

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

BCM Policy and its objectives

The main objective of BCP is to minimise/eliminate the loss to enterprises business in terms of

- Revenue Loss
- Loss of reputation
- Loss of Productivity
- Customer satisfaction

This policy document is a high level document which shall be the guide to make a systematic approach for disaster recovery, to bring awareness in people about the business continuity aspects and its importance

Objective of the policy is to provide a structure through which

- Critical services and activities undertaken for the customer is identified
- Plans will be developed to ensure continuity of key service delivery following disruption
- Invocation of incident management plans and BCP can be managed
- Incident Management Plan and BCP are subject to on-going testing, revision and updation as required
- Planning and Management responsibility are assigned to member of senior management team

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 functions within a pre-determined time after a disaster or extended disruption
- Components of BCP are
 - Business Resumption Planning
 - Disaster Recovery Planning
 - Crisis Management
- Objectives and Goals of BCP
 - Primary objective is to minimise the loss by minimising the cost associated with the disruptions and enable an organisation to survive a disaster
 - Key objectives of contingency plan should be
 - Provision for safety and well-being of people on the premises
 - Continue critical business operations
 - Minimise the duration of serious disruption to operations
 - Minimise immediate damage and losses
 - Establish management succession and emergency powers
 - Facilitate coordination of recovery tasks
 - Main Goals of BCP
 - Identify weakness and implement a disaster prevention program
 - Minimise the duration of serious disruption to business operations
 - Facilitate effective coordination of recovery tasks
 - Reduce the complexity of recovery effort

Developing a Business Continuity Plan

- Methodology for developing a BCP can be divided into eight phases. Extent of applicability to be tailored to respective organisation. Methodology to emphasise on the following
 - Providing Management with the understanding of efforts required
 - Obtaining commitment from top management
 - Define recovery requirements from business functions perspective
 - Documenting the impact of an extended loss to operations and key business functions
 - Selecting business continuity teams to ensure proper balance
 - Developing a business continuity plan –easily understandable, easy to use and maintain
- Eight Phases of BCP are as follows
 - Pre-Planning Activities
 - Vulnerability Assessment and Definition of Requirements
 - Business Impact analysis
 - Detailed Definition of Requirements
 - Plan Development
 - Testing Program
 - Maintenance Program
 - Initial Plan Testing and Plan Implementation

Phases of BCP

- Pre Planning Activities
 - Understanding of the existing and projected computing environment of the organisation
 - A steering committee to be established
 - Development of a policy to support the recovery programs
 - Awareness program to educate management and senior individuals who will be required to participate in the project
- Vulnerability Assessment and Definition of Requirements
 - Security assessment to be conducted]
 - Security assessment will enable the project team to improve any existing emergency plan and disaster prevention measures
 - Identify vulnerabilities
 - Present findings and recommendations resulting from the security assessment to the steering committee
 - Define scope of the planning effort
 - Develop a plan framework
 - Assemble project team and conduct awareness sessions
- Business Impact Assessment
 - Identify critical systems. Processes and functions

- Assess the economic impacts of incidents and disasters resulting in denial of access to systems services
 - Assess the length of time business units can survive without the use of information systems
- Detailed definition of requirements
 - A profile of recovery requirements is developed
 - Profile developed by identifying the resources required to support critical functions identified in Business Impact Analysis phase
 - Recoveries to be based on short term, intermediate term and long term outages
- Plan Development
 - Recovery plan components are defined and plans are documented
 - Also includes implementation of changes to user procedures
- Testing/Exercising Program
 - Testing/Exercising program is developed during this phase
 - Testing/exercising goals are established and alternative testing strategies are evaluated
- Maintenance Program
 - Maintenance of plans is critical
 - Plans must reflect the changes to environment supported by plans
- Initial plan Testing and Implementation
 - Once plans are developed, initial test of the plans are conducted and necessary modifications to the plans are made based on the test results

Components of BCM Process

Stage 1:- Information Collection

Stage 2:- BCM Strategies

Stage 3:- Development and Implementation

Stage 4:-Testing and Maintenance

Stage 5:- BCM Training

Information Collection

- Business Impact Analysis
- Classification of critical activities
 - Business Categorisation- Vital/Essential/Desirable
 - Disaster Scenarios-Major/Minor/ Trivial/Catastrophic
- Risk Assessment

