Chapter 6 Business Continuity Planning & Disaster Recovery Planning

LEARNING OBJECTIVES:

To develop business continuity plan

6.0 Introduction

Business continuity focuses on maintaining the operations of an organisation, especially the IT infrastructure in face of a threat that has materialised. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operation using a prioritised resumption list.

6.1 Business Continuity Planning

Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization 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.

When a risk manifests itself through disruptive events, the business continuity plan is a guiding document that allows the management team to continue operations and running the business under stressful and time compressed situations. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations Business continuity covers the following areas:

- Business resumption planning : The operation's piece of business continuity planning.
- Disaster recovery planning : The technological aspect of business continuity planning necessary to minimise losses and ensure continuity of critical business functions of the organisation in the event of disaster.
- Crisis management : The overall co-ordination of an organisation's response with the goal of avoiding or minimising damage to the organisation'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.

These resource sets can be broken down into the following components: information, technology, telecommunication, process, people, and facilities.

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 organisation to survive a disaster and to re-establish normal business operations.

The key objectives of the contingency plan should be to:

(i) Provide for the safety and well-being of people on the premises at the time of disaster;

(ii) Continue critical business operations;

(iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);

(iv) Minimise immediate damage and losses;

(v) Establish management succession and emergency powers;

(vi) Facilitate effective co-ordination of recovery tasks;

(vii) Reduce the complexity of the recovery effort;

(viii) Identify critical lines of business and supporting functions;

6.2 Developing a Business Continuity Plan

The methodology for developing a business continuity plan can be sub-divided into eight different phases.

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 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 ongoing business planning and system development processes in order that the plan remains viable over time.

The eight phases are described in detail in the following paragraphs:

(i) Pre-Planning Activity: In phase 1, we obtain an understanding of the existing and projected systems environment of the organisation. This enables us to refine the scope of business continuity planning 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.

- Steering Committee should be established for providing direction & guidance.
- The Business Continuity Manager should work with the Steering Committee.
- Two other key deliverables of this phase are:
- the development of a policy to support the recovery programs;
- an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

(ii) Vulnerability Assessment and definition of Requirement : Security and control within an organisation is a continuing concern. It is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimising the impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

This phase will include the following tasks:

(i) A thorough Security Assessment of the system 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.

(ii) The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans and disaster prevention measures where none exist.

(iii) Submit the Present findings and recommendations resulting from the activities to the Steering Committee so that corrective actions can be initiated in a timely manner.

(iv) Define the scope of the planning effort.

(v) Analyse, recommend and purchase recovery planning & maintenance software required to support the development & maintenance of the plans.

(vi) Develop a Plan Framework.

(vii) Assemble business continuity team and conduct awareness sessions.

(iii) 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 assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help understand the degree of potential loss which could occur.

A number of tasks are to be undertaken in this phase as enumerated under:

(i) Identify organisational risks - This includes single point of failure and infrastructure risks.

(ii) Identify critical business processes.

(iii) Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.

(iv) Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.

(v) Determine the maximum allowable downtime for each business process.

(vi) Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.

(vii) Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

There are a number of ways to obtain this information:

Questionnaires,

Workshops,

Interviews,

Examination of documents

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption.

(iv) Detailed Definition of requirements : During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analysing alternative recovery strategies.

This profile should include

- hardware (mainframe, data & voice communication & personal computers).
- software (vendor supplied, in-house developed, etc.).
- documentation (user, procedures).
- outside support (public networks, DP services, etc.).
- facilities (office space, office equipments, etc.).
- personnel for each business unit.

(v) Plan Development : The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies.

The recovery strategies may be two-tiered:

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

In this phase, recovery plans components are defined and plans are documented. IT 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. In the event of a disaster, it is survival and not business as usual.

(vi) Testing the Plan : The Testing/Exercising program is developed during this phase. Testing/Exercising goals are established and alternative testing strategies are evaluated. Unless the plan is tested on a regular basis, there is no assurance that in the event the plan is activated, the organisation will survive a disaster.

