CHAPTER-4

Business Continuity Planning and Disaster Recovery Planning

4.1 INTRODUCTION

In the past, firms only needed to plan for, and protect themselves against, events such as fires, hurricanes, tornadoes, earthquakes, floods, power failures and communication outages. These are statistically predictable, quantifiable, insurable and well-understood events. Today, firms must also consider events that are intentional, difficult to quantify, have ambiguous boundaries and involve dimensions of trust events such as cybercrime and denial-of-service attacks; terrorist targets of opportunity; wireless devices; trading partner connectivity; public infrastructure concerns, such as telecommunications, airlines and globalization; and protection of human capital.

Business Continuity Management (BCM), over the years has emerged a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption of all kinds. With the BCM Process in place, enterprises are able to assess the potential threats and manage the consequences of the disruption, which could reduce or eliminate the losses that would have resulted.

Business Continuity Plan Versus Disaster Recovery Plan

A business continuity plan focuses on development, planning and testing of the infrastructure plan developed to address the people, operational processes and business aspects of surviving an outage, primarily:

- What are the mission-critical processes?
- How quickly can they be restored?
- Who are the key personnel?
- How are they going to be notified of an emergency?
- Where and how will they continue to operate?

A disaster recovery plan encompasses the steps taken to implement and support the firm's infrastructure, including hardware, software and sites necessary for the recovery of mission-critical services and applications such as email, trading, voice, file server, accounting and mobility.

4.2 Need of Business Continuity Management:

To meet the enterprise business objective s and ensure continuity of services and operations, an enterprise shall adapt and follow well-defined and time-tested plans and procedures, build redundancy in teams and infrastructure, manage a quick and efficient transition to the backup arrangement for business systems and services.

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

Let us understand some key terms related to BCM:

A. 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.

B. BCP process:

BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.

The purpose of BCP is to ensure that vital business functions (critical business operations) are recovered and operationalized within an acceptable timeframe.

BCP identifies the critical functions of the enterprise and the resources required to support them.

C. Business Continuity Planning (BCP):

It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

Every Business must have a Business Continuity Plan as relevant to the activities of the enterprise.

4.2.1 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. The BCP is expected to provide:

- Reasonable assurance to senior management about the recovery capability of the system from unexpected incident or disaster.
- Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients'.

The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioning teams between the functional area(s) affected and other departments providing support services.

4.2.2 Scope of Business Continuity:

Top management of the enterprise needs to define the scope of the BCM program by identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis.

4.2.3 Advantages of BCM:

The advantages of BCM are that the enterprise:

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

4.3 BCM Policy

BCM Policy is a high level document, which guides the management to make a systematic approach for disaster recovery, to bring about awareness amongst the employee and to test and review the BCP.

The Objectives of BCM Policy is to provide a structure through which:

- The loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction is minimized.
- 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, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updation as required.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

Explain the objectives of Business Continuity Management Policy briefly
[Nov. 14 (4 Marks), PM]

4.4 Business Continuity Planning

Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business continuity covers the following areas:

- **Business Resumption Planning:** This is the operation's piece of business continuity planning.
- **Disaster Recovery Planning:** This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- **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:

- Risk assessment,
- Determination of recovery alternatives,
- Recovery plan implementation, and
- Recovery plan validation.

What is BCP? What are the three areas it should cover? [Nov. 17 (4 Marks)]

4.4.1 Objectives and Goals of Business Continuity Planning

The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide the safety and well-being of **people** on the premises at the time of disaster;
- Continue **critical business operations**; (For Banks eg; Deposits and Withdrawals, For Hospitals eg; ICUs)
- Minimize immediate **damage and losses**;
- Minimize the **duration** of a serious disruption to operations and resources;
- Establish **management succession** and emergency powers;
- Facilitate effective **co-ordination** of recovery tasks;
- Reduce the **complexity** of the recovery effort; (Eg; Hot Site, Refer Concept 4.14)
- Identify **critical lines** of business and supporting functions.