Prioritisation of the enterprise products and services and urgency of activities to deliver them

BCM Strategies

Assessment of strategies and finalising them

BCM-Development and Implementation

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

BCM-Testing and Maintenance

Testify the enterprise BCM to prove extent to which the strategies and plans are complete

BCM-Training Process

Extensive training in BCM , incident, Business continuity and recovery and restoration plans enable the same to become a part of the enterprise core values

Business Continuity Management Process

BCM processes are mapped as follows:-

- Organisation Structure:-
 - Nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance
- Implementing Business continuity in the Enterprise and Maintenance
 - In establishing and maintaining BCM, managers from each function on site represent their areas of the operation and handle the operation and maintenance of system within area of responsibility
 - Major activities to be carried out on implementation are
 - Defining scope and context
 - Defining roles and responsibilities
 - Engage and involve all stakeholders
 - Testing of Program on regular basis
 - Maintaining currency and appropriateness of business continuity plan
 - Convert policies and strategies into action
- BCM Documentation and Records
 - Following documents are classified as being part of Business Continuity Management System
 - Business Continuity Policy
 - Business Continuity Management System
 - Business Impact Analysis Report
 - Risk Assessment Report
 - Aim and objectives of each function
 - Activities undertaken by each function
 - Business Continuity Strategies
 - Incident Log
 - Training Program

BCM Information Collection Process

In order to design an effective BCM, it is pertinent to understand the following facts of the enterprise

- Enterprise objectives, stakeholder expectations
- Activities, assets and resources
- Impact and consequences over time of failure of these activities
- Perceived threats which could disrupt the enterprise's key products and services

BUSINESS IMPACT ANALYSIS

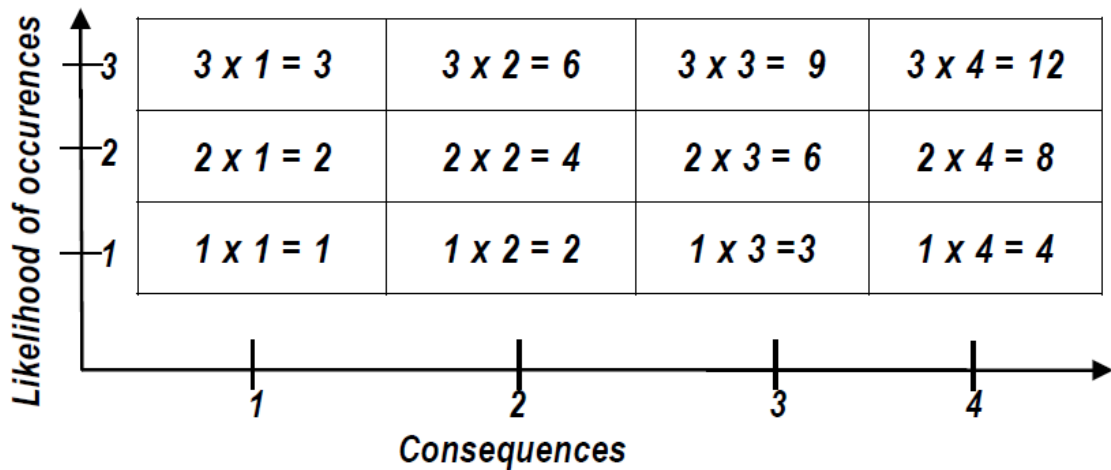
- Essentially a means of systematically assessing the potential impacts resulting from various events or incidents
- For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should
 - Assess impacts-if activity was disrupted over a period of time
 - Identify maximum time period after start of disruption within which activity is to be resumed
 - Identify critical business processes
 - Assess minimum level at which activity needs to be performed on its resumption
 - Identify the length of time within which normal levels of operation needs to be resumed
 - Identify inter-dependent activities, assets, supporting infrastructure or resources that have to be maintained continuously or recovered over time

Classification of Critical Activities

- BIA will result in the categorisation of
 - Infrastructure and business function- Vital/Desirable/Essential
 - Disaster Scenarios- Catastrophic, Major, Minor
- Business Categorisation (Vital/Essential/Desirable)- Parameters to be considered are
 - Loss of Revenue
 - Loss of Reputation
 - Decrease in Customer satisfaction
 - Loss of Productivity
- Disaster Scenarios (Major/Minor/Trivial/Catastrophic)

