For C.A. Final (New Course)

INFORMATION SYSTEMS CONTROL AND AUDIT

By Devang Dalal

FEATURES:

- **Based on the Institute's revised module.**
- **"Key" provided for memorizing important answers easily.**
  [KEY is like an acronym or a simple word, each letter of which relates to the points of the answer. It is based on mnemonic technique]
- **Revision section for quick overview.**
- **Chapter-wise past exam questions provided.**
- **Practice questions provided for all chapters.**
- **All answers in point form.**
- **Simple and lucid language**

CHAPTER 6

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

1. Business Continuity Planning
1.1. Objectives And Goals Of Business Continuity Planning
2. Developing A Business Continuity Plan
3. Phases Of Business Continuity Planning
3.1. Pre-Planning Activity
3.2. Vulnerability Assessment And Definition Of Requirement
3.3. Business Impact Analysis
3.4. Detailed Definition Of Requirements
3.5. Plan Development
3.6. Testing The Plan
3.7. Maintenance Program
3.8. Testing And Implementation
4. Types Of Plans
5. Threats And Risk Management
5.1. Single Points Of Failure Analysis
6. Software And Data Back-Up Techniques
7. Alternate Processing Facility Arrangements
8. Back-Up Redundancy
8.1. Types Of Back-Up Media
9. Disaster Recovery Procedural Plan
10. Insurance
10.1. Kinds Of Insurance
11. Testing Methodology And Checklist
11.1. Setting Objectives
11.2. Briefing Session
11.3. Debriefing Session
12. Audit Tools And Techniques

1. 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. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations including the quantification of the resources needed to support the operational commitments.

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, the advance planning and preparation 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 to a crisis in an effective timely manner, 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
- Recovery plan validation

1.1. OBJECTIVES AND GOALS OF BUSINESS CONTINUITY PLANNING

(Nov - 08)

The primary objective of a business continuity planning is to enable an organisation to survive a disaster and to re-establish normal business operations. In order to survive, the organisation 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

Therefore, the goals of the business continuity plan should be to:

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

2. DEVELOPING A BUSINESS CONTINUITY PLAN

(Nov - 08)

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:

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

3. PHASES OF BUSINESS CONTINUITY PLANNING:

Pakistan Vs Bangladesh Delayed Playing Their Match In India

The eight phases are described in detail in the following:

1. Pre-Planning Activities (Business continuity plan Initiation)
2. Vulnerability Assessment and General Definition of Requirements
3. Business Impact Analysis
4. Detailed Definition of Requirements
5. Plan Development
6. Testing Program
7. Maintenance Program
8. Initial Plan Testing and Plan Implementation

3.1. 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. 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 business continuity program.

3.2. 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:

- 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.
- The Security Assessment will enable the business continuity 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.
- Analyse, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
- Develop a Plan Framework.
- Assemble business continuity team and conduct awareness sessions.

3.3. BUSINESS IMPACT ANALYSIS

(Nov - 09)

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. The business impact analysis is intended to help understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

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

- Identify organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise potential threats that may lead to a disaster.
- Identify critical business processes.
- Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determine the maximum allowable downtime for each business process.
- Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- 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. 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.

3.4. DETAILED DEFINITION OF REQUIREMENTS

During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analysing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipments, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

3.5. 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)

3.6. TESTING THE PLAN

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. 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.

3.7. MAINTENANCE PROGRAM

Maintenance of the plans is critical to the success of actual recovery. The plans must reflect changes to the environment. 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. 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.

3.8. 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
- Modifying the plans as appropriate

4. TYPES OF PLANS

Boys Entered the Room

1. **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 some resources, the procedures specified in the backup plan might be straightforward.
2. **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. The actions to be initiated can vary depending on the nature of the disaster that occurs. When the situations that evoke the plan have been identified four aspects of the emergency plan must be articulated.
    1. The plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on.
    2. The plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.
    3. Any evacuation procedures required must be specified.
    4. 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.
3. **Recovery Plan:** Whereas the backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, 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. Again, the problem is that they will be required to undertake unfamiliar tasks.

5. THREATS AND RISK MANAGEMENT

(Jun - 09)

Be careful:
Do not confuse with question on Threats to computerised Environment from Chapter 5, paragraph – 2

Uncle Charlie HIDES

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.

1. **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.

2. **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 the confidentiality of data.

3. **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 the 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.

4. **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, updated antivirus software, division

of job and layered control to prevent impersonation, use of disk repair utility, 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.

5. **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.

6. **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.

7. **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 the adequacy of availability safeguards.

5.1. 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 points of failure have increased significantly due to the continued growth in the complexity in the organisation's IS environment. This growth has occurred due to changes in technology and customer's demands for new channels in the delivery service and/or products, for example E-Commerce. Organisations have failed to respond to increase in the exposure from single point of failure by not implementing risk mitigation strategies. One common area of risk from single point of failure is the telecommunication infrastructure. Because of its transparency, this potential risk is often overlooked. While the resiliency of network and the mean average failures of communication devices, e.g. routers, have improved, it is still a single point of failure in an organisation that may lead to disaster being declared. To ensure single point failures are identified within the organisations IS architecture at the earliest possible stage, it is essential, as part of any project, a technology risk assessment be performed.

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. SOFTWARE AND DATA BACK-UP TECHNIQUES - TYPES OF BACK-UPS

I Managed to Draw a Flower

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.

1. **Incremental Backup:** Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. 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, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

2. **Mirror back-up:** It 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.

3. **Differential Backup:** It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

4. **Full Backup:** 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. This is the simplest form of backup with a single restoring session for restoring all backed-up files.

7. 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 mainframe system-raised floors, air conditioning, power, communication lines, and so on. The mainframe is not present, it must be provided by the organisation wanting to use the cold site. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- **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.
- **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 swarm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
- **Reciprocal agreement:**

  (May - 10)

  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 organisations 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
    - What controls will be in place and working at the off-site facility

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

8. BACK-UP REDUNDANCY

Where is MOM

1. **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. At the very least, you should securely store them as far from your

computer as possible. Consider keeping one backup disk in the office and the other one or two off-site.

2. **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.
3. **Off-Site Backup:** Keeping all the eggs in one basket is not a smart strategy. That is why you should 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.
4. **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.

8.1. TYPES OF BACK-UP MEDIA

(Nov - 08)

The most common types of backup media available on the market today include:

1. **Floppy Diskettes:** Floppy diskettes are available with most desktop computers and they are the cheapest back-up solution. However, these drives have low storage capacity and are slow.
2. **Compact Disks:** Compact Disk read only memory (CD-ROM) drives are standard peripheral in most desktop computers. CD's are low cost storage media and have a higher storage capacity than floppy diskettes.
3. **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. Magnetic tape cartridges are used to store the data, which leaves it susceptible to loss of information over time or through breaking/stretching the tape.
4. **Disk Drives:** Disk drives are expensive but very fast compare to tape drives. The disk drive rotates at a very fast pace and has one or more heads that read and write data. If an organisation is looking for a fast method of backup and recovery then disk drives is the way to go – the difference in speed between a tape drive and a disk drive is hours compared to minutes, respectively.
5. **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. The downside is that the capacity is usually (at the time of writing this article) not more than 2GB in size.
6. **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.

7. **Optical Jukeboxes:** Optical Jukeboxes use magnetic optical disks rather than tapes to offer a high capacity backup solution. They are extremely expensive but offer excellent amounts of secure storage space, ranging from 5 to 20 terabytes. A jukebox is a tower that automatically loads internally stored disks when needed for backup and recovery – you just add a certain amount of CDs or DVDs when you first set it up, so maintenance is relatively low.
8. **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 so you won't have to sit and wait for the "please insert tape 2" prompt! If you use an autoloader you will need a third party application that knows how to handle it. 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.
9. **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.
10. **Zip Drive:** Zip Drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. Zip drives and disks come in various sizes. Zip drive comes with a software utility that provides the facility of copy the entire contents of hard drive to one or more Zip disks. The Zip drive can be purchased in either a Parallel or a Small Computer System Interface (SCSI) version.

There are a substantial amount of tools and media available for backing up data. 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 I.T budget?

9. DISASTER RECOVERY PROCEDURAL PLAN

(Nov - 08)

Disaster: The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following are the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This 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.

10. INSURANCE

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:

FARM BEES

- **Facilities:** Covers items such as reconstruction of a computer room, raised floors, special furniture.
- **Accounts Receivable:** Covers cash-flow problems that arise because an organization 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.
- **Business interruption:** Covers loss in business income because an organisation is unable to trade.
- **Equipment:** Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- **Extra expenses:** Covers additional costs incurred because an organisation is not operating from its normal facilities.
- **Storage media:** Covers the replacement of the storage media plus their contents – data files, programs, documentation.

10.1. KINDS OF INSURANCE

Dance Is Laila's Dream

The most common form of first-party insurance is property damage, while the most common form of third-party insurance is liability.

1. **First-party Insurances - Property Damages:** Perhaps the oldest insurance in the world is that associated with damage to property. 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.

2. **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. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world. While the

role of disaster recovery is well understood in business, the insurance industry was slow to accept the indemnity role relative to insuring data in a business interruption liability insurance context. Insurers are generally aggressive in limiting their own liability and have, in a number of instances, argued that a complete cessation of business is necessary to claim damage.

3. **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.

4. **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.

11. TESTING METHODOLOGY AND CHECKLIST

High Court Meeting on Friday

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

1. **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. The exercise is generally a brief one designed to look at the worst case scenario for equipment, ensuring the entire plan process is reviewed.
2. **Component -** A component is the smallest set of instructions within the recovery plan which enables specific processes to be performed. For example the process "System Load/IPL" involves a series of commands to load the system. However, in the recovery situation this may be different from normal operational requirements. Certain functions need to be enabled or disabled to suit the new environment. If this is not fully tested incompatibility problems with other components are likely. 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.

3. **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. It is when a series of components are combined without individual tests that difficulties occur. Examples of module testing include alternate site activation, system recovery, network recovery, application recovery, database recovery and run production processing.
4. **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.

11.1. SETTING OBJECTIVES

Each test is designed around a worst-case scenario for equipment as this will ensure the entire plan is examined for all possible disastrous situations. Only when every requirement associated with each component has been documented and verified can the recovery plan be said to be complete and functional. 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.

11.2. BRIEFING SESSION

No matter whether it is hypothetical, component, module or full test, a briefing session for the teams is necessary. The boundaries of the test are explained and the opportunities to discuss any technical uncertainties are provided. Depending on the complexity of the test, additional briefing sessions may be required to outline the general boundaries, discuss technical queries, and brief the senior management on the test objectives. The size of the exercise and the number of staff involved will determine the time between the

briefing sessions and the test. However this time period must provide sufficient opportunity for personnel to prepare adequately particularly the technical staff. It is recommended that 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:

- Team objectives
- Scenario of disaster
- Time of the test
- Location of each team
- Restrictions on specific teams
- Assumptions of the test
- Prerequisites for each team

11.3. 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. The format is to discuss the results of the findings of the test with a view of improving the recovery plan for future exercises. From these discussions, a set of objectives is developed for later inclusion into the report. An agenda could be:

- Overall performance
- Team performance
- Observations
- Areas of concern
- Next test (type and time)
- Test report

Each team leader has the responsibility of maintaining a log of events during each test. The information gathered from these logs, in addition to the post-mortem report by the test manager 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:

- Executive summary
- Objective results
- Performance
- Overall teams and list of actions
- Conclusion

12. AUDIT TOOLS AND TECHNIQUES

(Jun - 09)

I-PAD

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:

1. **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.
2. **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.
3. **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.
4. **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.

Past Exam Questions:

1. What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery? (10 marks) (Nov – 08)

Ans: Refer paragraph 9

2. Discuss the objectives and goals of Business Continuity planning. (5 marks) (Nov – 08)

Ans: Refer paragraph 1.1

3. Describe the methodology of developing a Business Continuity Plan. (5 marks) (Nov – 08)

Ans: Refer paragraph 2

4. Briefly explain the various types of system's back-up for the system and data together. (5 marks) (Nov – 08)

Ans: Refer paragraph 8.1

5. As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system? (10 marks) (June – 09)

Ans: Refer paragraph 5

6. What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them. (5 marks) (June – 09)

Ans: Refer paragraph 12

7. What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis? (10 Marks) (Nov - 09)

Ans: Refer paragraph 3.3

8. A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract? (5 marks) (May - 10)

Ans: Refer paragraph 7 – Reciprocal agreements

PRACTICE QUESTIONS

1. Describe the methodology and phases of developing a business continuity plan ?
2. Explain the significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan.
3. Explain briefly the following terms with respect to business continuity and disaster recovery planning.

(i) Emergency plan

(ii) Single points of failure analysis

(iii) First-party insurances

(iv) Cold-site, hot-site and warm-site

4. Explain briefly the software and data back-up techniques.
5. Explain audit tools and techniques used for disaster recovery plan.
6. Describe contents of a disaster recovery and planning document.
7. ABC Company is committed to implement the data backup policy through proper planning. What are the major tips that should be followed by the company for the backup ?
8. Differentiate between Incremental Backup and Mirror Backup.
9. A backup is to be prepared for XYZ Company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a 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 recover various systems, and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.
10. 'With good planning, a great deal of disaster recovery testing can be accomplished with moderate expenditure.' Briefly explain the types of testing techniques.

REVISION

CHAPTER 6: BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

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 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 • 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	The goals of the business continuity plan: • Identify weaknesses and implement a disaster prevention program • Minimise 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 minimisation • 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 back-up • Differential Backup • Full Backup	**ALTERNATE PROCESSING FACILITY ARRANGEMENTS:** • Cold site • Hot site • Warm site • Reciprocal agreement

<table>
<tr>
<td>BACK-UP REDUNDANCY: (Where is MOM)
• Where to Keep the Backups
• Multiple Backup Media
• Off-Site Backup
• Media - Rotation – Tactics</td>
<td>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</td>
<td rowspan="2">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.</td>
</tr>
<tr>
<td>INSURANCE: Policies usually can be obtained to cover the following resources – (FARM BEES)
• Facilities
• Accounts Receivable
• Media transportation
• Malpractice, errors
• Business interruption
• Equipment
• Extra expenses
• Storage media</td>
<td>KINDS OF INSURANCE: (Dance Is Laila’s Dream)
• Property Damages (First party)
• Business Interruption (First party)
• General Liability (Third party)
• Directors and Officers (Third-party)</td>
</tr>
</table>

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	