

SYSTEMATIC APPROACH

The image features four golden, stylized humanoid figures with large, reflective spherical heads. They are seated at a desk, each with a laptop open in front of them. The figures are positioned behind a large, silver, cylindrical object that dominates the foreground. The central text is overlaid on the figures and the cylinder.

**INFORMATION
SYSTEM
CONTROL
AND AUDIT**

FOR CA FINAL COURSE

PAPER 6

CA FINAL

INFORMATION SYSTEMS & CONTROL AUDIT

Prepared by:
CA AKHIL MITTAL
B.Com (H), ACA
Email Id: caakhil24.srcc@gmail.com, akhil_20srcc@yahoo.co.in

CHAPTER 6

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

1.) WHAT IS BUSINESS CONTINUITY PLAN

- A.) Defines plan to avoid **CRISES & DISASTERS**.
- B.) If plans are defined, plans for immediate recovery from these **CRISES**.
- C.) Plans for **continuance of business activities**.

2.) COVERAGE AREA OF THE BUSINESS CONTINUITY PLANS:

CODE TO REMEMBER: B-C-D

1. Business Resumption planning:

Provides mission critical business operation even at time of disaster & recovery of disaster.

2. Crisis Management:

It involves planning to manage crises events. The over all co-ordination of an organization's response to a crisis effectively in time with the aim of minimizing damage to the **organization profitability, operations etc.**

3. Disaster Recovery planning:

The technological aspect of BCP, the advance planning & preparations to minimize losses & ensure operations of critical business areas.

3.) GOAL & OBJECTIVE OF BUSINESS CONTINUITY PLAN

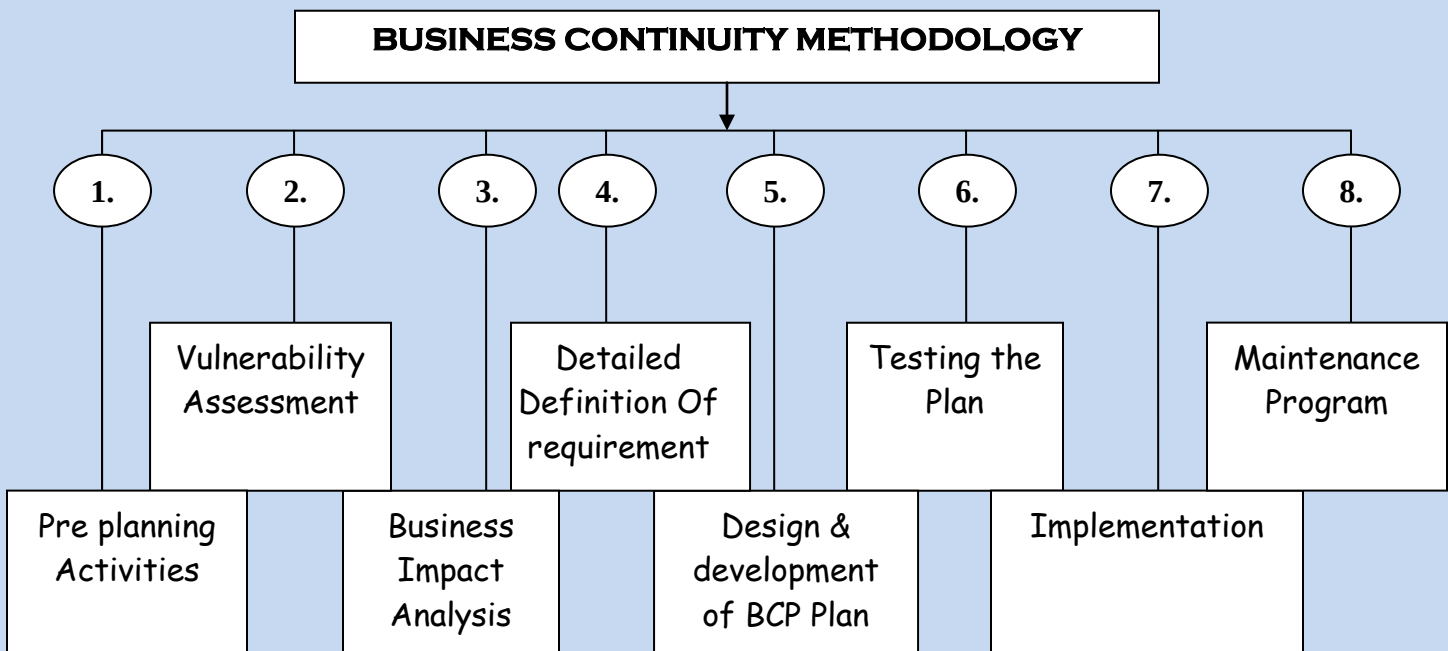
The main objective of business continuity planning is **to survive disaster & restart the normal operations of the business**. Following are the key objectives:

CODE TO REMEMBER: C.O.L.D.S

1. Critical processes and support functions to be identified
2. Operation which are crucial to business to be reassumed quickly.
3. Losses to be minimized.
4. Disruption to be minimized of the operations and resources.
5. Safety to the people at time of the disaster.