Scenario of disaster shall be decided with matrix below

- X-axis represents the Business impact of the infrastructure and business transaction as desirable (value=1) essential (Value =2) or Vital (Value=3)
- Y-axis represents the likelihood of occurrence of the disaster on a three point scale (1-3)



Risks are placed on matrix based on two criteria

- Likelihood:- Probability of the risk or occurrence of the disaster –on Y axis
- Consequences-Severity of the impact or extent of the damage caused by risk-on X axis

Likelihood of Occurrence

Risks can be classified under one of the following categories

- Definite(Scaled 3):- Risk almost certain to show up during project execution
- Likely(Scaled 2):-Risks having 60-80% chances of occurrence
- Unlikely(Scaled 1):- Rare and exceptional risks which have less than 10% chance of occurrence

Consequences

- Trivial/Insignificant(Scaled 1):- Risk causing a near negligible amount of damage to overall progress
- Minor (Scaled 2):- If a risk will result in some damage, extent of damage is not too significant
- Major(Scaled 3):- Risks with significant large consequences which can lead to a greater amount of loss
- Catastrophic(Scaled 4):- Risks which can make the project completely unproductive and unfruitful, to be a top priority during risk management

Decision

Based on the grid value- the risk can be assessed

- 8 to 12 - Catastrophic
- 4 to 6- Major

- 3- Minor
- 1,2 as Trivial

Risk Assessment

- Assessment of the disruption to critical activities, supported by resources such as people, process, technology, information, infrastructure supplies and stakeholders
- As a result of the BIA and the risk assessment enterprise should identify measures that
 - Reduce the likelihood of a disruption
 - Shorten the period of disruption
 - Limit the impact of a disruption on the enterprise's key products and services

BCM Strategy Process

- Preparation is required to implement the strategies for protecting critical functions and their supporting resources
- Enterprise to develop and document a series of plans, enabling them to effectively manage an incident

BCM Development and Implementation Process

- Enterprise to have an exclusive organisation structure , incident management team/crisis management team for an effective response and recovery from disruptions
- In event of an incident there should be a structure to enable enterprise to
 - Confirm impact of incident
 - Control of the situation
 - Contain the incident
 - Communicate with stakeholders
 - Coordinate appropriate response

Incident Management Plan

- IMP to have top management support with appropriate budget for development, maintenance and training.
- They should be flexible, feasible and relevant

Business Continuity Plan

- To recover or to maintain the activities in the event of a disruption to a normal business operation the BCP is invoked to support the critical activities required to deliver the enterprise objectives
- Recovery Strategies to be two-tiered
 - Business:- Logistics, accounting, human resources, etc. and
 - Technical:- Information Technology (E.g. desktop, client-server)

BCM Testing and Maintenance Process

BCM Testing

- A BCP has to be tested periodically because there could be flaws in the plan and in its implementation
- Plan may become outdated as the resources required to support the critical functions change
- BCP testing to include testing of the technical, logistical , administrative, procedural and other operational systems
- Testing would lead to improvement of capability by
 - Practicing capability to recover from an incident
 - Verifying BCP incorporates all the critical activities
 - Highlighting assumptions
 - Instilling confidence amongst exercise participants
 - Raising awareness of business continuity throughout the enterprise
 - Validating the effectiveness and timeliness of restoration of critical activities
- Objectives of Performing BCP tests are to ensure that
 - Recovery procedures are complete and workable
 - Competence of personnel can be evaluated
 - Sources such as business processes, systems, personnel are obtainable and operational to perform recovery processes
 - Manual recovery procedures and IT backup systems are current and can either be operational or restored
 - Success or failure of the business continuity training program is monitored
- Once plans are developed, initial test of the plans are conducted and any necessary modifications to the plans are made
 - Defining the test purpose/approach
 - Identifying test teams
 - Structuring the test
 - Conducting the test
 - Analysing test results
 - Modifying the plans as appropriate

BCM Maintenance

- Keep documentation up-to-date. Contracts and agreements may also need to reflect the changes
- Objectives of the maintenance tasks undertaken in development of BCP are to
 - Determine the ownership and responsibility for maintaining various BCP Strategies
 - Identify BCP Maintenance triggers
 - Determine the maintenance regime to ensure that the plans remain up-to-date
 - Determine the maintenance processes to update the plan
 - Implement version control procedures to ensure that the plan is up-to-date