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.
- The resources such as business processes, IS 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.

(vii) Maintenance Program : Maintenance of the plans is critical to the success of actual recovery. The plans must reflect changes to the environment.

The tasks undertaken in this phase are:

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

(viii) 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;
- Analysing test results; and
- Modifying the plans as appropriate.

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

6.3 TYPES OF PLANS

There are various kinds of plans that need to be designed. They include the following:

(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 for example, major fire, major structural damage, and terrorist attack.

When the situations that evoke 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 designated.

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

(ii) 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.

The backup plan needs continuous updating as changes occur.

The following resources must be considered :

(i) Personnel : Training and rotation of duties among information system staff so enable them to replace others when required. Arrangements with another company for provision of staff.

(ii) Hardware : Arrangements with another company for provision of hardware.

(iii) Facilities : Arrangements with another company for provision of facilities.

(iv) Documentation : Inventory of documentation stored securely on-site and off-site.

(v) Supplies : Inventory of critical supplies stored securely on-site and off-site with a list of vendors who provide all supplies.

(vi) Data/information : Inventory of files stored securely on site and off site.

(vii) Applications software : Inventory of application software stored on site and off site.

(viii) System software : Inventory of system software stored securely on site and off site.

(iii) Recovery Plan : The backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, whereas, recovery plans set out procedures to restore full information system capabilities.

- Recovery plans 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.
- Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur.
- If committee members leave the organisation, new members must be appointed immediately and briefed about their responsibilities.

(iv) 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 organisation 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.

To facilitate testing, a phased approach can be adopted.

- First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs.
- Next, a disaster can be simulated at a convenient time-for example, during a slow period in the day. Anyone who will be affected by the test (e.g., personnel and customers) also might be given prior notice of the test so they are prepared.
- Finally, disasters could be simulated without warning at any time. These are the acid tests of the organisation's ability to recover from a catastrophe.

6.4 THREATS AND RISK MANAGEMENT

To minimise threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, it can be useful to evaluate potential threats to computer systems.

Discussed hereunder are various threats, risks and exposures to computer systems and suggested control measures.

Lack of integrity: Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, division of job. implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails , audit of adequacy of data integrity.

Lack of confidentiality : Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails , audit of confidentiality of data.

Lack of system availability : Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programs and training of employees, installation of audit trails , audit of adequacy of availability safeguards.

Unauthorised users attempt to gain access to the system and system resources : Control measures to stop unauthorised users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Hostile software e.g. virus, worm, Trojan horses, etc.- Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.

Disgruntled employees : Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of a disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.

Hackers and computer crimes – Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorised changes to programs, installation of logging features and audit trails for sensitive information.

Terrorism and industrial espionage : Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

Single Points of Failure Analysis :

The objective is to identify any single point of failure within the organisation's infrastructure, in particular the information technology infrastructure.

- Single point's of failure have increased significantly due to the continued growth in the complexity in the organisation's IS environment.
- One common area of risk from single point of failure is the telecommunication infrastructure.
- Because of its transparency, this potential risk is often overlooked.
- To ensure single point failures are identified within the organisations at the earliest possible stage.

The objectives of risk assessment are to:

- Identify Information Technology risks
- Determine the level of risk
- Identify the risk factors
- Develop risk mitigation strategies

The benefits of performing a technology risk assessment are:

- A business-driven process to identify, quantify and manage risks while detailing future suggestions for improvement in technical delivery.
- A framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle.
- Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.
- Implementation of strict disciplines for active risk management during the project lifecycle.

6.5 SOFTWARE AND DATA BACK-UP TECHNIQUES

Types of Back-ups : When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

(i) 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.

(ii) 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.

It is very difficult to restore as we have start with recovering the last full backup, and then recovering from every incremental backup taken since.

(iii) 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.

(iv) 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 will probably include files that were already included in earlier differential backups.

(v) 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 can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

6.6 ALTERNATE PROCESSING FACILITY ARRANGEMENTS

Security administrators should consider the following backup options:

(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 mainframe 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 plus 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.

(iv) 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

(1) how soon the site will be made available subsequent to a disaster,

(2) the number of organisations that will be allowed to use the site concurrently in the event of a disaster,

(3) the priority to be given to concurrent users of the site in the event of a common disaster,

(4) the period during which the site can be used,

(5) the conditions under which the site can be used.

(6) the facilities and services the site provider agrees to make available, and

(7) what controls will be in place and working at the off-site facility.

These issues are often poorly specified in reciprocal agreements.

6.7 BACK-UP REDUNDANCY

- **Multiple Backup Media :** For data of high importance it is absolutely unacceptable to have a situation of data loss. Therefore, single point of failure such as failed backup disk that destroys the entire backup history should be eliminated.
- **Off-Site Backup :** off-Site backup is done to keep at least one copy of your redundant backups in an alternative location. In case the size of the backup is considerably big (>10GB), cost of high-speed link, security issues, and backup time will rule out the idea of backing up through high-speed links. A practical solution would be to take a backup into a removable backup disk, which will be shuttled out of your site into a secure location.
- **Where to Keep the Backups :** If removable-media backups are kept next to the computer, a fire or other disaster will probably destroy both. A secure off-site location is best. Consider keeping one backup disk in the office and the other one or two off-site.
- **Media - Rotation – Tactics :** Once in a while, rotate the active backup media with one of the offsite stored media. This will update the offsite media with the latest data changes. To reduce data loss in case of a major disaster, it is recommended to daily switch the active backup media with one of the stored.

Types of Back-up Media : The most common types of backup media available on the market today include :

(i) Floppy Diskettes : Floppy diskettes were available with most desktop computers earlier and they were the cheapest back-up solution. However, these drives have been discontinued due to low storage capacity and are slow.

(ii) DVD Disks : DVD (also known as "Digital Versatile Disc" or "Digital Video Disc") is a popular optical disc storage media format. Its main uses are video and data storage. Most DVDs are of the same dimensions as compact discs (CDs) but store more than six times as much data.

(iii) Tape Drives : Tape drives are the most common backup media around due to their low cost. The average capacity of a tape drive is 4 to 10 GB. The drawbacks are that they are relatively slow when compared with other media, and can tend to be unreliable.

(iv) Disk Drives : Disk drives are very fast compared to tape drives. The disk drive rotates at a very fast pace and has one or more heads that read and write data.

(v) Removable Disks : Using a removable disk such as a ZIP/JAZ drive is becoming increasingly popular for the backup of single systems. They are quite fast, not that expensive and easy to install and carry around.

(vi) DAT (Digital Audio Tape) drives : DAT drives are similar to a standard tape drive but they have a larger capacity. They are fast becoming popular and are slowly replacing the tape drive. The tapes come in DLT (Digital Linear Tape), SDLT (Super Digital Linear Tape), LTO (Linear Tape Open) and AIT (Advanced Intelligent Tape) format, offering up to 260GB of compressed data. The image below shows a typical HP DAT drive.

(vii) Optical Jukeboxes : Optical Jukeboxes use magnetic optical disks rather than tapes to offer a high capacity backup solution. They are ranging from 5 to 20 terabytes. A jukebox is a tower that automatically loads internally stored disks when needed for backup and recovery – just add a certain amount of CDs or DVDs when you first set it up, maintenance is relatively low.

(viii) Autoloader Tape Systems : Autoloader tape systems use a magazine of tapes to create extended backup volumes. They have a built-in capability of automatically loading or unloading tapes. Autoloaders use DAT tapes that come in DLT, LTO and AIT format. By implementing a type library system with multiple drives you can improve the speed of a backup to hundreds of Gigabytes per hour.

(ix) USB Flash Drive : USB flash Drive Plugs into the USB Port on laptop, PC, or Workstation. The USB flash Drive is available in various sizes. This Drive takes advantage of USB Plug and Play capability Saves and backs-up Documents and any File presentations which provides an excellent solution for mobile and storing data as a reliable Data retention media.

(x) Zip Drive : Zip Drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. The Zip drive can be purchased in either a Parallel or a Small Computer System Interface (SCSI) version. In the parallel version, a printer can be chained off the Zip drive so that both can be plugged into your computer's parallel port.

When making your selection, there are five fundamental factors that you should base your decision on.

- Speed : How fast can you backup and restore data using this media?
- Reliability : Can you risk purchasing media that's known to have reduced reliability to save on costs?
- Capacity : Is the media big enough for your backup load?
- Extensibility : If the amount of data grows, will the media support this demand?
- Cost : Does the solution you want fit into your budget?

Backup Tips

(i) Draw up a simple (easy to understand) plan of who will do what in the case of an emergency.

(ii) Be organized! Keep a record of what was backed up, when it was backed up and which backup media contains what data. You can also make a calendar of which type of backup is due on a certain date.

(iii) Utilize the Volume Shadow Copy (VSS) service in Windows Server 2003. This feature allows you to create point-in-time copies of data so that they can be restored and reverted to at any given time. For instance, if a user created a Word document yesterday and decides that he wants to revert to it today, he can do so using VSS.

(iv) Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.

(v) Create a reference point where you know everything is working properly. It will be quicker to restore the changes from tape.

(vi) Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.

(vii) Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

6.8 DISASTER RECOVERY PROCEDURAL PLAN

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, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison 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 organisation, 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 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.

6.9 INSURANCE

The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Policies are contracts that obligate the insurer to indemnify the policyholder or some third party from specific risks in return for the payment of a premium.

Adequate insurance coverage is a key consideration when developing a business recovery plan and performing a risk analysis.

Policies usually can be obtained to cover the following resources:

- **Equipment :** Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- **Facilities :** Covers items such as reconstruction of a computer room, raised floors, special furniture.
- **Storage media :** Covers the replacement of the storage media plus their contents – data files, programs, documentation.
- **Business interruption :** Covers loss in business income because an organisation is unable to trade.
- **Extra expenses :** Covers additional costs incurred because an organisation is not operating from its normal facilities.
- **Valuable papers :** Covers source documents, pre-printed reports, and records documentation, and other valuable papers.
- **Accounts receivable :** Covers cash-flow problems that arise because an organisation cannot collect its accounts receivable promptly.
- **Media transportation :** Covers damage to media in transit.
- **Malpractice, errors:** Covers claims against an organisation by its customers, and omission e.g., claims and omission made by the clients of an outsourcing vendor or service bureau.

Kinds of Insurance :

Insurance is generally divided into two general classes first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. Third-party insurance is designed to protect against claims made against the policyholder and his insurer for wrongs committed by the policyholder.

(a) First-party Insurances - Property Damages :

- It is designed to protect the insured against the loss or destruction of property.
- It is offered by the majority of all insurance firms in the world and uses time-tested forms, the industry term for a standard insurance contract accepted industry-wide.
- This form often defines loss as "physical injury to or destruction of tangible property" or the "loss of use of tangible property which has not been physically injured or destroyed." Such policies are also known as all risks, defined risk, or casualty insurance.

(b) First-party Insurances - Business Interruption : If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans.

(c) Third-party Insurance – General Liability : Third party insurance is designed to protect the insured from claims of wrongs committed upon others. It is in parts based on the legal theory of torts.

- Torts are civil wrongs which generally fit into three categories – intentional, negligent and strict liability.
- Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured.
- Strict liability torts, such as product liability issues, are generally covered under specialised liability insurance.

(d) Third-party Insurance - Directors and Officers : Errors and Omissions (E&O) insurance is protection from liability arising from a failure to meet the appropriate standard of care for a given profession. Two common forms of E & O insurance are directors and officers, and professional liability. Directors and officers insurance is designed to protect officers of companies, as individuals, from liability arising from any wrongful acts committed in the course of their duties as officers. These policies usually are written to compensate the officer's company for any losses payable by the company for the acts of its officer's.

6.10 TESTING METHODOLOGY AND CHECKLIST

With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests:

(i) Hypothetical : The hypothetical test is an exercise to verify the existence of all necessary procedures and actions specified within the recovery plan and to prove the theory of those procedures. It is a theoretical check and must be conducted regularly.

(ii) Component : A component is the smallest set of instructions within the recovery plan which enables specific processes to be performed.

Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods.

Examples of component tests include back-up procedures, offsite tape storage recovery, technology and network infrastructure assembly, recovery and restoration procedures and security package start-up procedures.

(iii) Module : A module is a combination of components. The ideal method of testing is that each component be individually tested before being included in a module. The aim of module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined. If one is able to test all modules, even if unable to perform a full test, then one can be confident that the business will survive a major disaster. Examples of module testing include alternate site activation, system recovery, etc.

(iv) Full : The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective detailed in the recovery plan. The test also verifies the interdependencies of various modules to ensure that progression from one module to another can be effected without problem or loss of data.

The two main objectives associated with full test are:

- To confirm that the total time elapsed meets the recovery time objective.
- To prove the efficiency of the recovery plan to ensure a smooth flow from module to module.

Activities to be done at the time of testing BCP/DRP plan

(i) Setting objectives:

Test objectives should include:

- Recovery of systems at the standby site, and establishment of an environment to enable full accommodation of the nominated applications.
- A fully documented set of procedures to obtain and utilise offsite tapes to restore the system and critical applications to the agreed recovery point, as set out in the recovery plan.
- Recovery of system/application/network/database data from the offsite/backup tapes.
- Detailed documentation on how to restore the production data as stipulated in the recovery plan, to the agreed recovery point.
- Fully documented procedures for establishing communication lines/ equipment to enable full availability and usage by appropriate areas e.g. business units, data entry, users, etc.
- Established communication lines/equipment as set out in the plan.
- Examination of the designated alternative sites and confirmation of all components are also noted in the plan.

(ii) Defining the Boundaries :

- Test boundaries are needed to satisfy the disaster recovery strategy, methodology and processes.
- The management team also must consider future test criteria to ensure a realistic and obtainable progression to meet the end objectives.
- Opportunities to test actual recovery procedures should be taken wherever possible e.g. purchase of new additional equipment, vendor agreements.
- Management must also decide whether or not to include internal (auditors/management) or external (data security services) observers or a combination of both.

(iii) Scenario :

- The scenario is the description of the disaster and explains the various criteria associated with such a disaster.
- The purpose is to explain to all the participants what is, or is not available, what tools can, or cannot be used, the objective of the exercise, the time of the disaster, and the planned recovery points.

(iv) Test Criteria :

- Not all tests require all personnel to attend.
- The test criteria advise all participants including observers as appropriate, where they are to be located and the time/day the exercise will take place.
- The role of the observer is to give an unbiased view and to comment on the area of success or concern to assist in future testing.

(v) Assumption : Assumptions will need to be made.

- They allow a test to achieve the results without being bound by other elements of the recovery plan,
- which may not yet have been verified.
- Assumptions allow prerequisites of a particular component/module to be established outside the test boundaries.

Examples include:

- All technical information documented in the plan, including appendices, are complete and accurate.
- All purchases (equipment, furniture, etc.) can be made in the recovery time required.
- Tapes and other equipment recalled from offsite are valid and useable.

(vi) Test Prerequisites :

- Before any test is attempted, the recovery plan must be verified as being fully documented in all sections, including all appendices and attachments that have been referenced to in each process.
- Each of the participating teams in the test must be aware of how their role relates to other teams, when and how they are expected to perform their tasks, and what tools are permissible.
- It is the responsibility of each team leader to keep a log of proceedings for later discussion and action to prepare better for future tests.

(vii) Briefing session :

- No matter whether it is hypothetical, component, module or full test, a briefing session for the teams is necessary.
- The size of the exercise and the number of staff involved will determine the time between the briefing sessions and the test.
- The final briefing be held not more than two days prior to a test date to ensure all activities are fresh in the minds of the participants and the test is not impacted through misunderstandings or tardiness.

An agenda could be:

(i) Team objectives

(ii) Scenario of disaster

(iii) Time of the test

(iv) Location of each team

(v) Restrictions on specific teams

(vi) Assumptions of the test

(vii) Prerequisites for each team

(viii) Checklists :

- Checklists are directly related to specific modules of the recovery plan and all sections relevant to particular test must be verified as complete before a test date is set.
- As these checklists follow various modules associated with the recovery plan, only those parts applicable to the forthcoming test are compulsory prerequisites for that test.

(ix) Analysing the test : While testing is beneficial, the effective recovery plan can be achieved only by constructive analysis of each test and its result through a post-mortem. This also maintains the momentum gained from the test, which is critical to the process of building a workable plan.

(x) Debriefing session : If the company has a dedicated Disaster Recovery Plan (DRP) team or co-ordinator assigned permanently, the team or co-ordinator would have the responsibility of conducting the briefing and debriefing sessions. If not, then the responsibility lies with the command team leader.

An agenda could be:

(i) Overall performance

(ii) Team performance

(iii) Observations

(iv) Areas of concern

(v) Next test (type and time)

(vi) Test report

Each team leader has the responsibility of maintaining a log of events during each test and is used to produce the test report. Any areas for improvement are noted for action, assigned to the appropriate team member and given a realistic completion date.

A typical format could be:

(i) Executive summary
(ii) Objective results
(iii) Performance
(iv) Overall teams and list of actions
(v) Conclusion

6.11 AUDIT TOOLS AND TECHNIQUES

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 categorised as under:

i. **Automated Tools :** Automated tools make it possible to review 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.

ii. **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.

iii. **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.

iv. **Penetration Testing :** Penetration testing can be used to locate vulnerabilities.

6.12 AUDIT OF THE DISASTER RECOVERY/BUSINESS RESUMPTION PLAN

(i) Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:

- Identification and prioritisation 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.

(ii) Determine if information backup procedures are sufficient to allow for recovery of critical data.

(iii) Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested.

(iv) Determine if resources have been made available to maintain the disaster recovery/ business resumption plan and keep it current.

(v) Obtain & review the existing disaster recovery/business resumption plan.

(vi) Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests

(vii) Obtain and review the existing business impact analysis.

(viii) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.

(ix) Determine if copies of the plan are safeguarded by off-site storage.

(x) Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?

(xi) Gain an understanding of the methodology used to develop the existing business impact analysis.

(xii) Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.

(xiii) Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?

(xiv) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.

(xv) Determine if the plan has been updated within past 12 months.

(xvi) Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?

(xvii) Review information backup procedures in general. The availability of backup data could be critical in minimising the time needed for recovery.

(xviii) 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?

(xix) Does the disaster recovery/ business resumption plan include provisions for Personnel

i) Have key employees seen the plan and are all employees aware that there is such a plan?

ii) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?

iii) Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?

iv) Does the disaster recovery/ business resumption plan include provisions for people with special needs?

v) Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?

(xx) 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 recover/business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, & 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.

(xxi) Information Technology

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritisation 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.

(xxii) 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?

(xxiii) Does the disaster recovery/ business resumption plan include the names and numbers of suppliers of essential equipment and other material?

(xxiv) Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.

(xxv) Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorise activation of the plan should the need arise.

SELF EXAMINATION QUESTIONS

1. Why is a business continuity plan important in an organisation?
2. What are the components of a business Continuity Plan?
3. Describe the methodology of developing a business continuity plan?
4. What are the various phases of developing a business continuity plan?
5. What is business impact analysis?
6. There are different kinds of business continuity plans. Comment?
7. Back-up Plan is one of the most important for an organisation. Comment?
8. As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?
9. What are the benefits of performing a technology risk assessment?
10. Describe various types of back-up techniques?
11. What is the importance of back-up redundancy?
12. What are the various alternate processing arrangements an organisation may consider?
13. Describe various back-up devices?
14. Describe various contents of a disaster recovery procedural plan?
15. What is the importance of taking insurance as a back-up measure? Describe various kinds of insurance?
16. Describe the various disaster recovery testing? Describe the testing procedure?
17. What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.
18. Give an overview of a disaster recovery plan?

BUSINESS CONTINUITY PLANNING The business continuity plan is a guiding document that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations.	**Business continuity plan covers:** Business resumption planning Disaster recovery planning Crisis recovery planning Crisis management	**The business continuity life:** Risk assessment Determination of recovery alternatives Recovery plan implementation Recovery plan validation
OBJECTIVES AND GOALS OF BUSINESS CONTINUITY PLANNING **The objectives:** • Provide for the safety 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 • Minimize immediate damage & 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	**The goals of the business continuity plan:** • 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 • Reduce the complexity of the recovery effort	

DEVELOPING A BUSINESS CONTINUITY PLAN: • Providing an understanding of the efforts required to develop and maintain a recovery plan to the management • Obtaining commitment from management • Defining recovery requirements from the perspective of business functions • Documenting the impact of an extended loss to operations and key business functions • Focusing appropriately on disaster prevention and impact minimization • Selecting business continuity teams • Developing a business continuity plan • Defining integration into ongoing business planning and system development processes	**PHASES OF BUSINESS CONTINUITY PLANNING: (Pakistan Vs Bangladesh Delayed Playing Their Match In India)** • 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	**THREATS AND RISK MANAGEMENT: (Uncle Charlie HIDES)** • Unauthorised users attempt to gain access to the system and system resources • Lack of Confidentiality • Hackers and computer crimes • Lack of Integrity • Disgruntled employees • Terrorism and Industrial Espionage • Lack of System Availability
TYPES OF PLANS: **(Boys Entered the Room)** • Back-up Plan • Emergency Plan • Recovery Plan	**SOFTWARE AND DATA BACK-UP TECHNIQUES: TYPES OF BACK-UPS: (I Managed to Draw a Flower)** • Incremental Backup • Mirror Backup • Differential Backup • Full Backup	**ALTERNATE PROCESSING FACILITY ARRANGEMENTS:** • Cold site • Hot site • Warm site • Reciprocal agreement

BACK-UP REDUNDANCY: **(Where is MOM)** • Where to Keep the Backups • Multiple Backup Media • Off-Site Backup • Media – Rotation – Tactics	**TYPES OF BACK-UP MEDIA:** • Floppy Diskettes • Compact Disks • Tape Drives • Disk Drives • Removable Disks • DAT (Digital Audio Tape) drives • Optical Jukeboxes • Autoloader Tape Systems • USB Flash Drive • Zip Drive	**DISASTER RECOVERY PROCEDURAL PLAN:** • The conditions for activating the plans • Emergency procedures • Fallback procedures • Resumption procedures • A maintenance schedule • Awareness and education activities • The responsibilities of individuals • Contingency plan • The purpose and scope of the plan • Contingency plan testing and recovery procedure • List of phone numbers of employees • Emergency phone list for fire, police, back-up location, etc. • Medical procedure to be followed • Insurance papers and claim forms • Names of employees trained for emergency situation, first aid and life saving techniques
TESTING METHODOLOGY AND CHECKLIST: **(High Court Meeting on Friday)** • Hypothetical • Component • Module • Full	**AUDIT TOOLS AND TECHNIQUES:** **(I-PAD)** • Internal Control Auditing • Penetration Testing • Automated Tools • Disaster and Security Checklists	

---****---