4.) BUSINESS CONTINUITY METHODOLOGY:

CODE TO REMEMBER: P.V. - BD² - T.I.M
Present Value of Bad Debt(2) with TIME



Now explaining the each methodology one by one:

1.) PRE-PLANNING ACTIVITIES:

In this phase, following aspects are being taken into consideration for effective business continuity plan:

- (a) Understanding **existing projected systems** environment of organization.
- (b) **Steering Committee** should be established to undertake planning.
- (c) **Manager** with steering committee for finalizing & implementing plan.
- (d) **Develop** policy to support **BCP**.
- (e) **Awareness** & education to management to participate in **BCP**.

2.) VULNERABILITY ASSESSMENT:

In this phase, assessment of **cause of disaster and probability** of disaster occurrence is performed. This phase includes:

- (a) **Analysis** of **possible threats**.
- (b) **Assessment** of all security measures & control for **IT system**.
- (c) This assessment helps **steering committee** in initiating actions in timely manner.
- (d) Scope of planning efforts.

3) BUSINESS IMPACT ANALYSIS:

In this phase, possible impact of **disasters on the business is analyzed**. This enables the business to know or identify **critical systems, processes & functions** and assess economic impact of various incidents. Following some matters are covered:

- Identify risks or disasters
- Identify critical processes
- Identify & quantify the threats to critical processes
- Identify the type & quantity of resources required for recovery etc.

4) DETAILED DEFINITION OF REQUIRMENTS:

Once **BIA** is prepared and accepted, the next step is searching of the details of disaster recovery requirement by the **business continuity team**. This report includes details of resources like **hardware, software, documents, office facility** and **personnel** for business. Here various strategies are determined i.e. **SHORT TERM, MEDIUM TERM & LONG TERM OUTAGES**.

5) DESIGN & DEVELOPMENT OF BCP PLAN:

This phase is extended phase of definitions requirement plans. Here recovery plans components are defined and plans are documented. **The objective of this phase is to DETERMINE THE AVAILABLE OPTIONS** & formulate the appropriate plan/strategy to provide **timely recovery**.

Recovery mode is 2 tiered:

- 1.) **Business-** Logistics, accounting, human resources etc.
- 2.) **Technical-** Information Technology.

6) TESTING THE PLAN:

The testing program is established in this phase. Testing goals are established and alternative testing strategies are evaluated. Unless the plan is tested on a regular basis, there is no assurance that in event the plan is activated, the organization will survive a disaster.

1

Following objectives of performing BCP tests to ensure:

Recovery Procedure must be

P
R
O
C
E
D
U
R
E

Workable



- 1.) Competence of personal in performance.
- 2.) Manual recovery procedures & IT backup are Operational.
- 3.) Business processes resources are obtainable & operational.
- 4.) Success & failure of the business continuity training program is monitored.

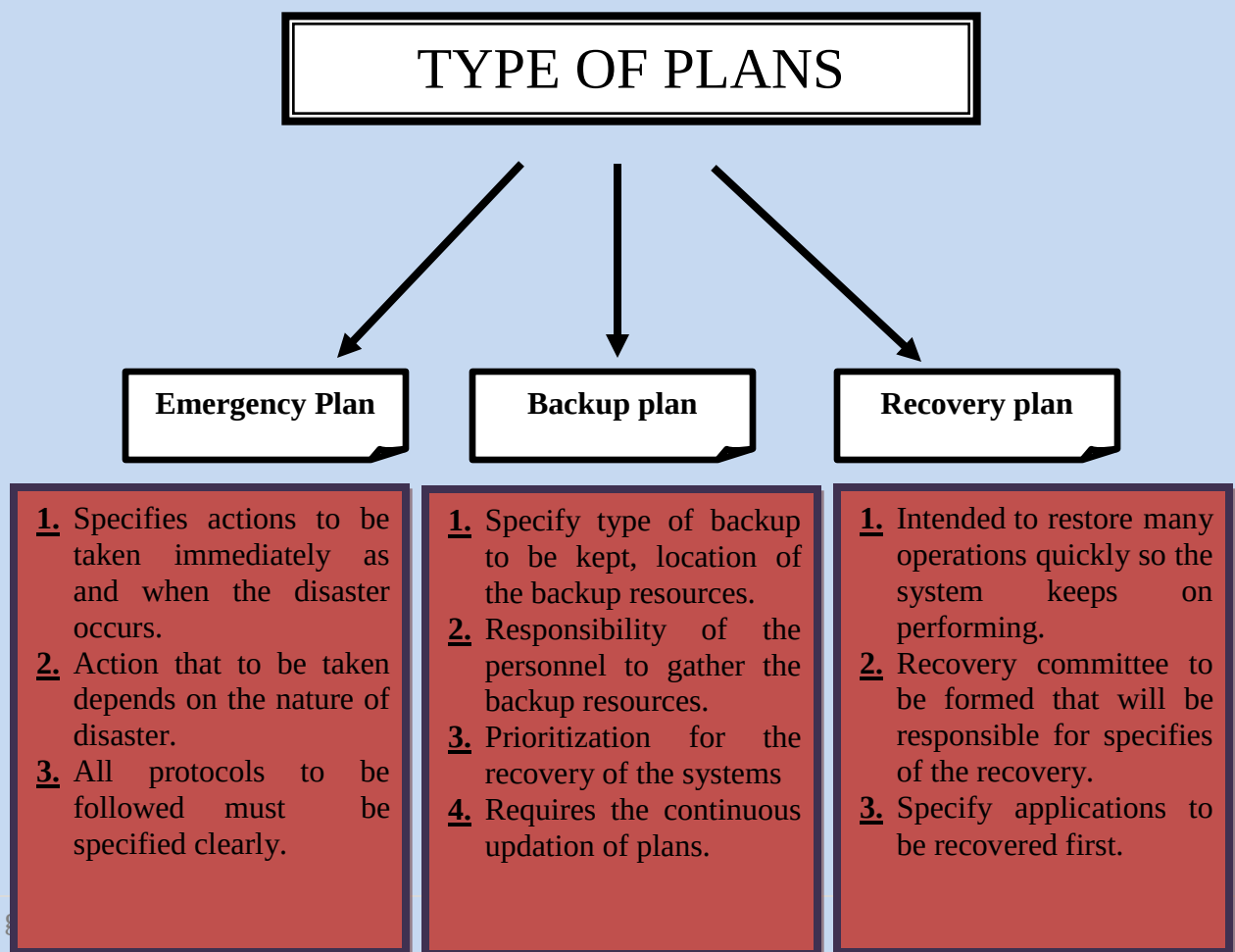
7) Maintenance program:

It is imperative to the success for actual recovery. It is critical that existing resources are revised to take recovery plan maintenance into account. Various tasks are undertaken under this phases which are as follows:

CODE TO REMEMBER: RC-PC
(Means PC ke liye we will be incurring repair cost, so MAINTENANCE

- (A) Determining the Responsibility for maintaining the BCP strategies.
- (B) Ensure that any changes in organization are Communicated to the personnel who are accountable for up to date updates of the plans.
- (C) Maintenance Processes to update the plan.
- (D) Control procedures to ensure that plan is maintained up-to-date.

5.) TYPE OF PLANS:

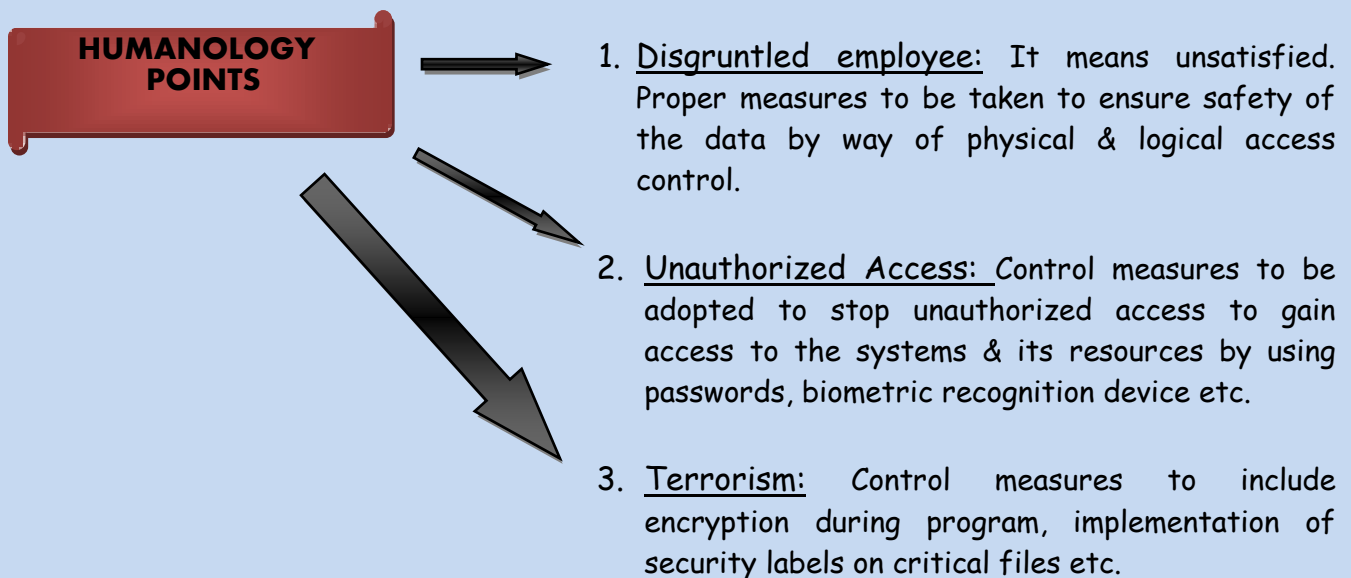


6.) TEST PLANS:

- ✓ It is a basic component of the test plan.
- ✓ **Purpose:** To identify the deficiencies in the emergency, backup, recovery plans
- ✓ Test plans must be reviewed periodically.
- ✓ To facilitate checking, a proper approach to be followed:
 - **Disaster recovery plan can be tested by desk checking.**
 - **A disaster can be simulated at a convenient time.**

7.) THREATS TO COMPUTER SYSTEM:

I AM DIVIDING THE VARIOUS POINTS INTO 3 CATEGORIES. THEY ARE AS UNDER:



TECHNOLOGY POINTS

1. Hacking: Installation of firewalls, intrusion detection system, changes of password, use of digital signature for transmitting data, installation of logging features & audit trail.
2. Hostile software: Establishing policy for sharing external software. Install updated anti-virus, use of diskless PCs & work stations.
3. Lack of system availability: Ensures the availability of systems, software & hardware.

OTHER POINTS

1. Lack of integrity: Control measures to be taken to ensure protection of data to prevent impersonation.
2. Lack of confidentiality: Use encryption & digital signature techniques, employee training and awareness, physical & logical access control etc.

SINGLE POINTS OF FAILURE ANALYSIS

The objective is to **identify** the single point of failure in the organization infrastructure. This failure is caused due to continuous growth in the complexity in organization IS environment. **One common area of risk is TELECOMMUNICATION INFRASTRUCTURE.**

Objective of technical risk assessment:

1. **IT risks identification.**
2. **Determining level of risks.**
3. **Identify risk factors.**
4. **Risk mitigation strategy.**

Benefit of performing technical risk assessment:

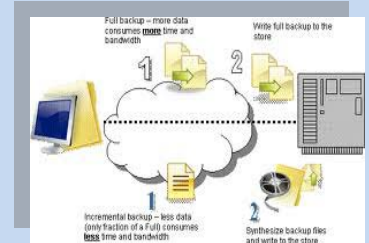
1. **Strict disciplines for active risk management.**
2. **Interpretation & communication of potential risks.**
3. **Framework that provides cyclic checkpoints during product life cycle.**

8.) BACKUP TECHNIQUES:

CODE TO REMEMBER: F-M.I.D

1. FULL BACKUP:

- Captures all files on the disk.
- Every back up generated files contains all the data.
- But it involves good amount of money & time in taking backup.



2. MIRROR BACKUP:

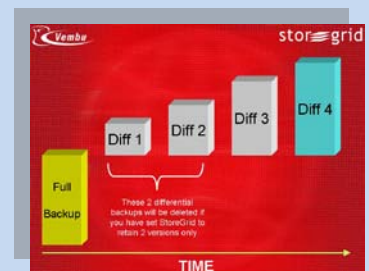
- It is identical to full backup.
- Here files are not compressed in zip files & not password protected.
- Most frequently used for taking backup.

3. INCREMENTAL BACKUP:

- Captures files that were created/changed since last backup.
- This is the most economical method
- Incremental backup are difficult to restore.

4. DIFFERENTIAL BACKUP:

- Stores files that have changed last full backup.
- So if a file is changed after full back up, differential backup is taken.



9.) ALTERNATE PROCESSING FACILITY TECHNIQUES:

FACILITY ARRANGEMENT

COLD SITE

HOT SITE

WARM SITE

RECIPROCAL AGREEMENT

1. COLD SITE:

- ❖ Here the facilities are being stored some other place.
- ❖ It has all the facilities needed to install a mainframe system & all other facilities.
- ❖ An organization can establish its own cold site facilities.

2. HOT SITE:

- ❖ Facilities are available at the site itself.
- ❖ All hardware & operations facilities are available at hot site.
- ❖ But it is very expensive to maintain.

3. WARM SITE:

- ❖ It is a mixture of both hot & cold site.
- ❖ For instance, a warm site contains all equipments & a small mainframe with sufficient power to handle critical application.

4. RECIPROCAL AGREEMENT:

- ❖ Two or more organization agrees to provide backup facilities to each other in an event of any disaster.
- ❖ This type of backup is relatively cheaper.

10.) BACKUP REDUNDANCY(REPETITIVE WORK, DOING MORE THAN NEEDED):

1. MULTIPLE BACKUP MEDIA:

- A. Best for the data which is of high importance.
- B. Here the data is being stored at multiple places.
- C. As such the possibility of single point of failure is eliminated.

2. OFF SITE BACKUP:

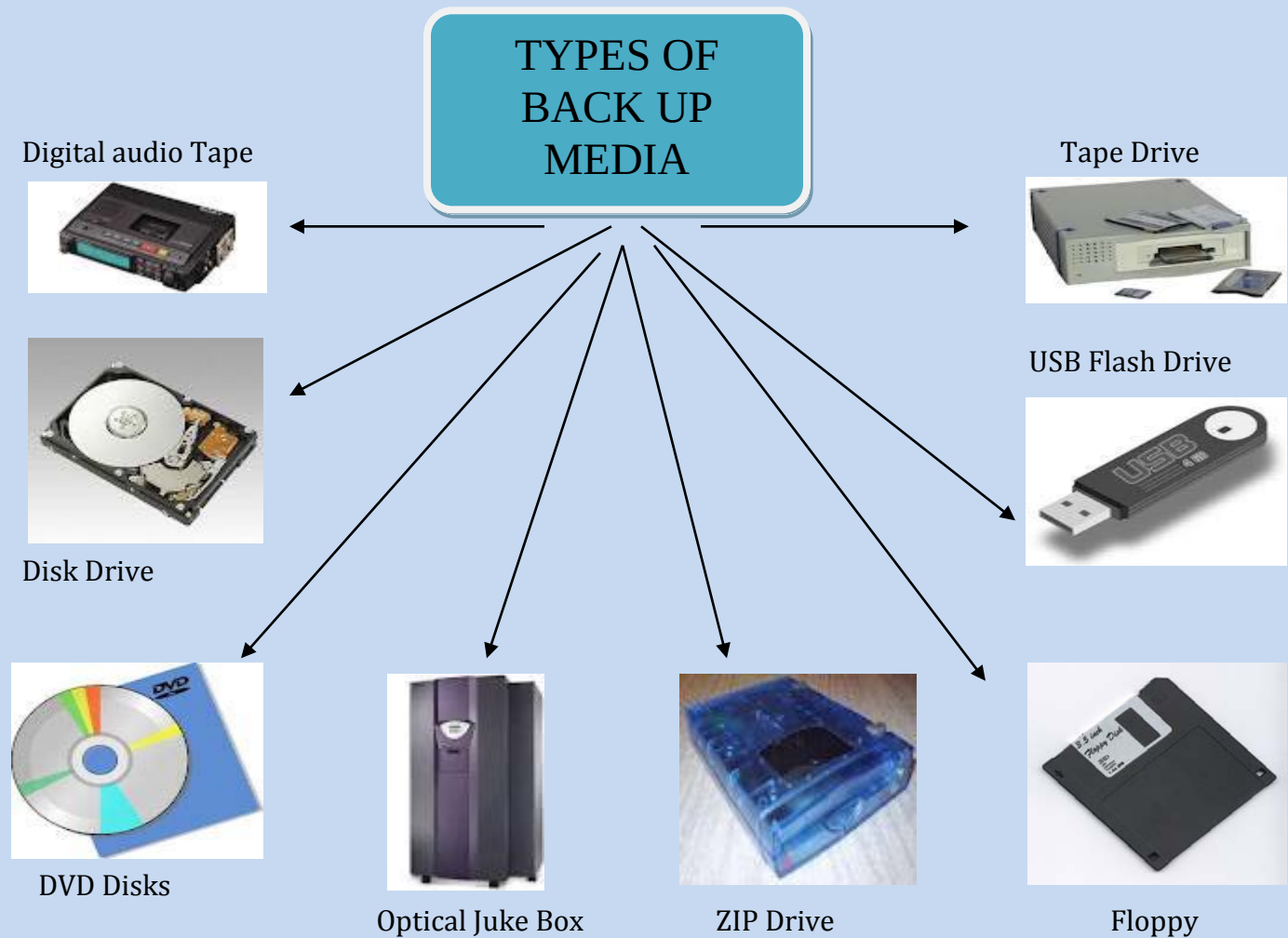
- A. Keep atleast 1 copy of back up in alternate location.
- B. Keep the data in a removable backup disk.

3. MEDIA ROTATION TACTICS:

- A. Rotate the active backup media with one of the offsite stored media.

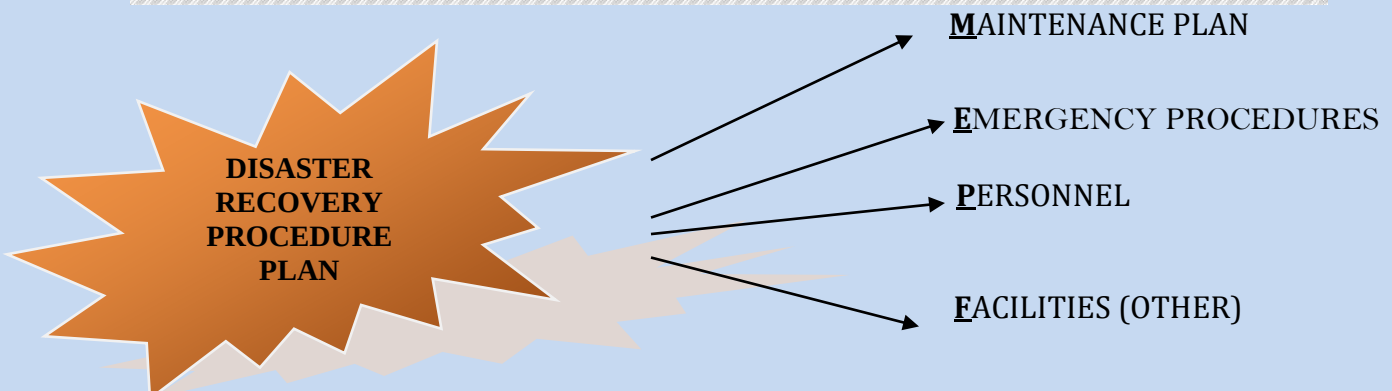
B. Rotate the active backup media with the stored ones.

11.) TYPES OF BACKUP MEDIA:



12.) DISASTER RECOVERY PROCEDURE PLAN:

CODE TO REMEMBER: M.E.-P.F.



MAINTENANCE PLANS INCLUDES:

1. Maintenance schedule, specifying how & when plan to be tested.
2. Conditions for activating plans, which describe the process to be followed before each plan is activated.

EMERGENCY PROCEDURES INCLUDES:

1. Emergency procedures to be taken following an incident which may affect business operations & human life.
2. Resumption procedures that describe the action to be taken to get back to normal business operations.
3. Contingency plan document list & its testing recovery procedures.

PERSONNEL:

1. Awareness & educational facilities to provide an understanding about the organization.
2. Responsibilities of individuals to execute the components of plan.
3. List of phone number of all employees.
4. Name of employees trained for the emergency situation.
3. List of vendors doing business with the organization.

FACILITIES:

1. Details of airlines, hotels & transport agreements.
2. Location of data & program files, data dictionary.
3. Insurance papers & claim forms.
4. Medical procedures to be followed in case of injury.

13.) INSURANCE:

The purpose of taking the insurance is to spread the economic cost to large number of people. It is of prime importance while developing a business recovery plan.

CODE TO REMEMBER: M.E./E.F.----B.P./C.T.S. [INSURANCE]

ME(maine) **EF** (Emergency form) fill kara----for **BP**(Blood pressure) & **CTS**(CT scan)

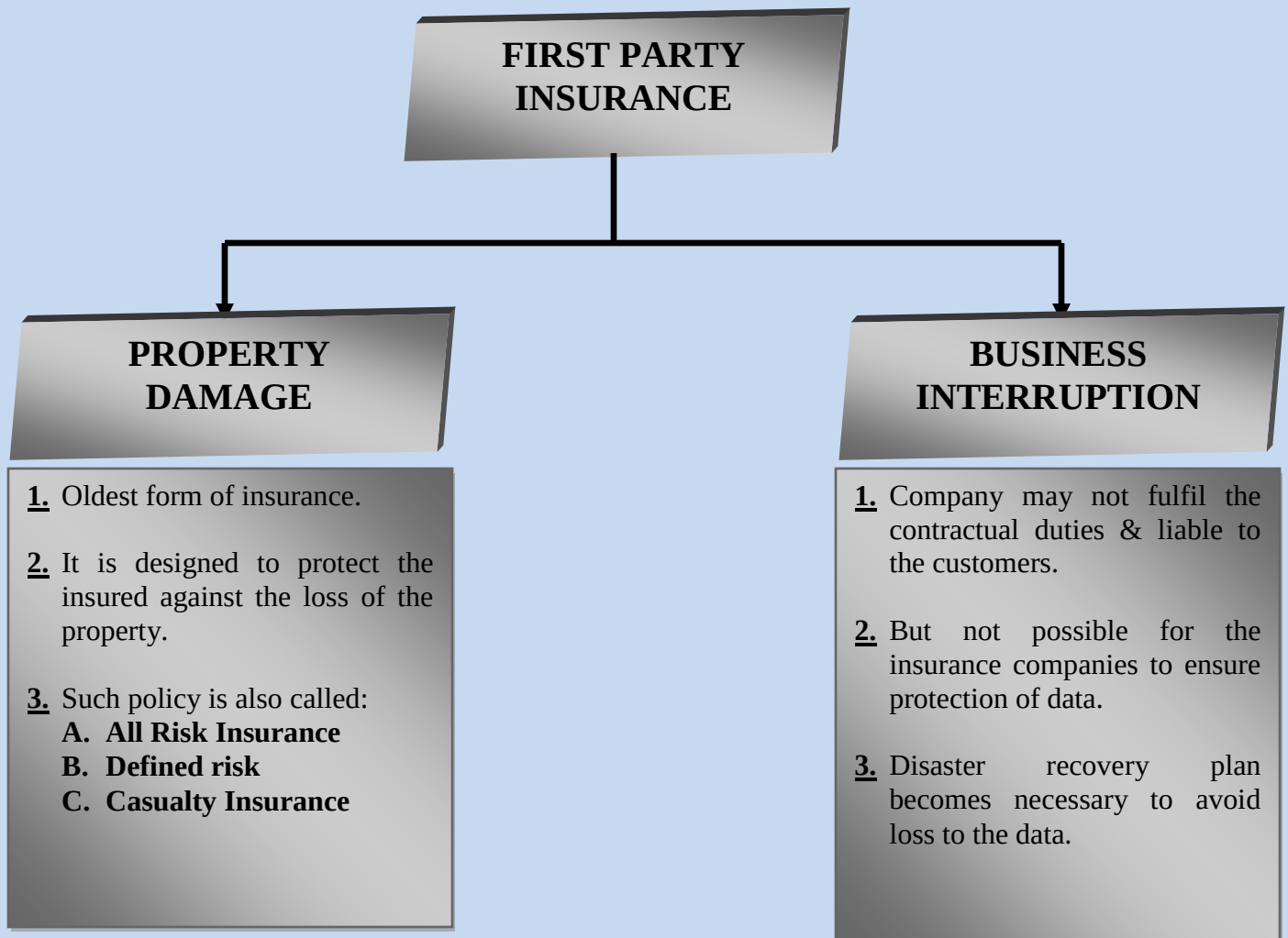
1. **M**alpractice & errors: **Cover claims of customer against organization.**
2. **E**quipments: **Covers repair/acquisition of hardware whether purchased or leased.**
3. **E**xpenses: **Covers additional cost incurred as company is not having arrangements for these additional expenses.**
4. **F**acilities: **Cover items such as reconstruction of computer room etc.**

5. **Business Interruption: Cover losses in business income as organization is not operating.**
6. **Papers: Cover important documents such as reports, source documents etc.**
7. **Cash Inflows: Covers cash flow problems as organization is not able to collect accounts receivable.**
8. **Transportation: Covers damage to media in transit.**

14.) KINDS OF INSURANCE:

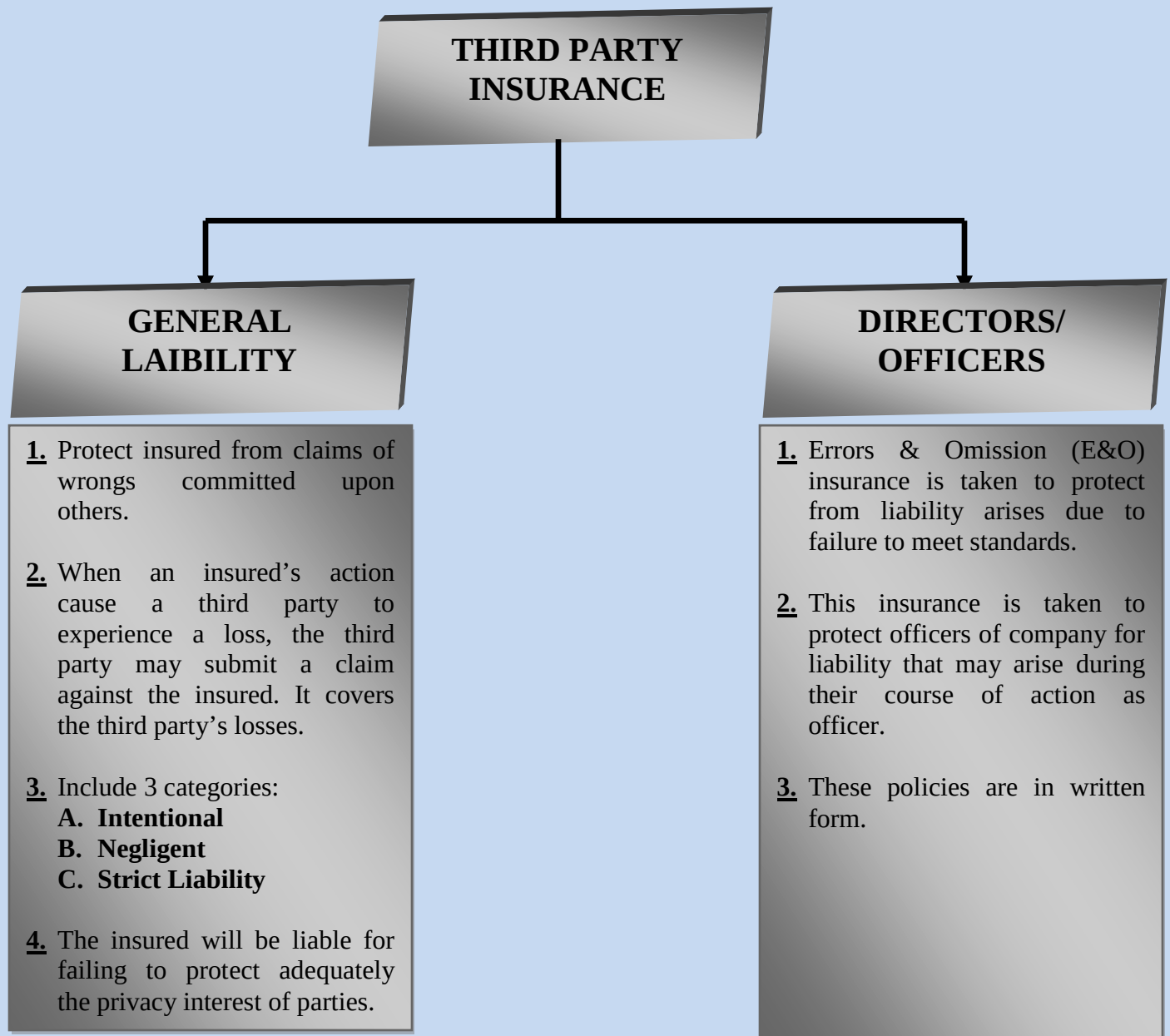
A. FIRST PARTY INSURANCE:

Here claim is by the policy holder against their own insurance.



B. THIRD PARTY INSURANCE:

Designed to protect against claims made against policy holder. For instance company



15.) TESTING METHODOLOGY & TESTING:

CODE TO REMEMBER: M.F.---H.C.
MF HUSSAIN IN HC (High Court)



A. Module:

1. It is combination of components.
2. Here each component is individually tested before included in a module.
3. Helps in verifying **validity & functionality** of recovery procedures.

B. Full:

1. These tests verify each component within every module.
2. Ensures interdependencies of various modules.
3. Objective :
 - Confirm total time elapsed meet the recovery time objective.
 - Proves efficiency of recovery plan.

C. Hypothetical :

1. It is an exercise to verify existence of necessary procedures & actions.
2. It is theoretical check & must be conducted regularly.

D. Component:

1. Component is smallest set of instructions with the recovery plan.
2. It is designed to verify details & accuracy of individual procedures within recovery plan.
3. Examples: **Backup, recovery & restoration procedures.**

Important note:

I hereby request the readers to study the following topics from the STUDY MATERIAL:

- | | |
|-----------------------------------|-------------------------|
| 1. Setting objectives of testing. | 6. De-briefing Session. |
| 2. Defining the boundaries. | 7. Checklists |
| 3. Scenario. | 8. Briefing Session. |
| 4. Test Criteria. | 9. Assumptions. |
| 5. Test Perquisites. | |

I am not briefing these topics as these are not important according to me. Otherwise I will provide you all if required.

16.) AUDIT TOOLS AND TECHNIQUES:

CODE TO REMEMBER: P.A.I.D.

- A. Penetrating testing:** Used to locate vulnerabilities.
- B. Automated Tools:** With the help of tool it is possible to review larger computer systems for flaws.
- C. Internal Control Auditing:** This includes INQUIRY, OBSERVATION & TESTING. This process can detect illegal acts, errors etc.
- D. Disaster & Security Checklists:** A checklist can be used to audit the system. This list to be based upon the disaster recovery policies.

@@@@@@@@@@@@@@@@ END OF CHAPTER @@@@@@@@@@@@@@@@@@