Reviewing BCM arrangements

Audit or self-assessment of the enterprise BCM program should verify that

- All key products and services and their supporting critical activities and resources have been identified
- Enterprise BCM policy, strategy, framework and policies reflect its priorities and requirements
- Enterprise BCM competence and BCM capability are effective and fit for purpose
- BCM maintenance and exercising programs have been effectively implemented
- Enterprise has an on-going programme for BCM training and awareness
- Change control processes are in place and operate effectively

BCM Training Process

An enterprise uses training as a tool to initiate culture of BCM in stakeholders by

- Developing BCM program more efficiently
- Providing confidence in stakeholders
- Increasing resilience over time
- Minimising the likelihood and impact of disruptions

Developing a BCM culture is supported by

- Leadership from senior personnel
- Assignment of Responsibilities
- Awareness raising
- Skills training
- Exercising plans

Competencies for the personnel assigned specific management responsibilities are

- Actively listens to others
- Provides support in difficult or challenging circumstances
- Responds constructively to difficult circumstances
- Adopts leadership style appropriately
- Recognises and acknowledges the contribution of colleagues
- Encourages and actively responds to new ideas

Types of Plans

Various Plans that need to be designed are

- Emergency Plan
- Back-up Plan
- Recovery Plan
- Test Plan

Emergency Plan

- It specifies that actions to be undertaken immediately when a disaster occurs
- Management needs to identify the situations when this plan needs to be invoked
- Eg. Major fire, Major structural damage, terrorist attack
- Four aspects to be considered here
 - Who is to be notified immediately
 - Actions to be undertaken
 - Evacuation Procedures
 - Return Procedures (conditions to be met before it is considered safe)

Back-up Plan

The Back-up Plan specifies

- Type of backup to be kept
- Frequency with which the backup is to be undertaken
- Procedure for making backup
- Location of backup resources
- Site where these resources can be assembled
- Personnel responsible for the backup

Recovery Plan

- Backup plan is intended to restore operations quickly so that IS function can continue to service an organisation
- Recovery plans set out procedures to restore the full information system capabilities
- Plan may indicate which applications are to be recovered first

Test Plan

- The purpose of the test plan is to identify the deficiencies in the emergency, backup or recovery plans or in the preparedness of an organisation and its personnel for facing a disaster

Types of Backup

- Full Backup
 - A full backup is exactly what the name implies.
 - It is a full copy of your entire data set.
 - Although full backups arguably provide the best protection, most organizations only use them on a periodic basis because they are time consuming, and often require a large number of tapes or disk.
 - Advantages
 - Restores are fast and easy
 - Easy to maintain and restore different versions

- Disadvantages
 - Backups can take very long as each file is backed up again every time the full backup is run
 - Consumes most storage space compared to incremental and differential backup
- Incremental Backup
 - Because full backups are so time consuming, incremental backups were introduced as a way of decreasing the amount of time that it takes to do a backup.
 - Incremental backups only backup the data that has changed since the previous backup.
 - For example, suppose that you created a full back up on Monday, and used incremental backups for the rest of the week. Tuesday's backup would only contain the data that has changed since Monday. Wednesday's backup would only contain the data that has changed since Tuesday.
 - Advantages
 - Much faster backups
 - Efficient use of storage space
 - Disadvantages
 - Restores are slower than full backup and differential backups
 - Restores are little more complicated. All backups are required to perform a restore
- Differential Backup
 - A differential backup is similar to an incremental backup in that it starts with a full backup, and subsequent backups only contain data that has changed.
 - The difference is that while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup.
 - Suppose for example that you wanted to create a full back up on Monday and differential backups for the rest of the week.
 - Tuesday's backup would contain all of the data that has changed since Monday. It would therefore be identical to an incremental backup at this point. On Wednesday, however, the differential backup would backup any data that had changed since Monday.
 - Advantages
 - Much faster backups than full backups
 - More efficient use of storage than full backups since only files changed since the last full backup
 - Faster restores than incremental backups
 - Disadvantages
 - Backups are slower than incremental backups
 - Not as efficient use of storage space like incremental backups
 - Restores are slower than with full backups

