BCP and DRP

Chapter 6.1

Contents

- Threats to computer system and suggested control measures
- How organization’s infrastructure is at risk?
- Single point analysis

Threats and Risk Management

Threats/Risk/Exposure to **computer system** and suggested control measures

ALSO How Organization's infrastructure is at Risk and suggested control measures	**Suggested Control Measures**
Lack of Integrity	1. Implementation of security policy, procedure and standards 2. Use of encryption techniques and digital signatures 3. Authentication and access control techniques 4. Security awareness programs and training of employees 5. Installation of audit trails
Lack of Confidentiality	1. Development of security policy, procedure and standards 2. Use of encryption techniques and digital signatures 3. Implementation of physical and logical access controls 4. Employee awareness and training 5. Installation of audit trials
Lack of System Availability	1. Implementation of physical and logical access controls 2. Security awareness programs and training of employees 3. Installation of audit trials
Disgruntled Employees	1. Installation of physical and logical access controls 2. Security awareness programs and training of employees
Hackers and Computer Crimes	1. Use of encryption techniques and digital signatures 2. Installation of audit trials
Unauthorized users attempt to gain access to the system and system resources	1. Identification and authentication mechanism like logical and physical access 2. Use of encryption during checksum
Terrorism and Industrial Espionage	1. Use of encryption during program storage and data storage 2. Installation of intrusion detection programs

How organization’s infrastructure is at risk from a large number of potential threats and hazards ?

Human errors	Equipment failure	Utility Outage	Supply chain	Fire	Strike
Outsourcing	Technology	Organizational Infrastructure	Outage	Third Parties	Vendors
Environmental Conditions	Internet	Water Leaks	Viruses	Terrorism	Hackers

Single Point Failure Analysis
(The objective is to identify any single point of failure within the organization's infrastructure, in particular the information technology infrastructure

To ensure single point failure are identified within the organization's IS architecture at the earliest possible stage, it is essential, as a part of any project, **a technology risk assessment** be performed	
Objectives of Risk Assessment or Technology Risk Assessment	Benefits of performing technology risk assessment (It is)
Identify information technology risk	A business-driven process to identify, quantify and manage risks while detailing future suggestions for improvement in technical delivery
Determine level of risk	A framework that governs technical choice and delivery processes with cyclic check points during the project life-cycle
Identify the risk factors	Interpretation and communication of potential risk impact where appropriate, risk reduction to a perceived acceptable level
Develop risk mitigation strategies	Implementation of strict disciplines for active management during the project life-cycle