Therefore, the goals of the Business Continuity Plan should be to:

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

Write short note on Goals of the business continuity plan [Nov 13 (4 Marks), Nov 12 (4 Marks)]

Discuss the objectives of Business Continuity Planning [PM]

4.5 DEVELOPING A BUSINESS CONTINUITY PLAN (BCP)

The methodology for developing a BCP can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organization. The methodology emphasizes on the following:

1. Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;

2. Obtaining commitment from appropriate management to support and participate in the effort;
3. Defining recovery requirements from the perspective of business functions;
4. Documenting the impact of an extended loss to operations and key business functions;
5. Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
6. Selecting business continuity teams that ensure the proper balance required for plan development;
7. Developing a business continuity plan that is understandable, easy to use and maintain; and
8. Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Discuss the methodology of developing a Business Continuity Plan [May 14 (4 Marks)]

What are the elements to be included in the methodology for the development of disaster recovery / business resumption plan? [Nov 12 (6 Marks)]

Discuss the methodology of developing a Business Continuity Plan. Also enumerate its eight phases. [PM]

The eight phases are given as follows:

1. Pre-planning Activities	5. Plan Development
2. Vulnerability Assessment & General Definition of Requirements	6. Testing Program
3. Business Impact Analysis	7. Maintenance Program
4. Detailed Definition of Requirements	8. Initial Plan Testing and Plan Implementation

Phase 1 – Pre-Planning Activities (Project Initiation)

This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to:

- Refine the scope of the project and the 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. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules.

Two other key deliverables of this 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 project.

Phase 2 – Vulnerability Assessment and General Definition of Requirements

While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- 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.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.

While developing a Business Continuity Plan what are the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement'?
[Nov. 17 (6 Marks)]

While developing a Business Continuity Plan, what are the key tasks that should be covered in the 2nd phase 'Vulnerability Assessment and General definition of Requirements'? [PM]

Phase 3 – Business Impact Assessment (BIA)

A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:

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

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Phase 4 – Detailed Definition of Requirements

During this phase, a profile of recovery requirements is developed.
This profile is to be used as a basis for analyzing alternative recovery strategies.
The profile is developed by identifying resources required to support critical functions identified in Phase 3.
This profile should include hardware, software, documentation, outside support, facilities and personnel for each business unit.
Recovery Strategies will be based on short term, intermediate term and long term outages.

Phase 5 – Plan Development

During this phase, recovery plans components are defined (i.e. determine available options) and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

Phase 6 – Testing/Exercising Program

The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

Phase 7 – Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.

Phase 8 – Initial Plan Testing and Implementation

Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- Defining the test purpose/approach;
- Identifying test teams;
- Structuring the test;
- Conducting the test;
- Analyzing test results; and
- Modifying the plans as appropriate.

4.6 Components of BCM Process

1. **BCM-Process:**
   The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.

2. **BCM-Information Collection Process:**
   The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.

3. **BCM – Strategy Process**
   Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.

4. **BCM – Development and Implementation Process**
   Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

5. **BCM – Testing and Maintenance Process**
   BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.

6. **BCM – Training Process**
   Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

In today's fiercely competitive business environment which allows for no downtime, a comprehensive Business Continuity Plan is of paramount importance. What are the various components of a BCM process? [May 17 (6 Marks)]

Explain the five stages or components of BCM process which will help BB to manage any future disruptions of the proposed new Core Banking System [May 16 (5 Marks)]

These Components are explained detailed in below:

4.7 Business Continuity Management Process

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

2. **Implementing Business Continuity in the Enterprise and Maintenance:** In establishing and implementing the BCM system in the organization, managers from each function will participate. The program should be communicated to all the stakeholders with appropriate training and testing. In implementation, the major activities that should be carried out include:

   - Defining the scope & context;
   - Defining roles and responsibilities;
   - Engaging and involving all stakeholders;
   - Testing of program on regular basis;
   - Maintaining the currency & appropriateness of business continuity program;
   - Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and business impact analysis (BIAs);
   - 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. The following documents (representative only) are classified as being part of the business continuity management system:

   - The business continuity policy;
   - The business continuity management system;
   - The business impact analysis report;
   - The risk assessment report;
   - The aims and objectives of each function;
   - The activities undertaken by each function;
   - The business continuity strategies;
   - The overall and specific incident management plans;
   - The business continuity plans;
   - Change control, preventative action, corrective action, document control and record control processes;
   - Local Authority Risk Register;
   - Exercise schedule and results;
   - Incident log; and
   - Training program

List out the major activities to be carried out in the implementation of a Business Continuity Plan [May 17 (4 Marks)]

HINT: Refer 2nd point in Concept 4.7

What are the major documents that should be mandatory part of any Business Continuity Management System? [May 17 (6 Marks)]
HINT: Refer 3rd Point in Concept 4.7

What are the major documents that should be the part of a Business Continuity Management system? Explain in brief. [PM]

4.8 BCM Information Collection Process

In order to design an effective BCM, it is pertinent to understand the enterprise from all perspectives of interdependencies of its activities, external enterprises and including:

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

4.8.1 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 business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold, "that is, the length of time business units can survive without access to the system, services and facilities. Major tasks, which are to be undertaken in this analysis, are given as follows:

- 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; (For Banks eg; Deposits and Withdrawals, For Hospitals eg; ICUs)
- 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.

What is Business Impact Analysis? Enumerate the tasks which are to be undertaken in this analysis. [May 13 (6 Marks)]

4.8.2 Classification of Critical Activities:

BCP leader and BCP team leaders in consultation with respective function owner shall carry out Business Impact Analysis for infrastructure and business transactions. BIA will result in categorization (like Vital, Essential and Desirable) of infrastructure and business function following by disaster scenarios (Catastrophic, major, minor trivial) for various disaster causes (fire, flood, system failure etc.), which is given as follows:

- **Business Categorization (Vital/Essential/Desirable):** The parameters considered in deciding whether a function/service is Vital/Essential/Desirable are:
  - Loss of revenue;
  - Loss of reputation;
  - Decrease in customer satisfaction; and
  - Loss of productivity (man-hours)

These parameters shall be graded in a three-point scale 1-3 where,
1 = Low (L)
2 = Medium (M)
3 = High (H)

- **Disaster Scenarios (Major/Minor/Trivial/Catastrophic):** The scenario of disaster shall be decided with the matrix given below:
  The X-axis represents the Business impact of the infrastructure and business transaction as desirable (value=1), essential (value=2) or vital (value=3). The Y -axis represents the likelihood of occurrence of the disaster on a three point scale (1-3).

3 (minor)	6 (Major)	9 (Catastrophic)
2 (Trivial)	4 (Major)	6 (Major)
1 (Trivial)	2 (Trivial)	3 (Minor)

Fig. 4.8.1: Business Impact [Desirable (1), Essential (2), Vital (3)]

Identify all the mission critical processes for categorizing into Vital, Essential and Desirable and looking for the probable disasters as per the list attached.

The Business Impact Analysis matrix is also used to assess Risk and is thus also referred as Risk Assessment Matrix. The interpretation of Fig. 4.8.1 can be drawn like this.

In a risk assessment matrix, risks are placed on the matrix based on two criteria:
1. **Likelihood:** the probability of a risk or the occurrence of the disaster – On Y Axis
2. **Consequences:** the severity of the impact or the extent of damage caused by the risk - On X Axis

Likelihood of Occurrence
Based on the likelihood of the occurrence of a risk, the risks can be classified under one of the following categories:

1. **Definite (scaled 3):** A risk that is almost certain to show-up during project execution. If you're looking at percentages a risk that is more than 80% likely to cause problems will fall under this category.
2. **Likely (scaled 2):** Risks that have 60-80% chances of occurrence can be grouped as likely.
3. **Unlikely (scaled 1):** Rare and exceptional risks which have a less than 10% chance of occurrence.

Consequences:

The consequences of a risk can again be ranked and classified into one of the f ollowing categories, based on how severe the damage can be.

1. **Trivial/Insignificant (scaled 1):** Risks that will cause a near negligible amount of damage to the overall progress of the project.
2. **Minor (scaled 2):** If a risk will result in some damage, but the extent of damage is not too significant.
3. **Major (scaled 3):** Risks with significantly large consequences which can lead to a great amount of loss are classified as critical.
4. **Catastrophic (scaled 4):** These are the risks which can make the project completely unproductive and unfruitful, and must be a top priority during risk management.

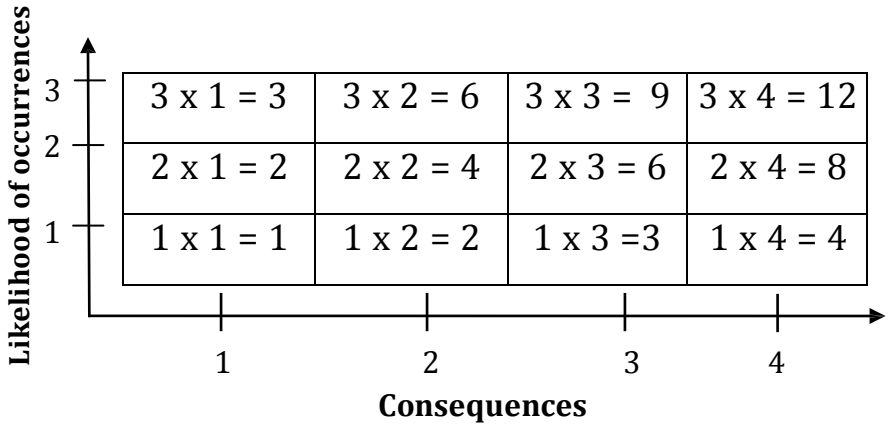

Fig. 4.8.2: Business Impact Matrix (2)

Like-wise the grid can be extended depending upon the criteria one chooses. Depending upon the grid value, the risk can be assessed.

- Like values 8 to 12 can be categorized into Catastrophic.
- Values 4 to 6 can be denoted as Major.
- Value 3 can be given as Minor.
- Values 1 and 2 can be denoted as Trivial.

In some books, the values can be classified into High, Medium, Low, and Very Low.

4.8.3 Risk Assessment

1. The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as people, process, technology, information, infrastructure supplies and stakeholders.
2. The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality.

3. Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.
4. Vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.
5. The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist.
6. Impacts might result from the exploitation of vulnerabilities by threats. As a result of the BIA and the risk assessment, the enterprise should identify measures that:
   - reduce the likelihood of a disruption;
   - shorten the period of disruption; and
   - limit the impact of a disruption on the enterprise's key products and services.

   These measures are known as loss mitigation and risk treatment.

Write short note on Risk Assessment **[May 14 (4 Marks)]**

4.9 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. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

The 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.

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

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

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:

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

The plan development phase also includes the implementation of changes to use procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of recovery teams, their roles and responsibilities. Recovery standards are also developed during this phase. The organization's recovery strategy needs to be developed for the recovery of the many business processes.

4.11 BCM Testing and Maintenance Process:

4.11.1 BCM Testing:

A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change.

Testing of BCP lead to improvement of BCM capabilities by:

- Practicing the enterprise's ability to recover from an incident;
- Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities;
- Highlighting assumptions, which need to be questioned;
- Instilling confidence amongst exercise participants;
- Raising awareness of business continuity throughout the enterprise by publicizing the exercise;
- Validating the effectiveness and timeliness of restoration of critical activities; and
- Demonstrating competence of the primary response teams and their alternatives

In case of Development of BCP, the objectives of performing BCP tests are to ensure that:

- The recovery procedures are complete and workable.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.

- The manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- The success or failure of the business continuity training program is monitored.

4.11.2 BCM Maintenance:

Major 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 organizational, 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 version control procedures to ensure that the plan is maintained up-to-date.

Explain the maintenance tasks undertaken in the Development of BCP. [Nov 16 (4 Marks)]

Discuss the maintenance tasks undertaken in the development of a BCP in brief. [PM]

Explain the objectives of performing BCP tests while developing a business continuity plan.[PM]

4.11.3 Reviewing BCM Arrangements:

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

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

As an IS auditor, What are the key areas you would verify during review of BCM arrangements of an enterprise. [May 15 (4 Marks), PM]

While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. [Nov 14 (6 Marks), PM]

What are the key aspects that should be verified during audit/self-assessment of an enterprise BCM program while reviewing BCM arrangements? [PM]

4.12 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 impact of disruptions

Development of a BCM culture is supported by:

- Leadership from senior personnel in the enterprise;
- Assignment of responsibilities;
- Awareness raising;
- Skills training; and
- Exercising plans.

4.12.1 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 organization 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;
- Adapts leadership style appropriately to match the circumstances;
- Promotes a positive culture of health, safety and the environment;
- Recognizes and acknowledges the contribution of colleagues;
- Encourages the taking of calculated risks;
- Encourages and actively responds to new idea;
- Consults and involves team members to resolve problems;
- Demonstrates personal integrity; and
- Challenges established ways of doing things to identify improvement opportunities.

What competencies are necessary for personal assigned specific management responsibilities within the system while developing BCM? [Nov 16 (4 Marks)]

4.13 TYPES OF PLANS

There are various kinds of plans that need to be designed for Business Continuity Management (BCM) that include the following:

1. Emergency Plan:

The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

2. Back-up Plan:

The backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. For example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire.

The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly.

3. Recovery Plan:

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. Periodically, the recovery committee must review and practice executing their responsibilities so they are prepared should a disaster occur.

4. Test Plan:

The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted.

Explain the Various Plans that need to be designed for Business Continuity Management
[Nov 15 (6 Marks)]

Out of various types of plans used in business continuity planning, discuss recovery plan in brief.
[May 12 (5 Marks)]

Explain briefly the following terms with respect to business continuity and disaster recovery planning:

a. Emergency Plan
b. Recovery Plan
c. Test Plan **[PM]**

4.14 TYPES OF BACK-UPS

Types of Back-Ups:

Full Backup	Incremental Backup	Differential Backup	Mirror Backup

1. Full Backup:

A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. 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.

For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

Advantages	Disadvantages
1. Restores are fast and easy to manage. 2. Easy to maintain & Restore different versions.	1. Backup can take long time to complete. 2. Consumes most storage spaces.

2. Incremental Backup:

An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. 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. The cycle continues this way.

Advantages	Disadvantages
1. Faster backup 2. Efficient use of space as all files doesn't get duplicated.	1. Restores are slower and complicated

3. Differential Backup:

Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full

backup is done first and subsequent backup runs are the changes made 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.

For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and 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	Disadvantages
1. Faster backup than full backup. 2. Efficient use of space since files changed till last time will be copied. 3. Faster restore than incremental backup.	1. Restores are slower and complicated. 2. Backup slower than incremental backup.

4. Mirror back-up:

Mirror backups are, as the name suggests, a 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. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.

For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backup.

Advantages	Disadvantages
1. Backup is clean and don't contain old files.	1. Source file may be deleted accidently.

Write Short note on Types of Backups [Nov 16 (4 Marks), Nov 14 (4 Marks)]

Briefly explain various types of system's back-up for the system and data together. [PM]

Write short note on following;
a. Types of Backups
b. Backup option sites for Alternate Processing facility Arrangements. [PM]

Differentiate between Incremental Backup and Differential Backup. [PM]

4.15 Alternate Processing Facility Arrangements

Security administrators should consider the following backup options:

- **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 soon. An organization can establish its own cold-site facility or enter into an agreement with another organization to provide a cold-site facility.
- **Hot Site:** If fast recovery is critical, hot site backup might be appropriate. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.
- **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.
- **Reciprocal Agreement:** Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

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;
- The **number of organizations that will be allowed to use the site** concurrently in the event of a disaster;
- The **priority** to be given to concurrent users of the site in the event of a common disaster;
- The **period** during which the site can be used;
- The **conditions** under which the site can be used;
- The **facilities** and services the site provider agrees to make available; and
- What **controls** will be in place and working at the off-site facility.

What are the issues that the security administration should consider when drafting the contract with a third party for a backup and recovery site? [Nov. 17 (5 Marks)]

(OR)

Write Short Note on Third party site for backup and recovery [Nov 15 (4 Marks)]

Write Short Note on Back-up option sites for Alternate Processing facility arrangements. [May 15 (4 Marks)]

HINT: Refer Cold Site, Hot Site, Warm Site, Reciprocal Agreement.

Explain briefly the following terms with respect to alternate processing facility arrangements in business continuity and disaster recovery planning.

a. Cold Site
b. Hot Site
c. Warm Site [PM]

A company has decided to outsource its recovery process to third party site. What are the issues that should be considered by the security administrator while drafting the contract? [PM]

Differentiate between Cold Site and Hot Site. [PM]

4.16 Disaster Recovery Procedural Plan

The disaster recovery planning document may include the following areas:

- The 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 jeopardizes (i.e. threatens) business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning (i.e. cooperating) with appropriate public authorities e.g. police, fire, services and local government.
- 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 procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- 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.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- 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.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back -up location, etc.
- Medical procedure to be followed in case of injury.
- Insurance papers and claim forms.
- Back-up location contractual agreement, correspondences.
- Primary computer centre hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

What are the contents of Disaster Recovery Planning? [PM]

4.17 Audit of the BCP/DRP

In this phase, auditor is entrusted with the responsibility to evaluate the process of developing and maintaining documented, communicated and tested plans for the continuity of the business operations. Main objective of the auditor of BCP is to assess the **ability of the enterprise to continue critical operations** during the period of contingency.

Sample list of BCP Audit steps are given below:

1. **Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:**
   - Identification and prioritization of the activities, which are essential to continue functioning.
   - The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
   - Operations managers and key employees participated in the development of the plan.
   - The plan identifies the resources that will likely be needed for recovery and the location of their availability.
   - The plan is simple and easily understood so that it will be effective when it is needed.
   - The plan is realistic in its assumptions.

2. **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?
   - Does the disaster recovery/business resumption plan include provisions for Personnel?
   - Have key employees seen the plan and are all employees aware that there is such a plan? Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
   - Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
   - Does the disaster recovery/ business resumption plan include provisions for people with special needs?
   - Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?

3. **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?
   - Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
   - Review any agreements for use of backup facilities.
   - Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?

- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?
- Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

4. Information Technology

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- Does the disaster recovery/business resumption plan include arrangements for emergency telecommunications?
- Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- 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.

5. Administrative Procedures

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

What are the steps to be taken by an IS auditor with respect to IT in the process of BCP/DRP audit? [May 16 (6 Marks)]

HINT: Refer 4th Point in Concept 4.17

While auditing a Disaster' Recovery Plan (DRP) for information technology (IT) assets, what concerns are required to be addressed? Briefly explain. [May 14 (4 Marks)]
HINT: Refer 4th Point in Concept 4.17

How an auditor will determine whether the disaster recovery plan was developed using a sound and robust methodology? Explain. [Nov 13 (6 Marks)]
HINT: Refer 1st Point in Concept 4.17

MISCELLANEOUS QUESTIONS

Write short note on Audit Tools and Techniques used in Disaster Recovery Plan. [May 13 (4 Marks)]

Answer:

Audit Tools and Techniques in Disaster Recovery Plan: The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:

- **Automated Tools:** Automated tools make it possible to review the large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.
- **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- **Disaster and Security Checklists:** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- **Penetration Testing:** Penetration testing can be used to locate vulnerabilities**.**

Which aspects should be covered while drafting IS security policy for Business Continuity Planning? [May 13 (5 Marks)]

Answer:

The following are the major aspects, which should be covered while drafting IS Security Policy for Business Continuity Planning:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.
- If subsidiaries, divisions, departments, and other organizational units wish to be supported by the management information systems department on a priority basis in the event of an emergency or a disaster, they must implement hardware, software, policies, and related procedures consistent with related standards.
- Computer operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. All departments must use the same framework when preparing information systems contingency plans.
- In addition, recovery priority of all the applications must also be defined by assessing the criticality of the applications. Further, a classification may also be done for application criticality.
- Management must prepare, periodically update, and regularly test emergency response plans and disaster recovery plans that will allow all critical computer systems to continue processing and be available in the event of an interruption or degradation of service and also in the event of a major loss, such as a flood, earthquake.

With reference to Information Security policy, explain the following :
i. Incident handling
ii. Business continuity management **[Nov 13 (4 Marks)]**

Answer:

With reference to Information Security Policy, the brief explanation of the given terms is given as follows:

Incident Handling: For incident handling, following are the major points to be addressed:

- Security incident reporting times and approach must be consistent at all the times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analyzed to identify weaknesses or trends.
- Procedures for the collection of evidence relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches or concerted attempts by third parties to identify security weaknesses.

Business Continuity Management: In Business Continuity Management, following points should be addressed:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.

Write short notes on following:

a. BCP Manual
b. BCP Strategy Process
c. Back-up plan
d. BCM Testing
e. BCM Maintenance **[PM]**

SUMMERY OF EXAMINATION WEIGHTAGE:

ATTEMPT	MARKS
N-17	15
M-17	16
N-16	12
M-16	11
N-15	10
M-15	8
N-14	14
M-14	12
N-13	14
M-13	15
N-12	10
M-12	5