- Restores are little more complicated than full backups but simpler than incremental backups
- Mirror Backups
 - Mirror backups are mirror of the source being backed up.
 - With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup.
 - Mirror backups to be used with caution as a file could be deleted by accident, sabotage or virus
 - Advantages
 - Backup is clean and does not contain old and obsolete data
 - Disadvantages
 - There is a chance that the files in the source are deleted accidentally, by sabotage or through a virus and may also be deleted from the backup mirror

Alternate Processing Facility Arrangements

- Hot Site
 - A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster.
 - For example, if an enterprise's data centre becomes inoperable, that enterprise can move all data processing operations to a hot site.
 - A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment.
- Cold Site
 - A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations.
 - A cold site is less expensive, but it takes longer to get an enterprise in full operation after the disaster.
- Warm Site
 - A Warm site provides an intermediate level of backup.
 - It has all cold site facilities in addition to hardware that may be difficult to obtain and install
- Reciprocal Agreement
 - Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster

If the third party site is to be used for the backup and recovery purposes, security administrators to ensure that a contract is written to cover issues like

- How soon the site would be made available subsequent to disaster
- Number of organisations that will be allowed to use the site concurrently

- Priority to be given to concurrent users of the site
- Period during which the site can be used
- Conditions under which the site can be used
- Facilities and services the site provider agrees to make available and
- What controls will be in place and working at the off-site facility

Disaster Recovery Procedural Plan

The disaster recovery planning document may include the following areas

- Conditions for activating the plans
- Emergency Procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life
- Fallback procedures describing actions to be taken to move essential business activities or support services
- Resumption procedures, describing 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
- Contingency plan testing and recovery procedure
- Checklist for inventory taking and updating the contingency plan on regular basis
- List of phone numbers of employees in case of emergency
- Insurance papers and claim forms
- Alternate manual procedures to be followed such as preparation of invoices
- Details of airlines, hotels and transport arrangements

Audit of BCP/DRP

In 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 disruption

Sample list of BCP Audit Steps

- Determine if a disaster recovery /business resumption plan exists , developed using strong methodology that includes the following elements
 - Identification and prioritisation of activities
 - Plan is based on business impact analysis
 - Operations managers and key employees participated in plan development
 - Plan identifies resources needed for recovery and location of the availability
 - Plan is simple and easily understandable
 - Plan is realistic in assumptions
- Determine if information backup procedures are sufficient for recovery of critical data
- Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested

- Determine if resources have been made available to maintain the disaster recovery/business resumption plan and keep it current
- Obtain and review the current DRP/BCP
- Obtain and review the current BIA
- Determine of the copies of the plan are safeguarded by the off-site storage
- Gain an understanding of the methodology used to develop the existing disaster recovery / business resumption plan
- Have resources allocated to DRP/ BCP become outdated or ineffective
- Determine if the plan has been updated within the last 12 months
- Review information backup procedures in general
- Interview functional area managers or key employees to determine their understanding of the plan
 - Does the plan include provisions for personnel
 - Have key employees seen and are aware of the plan
 - Does Disaster recovery/business resumption plan include contact information
 - Does DRP/BCP include provisions for people with special needs
 - Does DRP/BCP have provision for replacement of staff when necessary
- Building, utilities and transportation
 - Does the BCP/DRP have the provision for inspection by building engineer after the disaster
 - Does BCP/DRP plan consider the need for alternative shelter
 - Review any agreements for the use of backup facilities
 - Verify that the backup facilities were adequate
 - Building safety features regularly inspected and tested
- Information Technology
 - Determine if the plan reflects the current IT environment
 - Determine if plan includes prioritisation of the critical applications and systems
 - Plan includes time requirements for recovery/availability of each critical system
 - DRP/BCP include arrangements for emergency telecommunications
 - Plan for alternative means of data transmission if the computer network is interrupted
 - Determine if testing schedule exists and is adequate
- Administrative Procedures
 - Does the DRP/BCP cover the administrative and management aspects in addition to operations
 - Is there a designated operations centre where incident management teams can coordinate response and recovery
 - Determine if the BCP/DRP covers procedures for disaster declaration, general shutdown and mitigation of operations
 - Have essential records been identified

- To facilitate retrieval, are essential records separated from those that will not be needed immediately
- Does DRP/BCP include the names and numbers of suppliers of essential equipment and other material
- Does the DRP/BCP include provisions for approval to expend funds that were not budgeted
- Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery