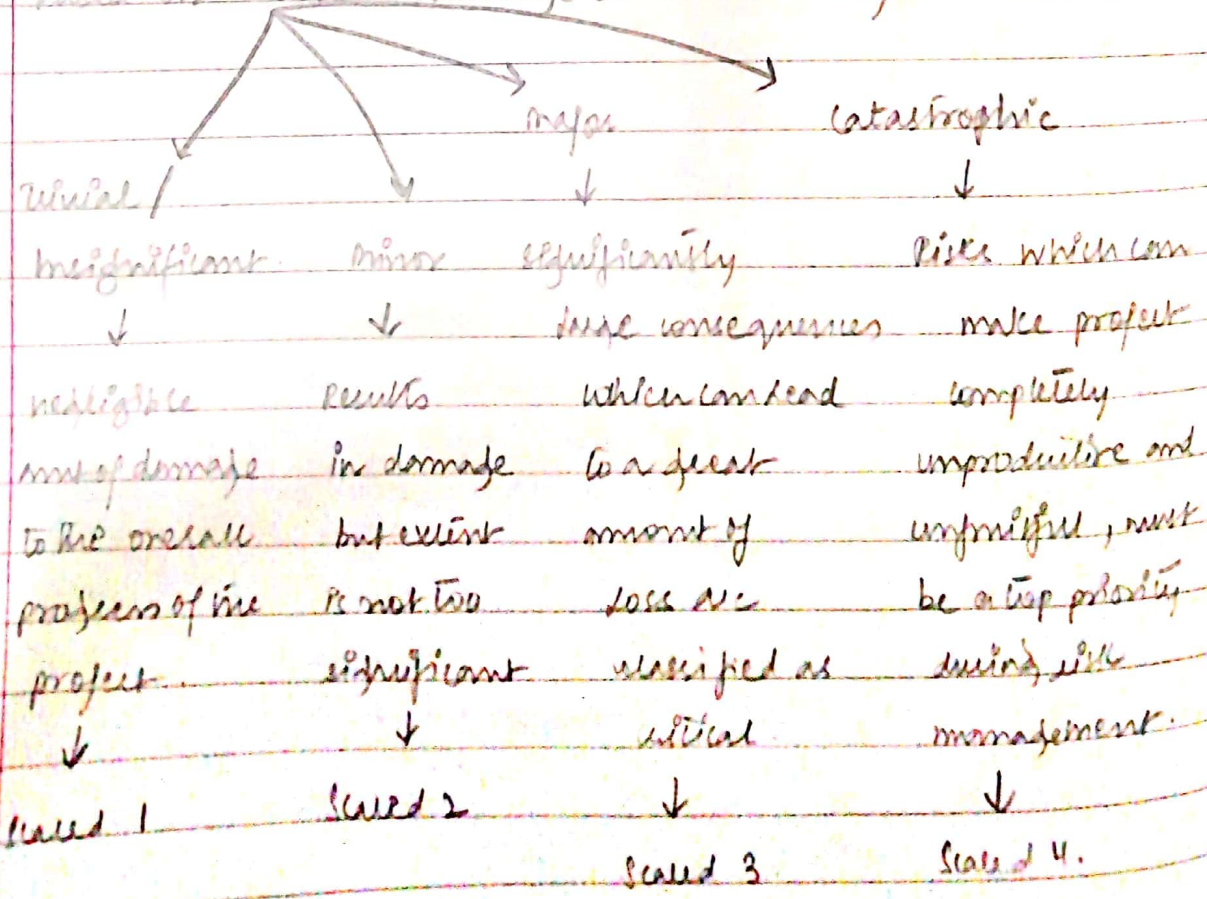


definite (rated 3)	likely (rated 2)	unlikely (rated 1)
↓	↓	↓
>80%	60-80%	<10%
↓		↓
almost certain to show-up during project execution		rare and exceptional

megzway

consequences:-

Based on lesser the damage can be caused by risk



RISK ASSESSMENT

It's assessment of the disruption to critical activities, which are supported by resources such as people, process, technology, info, infra, supplies and stakeholders



Enterprise should determine the threats and vulnerabilities of each resource and the impact.



ENTERPRISE decision to select a risk assessment approach, but it is imp. 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 etc.



vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats.



The security assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist. This is similar to vulnerability assessment phase of developing a BCP.



Impacts might result from the exploitation of vulnerabilities by threats. As a result of 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.



the enterprise might include one or more of all of the strategies for each critical activity.

megzway

BCM Strategy Process.

much preparation is needed to implement the strategies for protecting critical functions and their supporting resources.

ex - Establish procedures for backing up files and applications.

or, purchase of equipment, especially to support a redundant capability.



Enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and/or reduce the potential impact of those incidents and resilience and mitigation measures for both critical and non critical activities.

BCM Dip

(BCM Development and Implementation process)

The enterprise should have an exclusive organisation structure, Incident management Team/ Crisis Management for an effective response and recovery from disruptions.

In the event of any incident, there should be a structure to enable the enterprise to :-

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

megzway

1. imp

(The Incident management Plan)

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; provide the basis for managing all possible issues; including the stakeholder and external issues, facing the enterprise during an incident.

2. BCP

(at least earlier)

BCMTBMP

BCM testing & maintenance process.

"1" BCM T (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.



BCM testing should be consistent with the scope of the BCP(s) giving due regard to any relevant legislation and regulation.



Testing may be based on a predetermined outcome or allow the enterprise to develop innovative solutions



The BCP testing programme should include testing of the technical, logistical, administrative, procedural and other operational systems.



It will lead to improvement of BCM plans by :-

1. Practising the enterprise's ability to recover from an incident
2. Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities

megzway

3. Highlighting assumptions, which need to be questioned.
4. Instilling confidence amongst exercise participants.
5. Raising awareness of business continuity throughout the enterprise by publicizing the exercise.



upon

Frequency of testing should depend upon the enterprise's needs, environment in which it operates and stakeholder requirements.



Testing programme should be flexible, taking into account the rate of change within the enterprise and the outcome of previous one.



Objectives of performing BCP tests are to ensure that :-

- (i) Recovery procedures are complete and workable.
- (ii) Competence of personnel in their performance of recovery procedures can be evaluated.
- (iii) Sources such as business processes, systems are obtainable, and operation to perform recovery processes.
- (iv) Manual recovery procedures and IT Backup systems are current and can either be operational or restored.
- (v) Success or failure of the Business continuity training programme is monitored.

megzway

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.

Approach taken to test the plans depends largely on recovery strategies selected to meet recovery requirements of the organisation.

"2" BCM M.

- Demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program (1) the key people who are to implement the BCM strategy (2) the key people are trained and competent (3) monitoring and control of BCM risks faced by the enterprise (4) monitoring and control of BCM risks faced by the enterprise (5) Evidence that material changes to the enterprise's structure, products & services etc have been incorporated into the enterprise's business continuity and incident management plans.

Maintenance tasks undertaken in development of BCP are to :-

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

- Identify the BCP maintenance triggers to ensure that any organisational, operational and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date.
- Determine the maintenance regime to ensure the plan remains up-to-date.
- Determine the maintenance processes to update the plan, and
- Implement control procedures to ensure that the plan is maintained up-to-date.

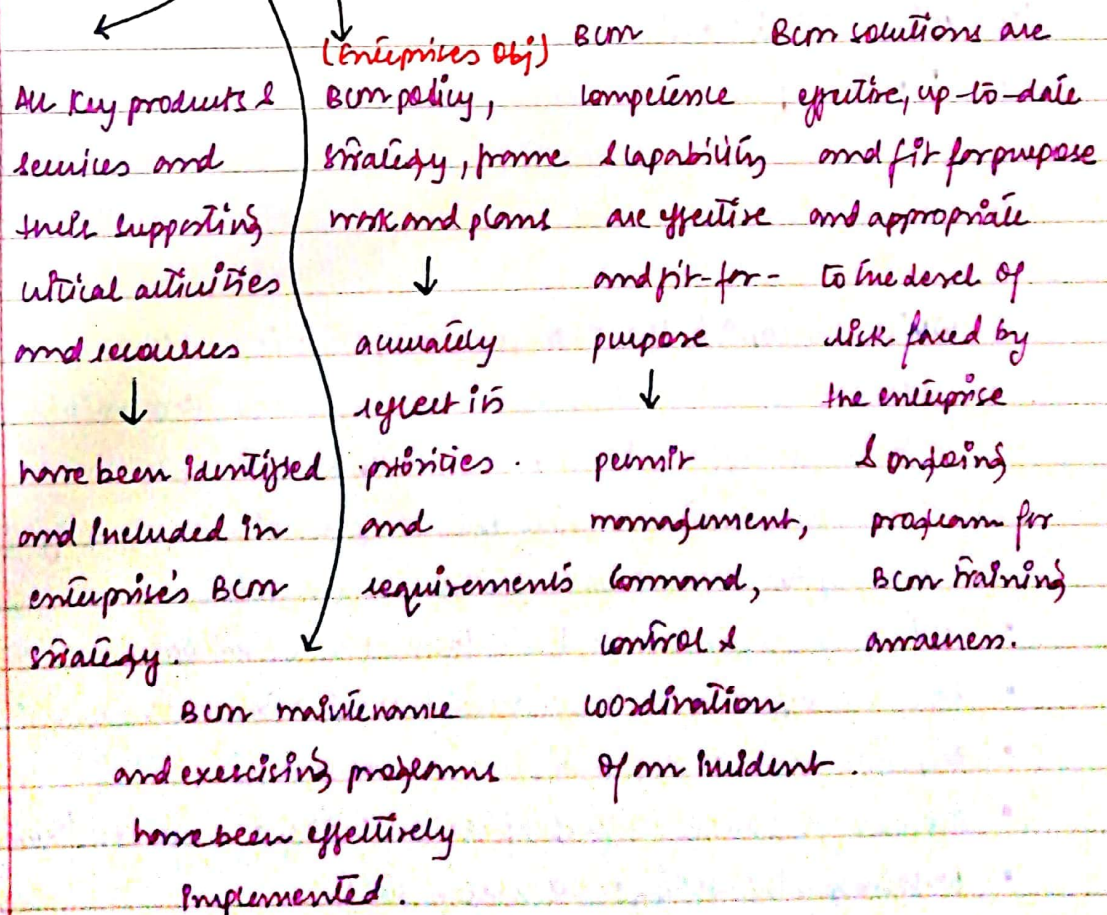
"3"

RBCM

(Reviewing BCP arrangements)

megzway

An Auditor self assessment of the enterprise's BCP programme should verify that :



BCM TRAINING PROCESS :-

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

- developing a BCM program more efficiently.
- providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions.
- increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels; and
- minimizing the likelihood and impacts of disruptions.

Development of a BCM culture is supported by :-

- (i) Leadership from senior personnel in the enterprise.
- (ii) Assignment of responsibilities.
- (iii) Awareness raising.
- (iv) Skills training; and
- (v) Exercising plans.

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 org. 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.
- Promotes a positive culture of health, safety and the environment.
- Encourages the taking of calculated risks.

Types of Back-up:

When the backups are taken of the system and data together, they are called total system back-up.

FULL BACKUP.

- captures all files on the disk or within the folder selected for backup
- In FB system, every backup generation contains every file in the backup set.
- At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed. (Monday backup kiya, phir Tuesday kiya, tou joun pehle hi ho gaya woh backup Tuesday wala with new ones, wohin previous folder have not changed or not).
- It is initial or first backup followed with subsequent incremental or differential backup, it is common to start fresh backup after several incremental or differential backup.
- also done for all backups already runned for smaller folders or projects that do not occupy too much storage space.



INCREMENTAL BACKUP.

- megzway
- captures files that were created or changed since last backup, regardless of backup types.

It can be full backup or simply last incremental backup.

- One full backup is done first and subsequent backups runs are just the changed files and new files added since last backup.

(Monday backup full)
Tuesday only backup files that have changed since Monday,
Wednesday

backup will be changed files & new ones since Tuesday



DIFFERENTIAL BACKUP.

- Falls in the middle between full backups and incremental backup

- stores files that have changed since the last full backup.

- One full backup is done first and subsequent backup runs are the changes made since the last full backup.

- Two step operation:

(i) Restoring from the last full backup and

(ii) then restoring the appropriate differential backup.

MIRROR BACKUP.

- As name suggest, A mirror of the source being backed up
- When file in the source is deleted, that file is eventually also deleted in the mirror backup
- That is way it should be used with caution as a file that is deleted by accident, sabotage or enough virus may also cause that same file in mirror to be deleted as well
- Some may not consider it even a backup.
- Identical to full backup, with exception that the files are not zipped and not password protected
- Used to create exact copy of backup data.

STATEMENT SHOWING INDIVIDUAL ADVANTAGES & DISADVANTAGES OF BACK UPS.

TYPE OF BACKUPS	ADVANTAGE	DISADVANTAGE
FULL BACKUPS	→ Restores are fast and easy to manage as the entire list of files and folders are in one backup set.	→ Take very long as each file is backup again every time the full backup is run.
	→ Easy to maintain and restore different versions.	→ consumes the most storage space compared to incremental & differential backups
INCREMENTAL BACKUP	→ much faster backups	→ Restores are slower than with full backup and differential backup.
	→ Efficient use of storage space as files are not duplicated.	→ Restores are less complicated
	→ Less storage space used comparing to running full backups and even differential backups.	→ All backup sets are needed to perform a restore.
DIFFERENTIAL BACKUP.	→ much faster backups than full backups.	→ slower backups in comparison to incremental backups.
	→ more efficient use of storage space than full backups.	→ not as efficient use of storage space as compared to incremental backups
	→ faster restore than incremental backups.	→ All files added or edited after the initial full backup will be duplicated again with each subsequent Diff. Backup.

megzway

→ Restores are slower than with full backups.

→ more complicated than full backups but simpler than incremental backups.

only the full backup set and last differential backup are needed to perform a restore.

MIRROR BACKUPS.

→ Backup is clean and does not contain old and obsolete files.

→ there is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.

ALTERNATE PROCESSING FACILITY

ARRANGEMENTS :-

Security Administrators should consider the following backup options.

(C) L P
(C) L
(C) L
(C) L
(C) L
(C) L
(C) L
(C) L

→ If an organisation can tolerate some downtime, cold site backup might be appropriate.
 → If fast recovery is critical, an org might need hot site backup.
 → provides an intermediate level of backup
 → 2 or 3 orgs might agree to provide backup facilities to each other in the event of

→ Has all the facilities needed to install a mainframe system - raised floor, AC, power etc.
 → All hardware and software and operation facilities will be available at the hot site.
 → It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.
 one suffering disaster
 → Relatively cheap backup option but each party must maintain sufficient capacity to operate another critical system

→ Can establish its own cold-site facility or enter into an agreement with another org to provide a cold site facility.
 → In some cases, software, data & supplies might also be stored there.
 → Expensive to maintain
 → Usually shared with other orgs that hot-site needs.

megzway

**

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.
- no. of organisations that will be allowed to use the site concurrently in the event of a disaster.
- the priority to be given to constituent users of the site in the event of a common disaster.
- the period during which the site can be used
- conditions
- facilities and services.
- what controls will be in place and working at the off-site facility

These issues are often poorly specified in it, they can be difficult to enforce under a RA because of the informal nature of the agreement.

megzway

DISASTER RECOVERY PROCEDURAL

PLAN :

conditions for activating the plans, which describe the process to be followed before each plan, are activated

Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life.

Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time scale.

Resumption procedure which describe the actions to be taken to return to normal business operations.

Contingency plan document distribution list

detailed description of the purpose and scope of the plan.

List of phone no. of employees in the event of an emergency.

Emergency phone list for fire, police etc

medical procedure to be followed in case of injury.

Insurance papers and claim forms.

megzway

AUDIT OF THE BCP/DRP

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.

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) plan is based upon a BIA that considers the impact of the loss of essential functions.
 - (c) Operations managers and key employees participated in the development of the plan.
 - (d) Plan identifies the resources that will likely be needed for recovery and the location of their availability.
 - (e) Plan is simple and easily understood so that it will be effective when it is needed.
 - (f) Plan is realistic in its assumptions.
- (ii) Determine if info 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.

TYPES OF PLANS.

1. Emergency Plan :-

The plan specifies the actions to be undertaken immediately when a disaster occurs.



Management must identify those situations that require the plan to be invoked.



Actions to be initiated can vary depending on the nature of the disaster that occurs.



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



When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated

Plan must show who is to be notified immediately when the disaster occurs	Actions to be undertaken	Any evacuation procedures required must be specified	Return procedures (conditions that must be met before the site is considered safe) must be designated
---	--------------------------	--	---

Moreover, the personnel responsible for the actions must be identified and protocols to be followed must be specified clearly.

megzway

2. BACK-UP 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 restoring various systems and a time frame for recovery of each system

Procedures → might be straightforward
→ could be complex and somewhat uncertain.

Plan needs continuous updating as changes occur

3. RECOVERY PLAN.

Procedures to restore full IS capabilities (Backup plan is intended to restore operations quickly so that IS functions can continue to serve an organization)

RP should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken

should specify the responsibilities of the committee and provide guidelines on priorities to be followed.

Applications are to be recovered first.

members of recovery committee must understand their responsibilities.

↓
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.

TEST PLAN:-

Final component of a disaster recovery plan is a test plan.

↓
Identifies deficiencies in the emergency, backup or recovery plans or in the preparedness of an organization and its personnel for facing a disaster.

↓
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, these plans must be tested, to facilitate testing, a phased approach can be adopted.

1stly.
Disaster recovery plan can be tested by desk checking and inspection and walk-throughs.

2ndly.
Disaster can be simulated at a convenient time.

↓
Finally, disasters could be simulated without warning at any time. These are the acid test of the organizations ability to recover from a catastrophe.