Business Continuity Planning and Disaster Recovery Planning

Basic Concepts

1. **Business Continuity Management**: Business Continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Key terms relating to BCM are:
   - **Business Contingency**: A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.
   - **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.
   - **Business Continuity Planning (BCP)**: It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

2. **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.

3. **BCM Policy**: The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the enterprise, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process market, technology or organizational structure.
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.

5. Objectives 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, an organization must assure that critical operations can resume normal processing within a reasonable time frame.

6. Developing a Business Continuity Plan: The methodology for developing a business continuity plan can be sub-divided into eight different phases: Pre-Planning Activities (Business continuity plan Initiation), Vulnerability Assessment and General Definition of Requirements, Business Impact Analysis, Detailed Definition of Requirements, Plan Development, Testing Program, Maintenance Program, Initial Plan Testing and Plan Implementation.

7. Components of BCM Process: Components of BCM Process are shown in the Fig. 4.1:
8. **BCM Management Process**: A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management.

9. **BCM Information Collection Process**: The pre-planning phase of Developing the BCP also involves collection of information. It enables the organization to define the scope of BCP and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan. Two other key deliverables of that phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to
participate in the business continuity program.

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

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

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

11. **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.

12. **BCM Testing and Maintenance Process:** A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BCP. A 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, (e.g. plan and scope in advance) or allow the enterprise to develop innovative solutions.

The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the enterprise’s business continuity program; that the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise’s structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise’s business continuity and incident management plans.

13. **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.

14. **Types of Plans:** Various plans are as under:

- **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
• **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.

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

• **Test Plan:** The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to assure that the DR plan will work and to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. Periodically, test plans must be invoked.

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

• **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes, prevents it from being a realistic proposition for backing up a large amount of data.

• **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

• **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

• **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

16. **Alternate Processing Facility Arrangements:** Security administrators should consider the following backup options:

• **Cold site:** If an organisation can tolerate some downtime, cold-site backup might be
appropriate. A cold site has all the facilities needed to install a system-raised floors, air conditioning, power, communication lines, and so on.

- **Hot site**: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain.

- **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.

17. **Audit of the BCP/DRP**: In a BCP Audit, the auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. BCP Auditor is expected to identify residual risks, which were not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.

**Question 1**

*Discuss the objectives of Business Continuity planning.*

**Answer**

**Objectives of Business Continuity Planning**: The primary objective of a business continuity planning is to 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 for 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 (both information processing and other resources);
- Minimise immediate damage and losses;
- Establish management succession and emergency powers;
Facilitate effective co-ordination of recovery tasks;
Reduce the complexity of the recovery effort;
Identify critical lines of business and supporting functions.

Question 2
Describe the methodology of developing a Business Continuity Plan. Also enumerate its eight phases.

Answer
The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

(i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
(ii) Obtaining commitment from appropriate management to support and participate in the effort;
(iii) Defining recovery requirements from the perspective of business functions;
(iv) Documenting the impact of an extended loss of availability to operations and key business functions;
(v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
(vi) Selecting business continuity teams that ensure the proper balance required for plan development;
(vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
(viii) Defining how business continuity considerations must be integrated into on-going business planning and system development processes in order that the plan remains viable over time.

The eight phases are given as follows:
(i) Pre-Planning Activities (Business Continuity Plan Initiation),
(ii) Vulnerability Assessment and General Definition of Requirements,
(iii) Business Impact Analysis,
(iv) Detailed Definition of Requirements,
(v) Plan Development,
(vi) Testing Program,
Question 3

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'?

Answer

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.

Question 4

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

Answer

All documents that are part of the BCM are subject to document control and record control processes. The following are the major documents, which should be the part of the business continuity management system:

- The business continuity policy;

- 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.

Question 5
Discuss the maintenance tasks undertaken in the development of a BCP in brief.

Answer
Major maintenance tasks undertaken in development of a 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.

Question 6
Briefly explain various types of system’s back-up for the system and data together.

Or

Explain briefly data back-up techniques.

Answer
Types of system’s Back-ups: When the back-ups are taken of the system and data together, they are called Total System’s Back-up. Various types of back-ups are given as follows:
• **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

• **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

  Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering files, which were charged subsequently from every subsequent incremental backup.

• **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

  Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

• **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

**Question 7**

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

(i) **Emergency Plan**

(ii) **Recovery Plan**

(iii) **Test Plan**

**Answer**

(i) **Emergency plan:** The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. 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.
When the situations that invoke the plan have been identified, four aspects of the emergency plan must be articulated. First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be defined. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

(ii) **Recovery Plan**: The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. 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.

(iii) **Test Plan**: The final component of a disaster recovery plan is a 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. They also fear a real disaster could arise as a result of the test procedures.

**Question 8**

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

(i) **Cold Site**

(ii) **Hot Site**

(iii) **Warm Site**

**Answer**

(i) **Cold site**: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a system-raised floors, air
conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

(ii) **Hot site**: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

(iii) **Warm site**: A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

**Question 9**

*A company has decided to outsource its recovery process to a third party site. What are the issues that should be considered by the security administrators while drafting the contract?*

**Answer**

If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

- 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;
- Procedures to ensure security of company’s data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

**Question 10**

*Describe contents of a Disaster Recovery and Planning Document.*

**Answer**

**Disaster Recovery Procedural Plan Document**: The disaster recovery and planning document may include the following areas:

- The conditions for activating the plans, which describe the process to be followed before each plan, is activated.
• Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaising 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 the process for maintaining the plan.

• Awareness and education activities, which are designed to create an understanding of the disaster recovery process.

• 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.

• Back-up location contractual agreement, correspondences.

• Insurance papers and claim forms.

• Primary computer center 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 during the period of disruption such as manual preparation of invoices.

• Names of employees trained for emergency situation, first aid and life saving techniques.

• Details of airlines, hotels, supplies and transport arrangements.
Exercise

1. Explain the objectives of performing BCP tests while developing a business continuity plan.
2. Briefly explain the maintenance tasks undertaken in the development of a business continuity plan.
3. What are the key aspects that should be verified during audit/self-assessment of an enterprise’ BCM program while reviewing BCM arrangements?
4. Differentiate between Incremental Backup and Differential Backup.
5. Write short notes on the following:
   (i) BCP Manual
   (ii) BCP Strategy Process
   (iii) Back-up Plan
   (iv) BCM Testing
   (v) BCM Maintenance
6. Differentiate between Cold Site and Hot Site.