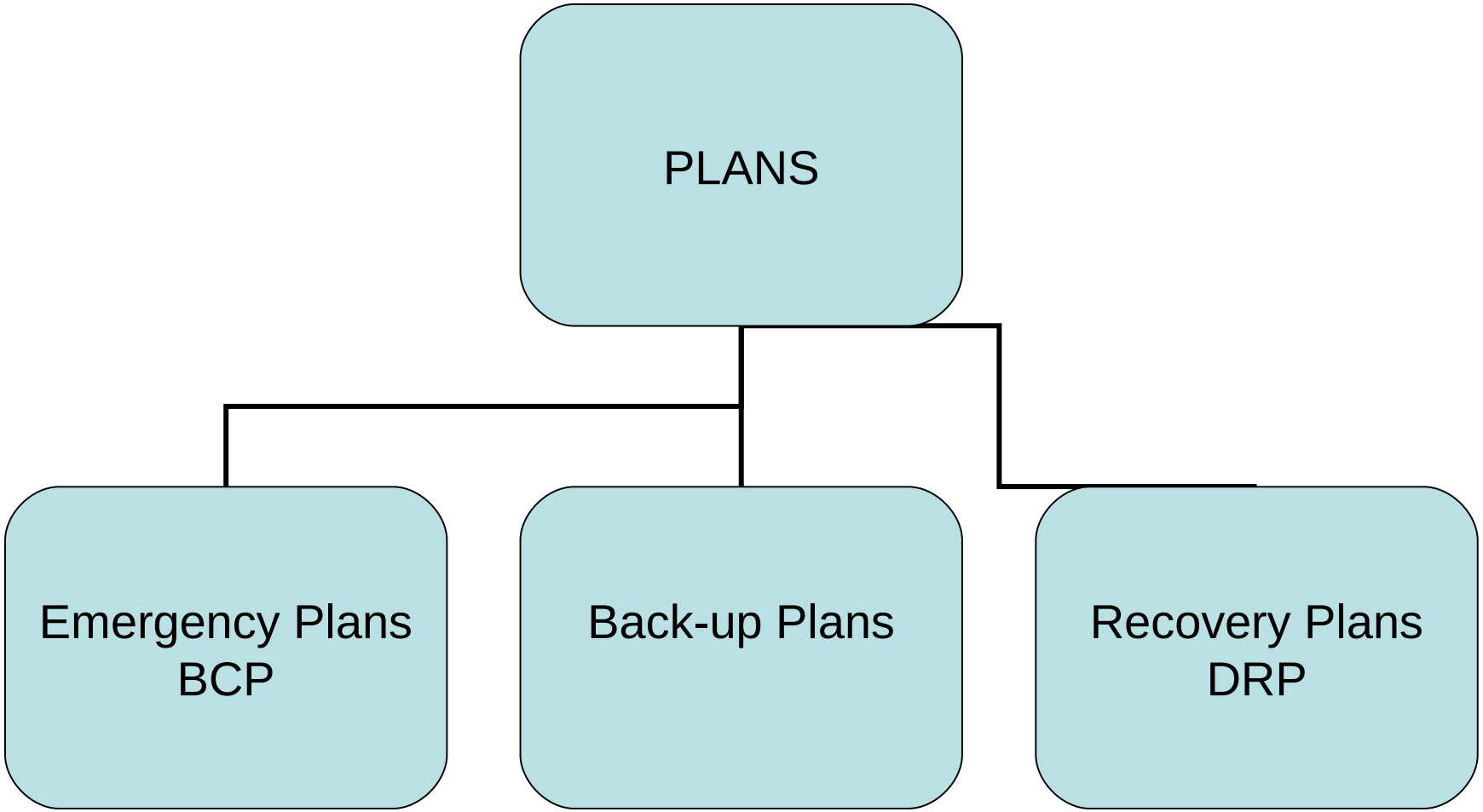
BCP and DRP

Chapter 6.2

Contents

- Types of plans
  - Emergency Plans

Types of plans

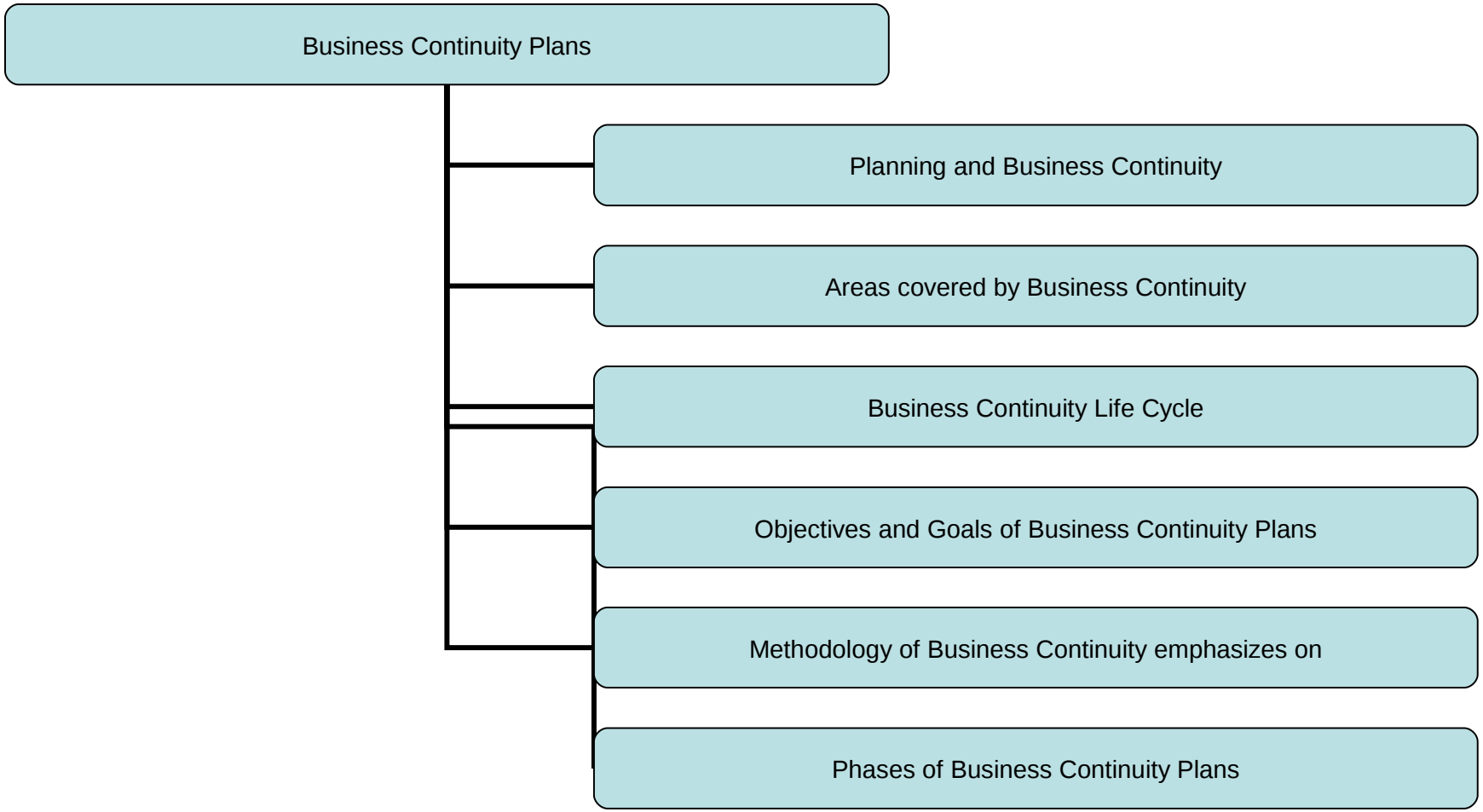


Emergency Plans

- It specifies the actions to be taken immediately after disaster occurs
- Management must identify those situations
- These situations require planning
- The actions to be initiated may vary depending on the nature of disaster that occurs
- When situations that evoke the plan have been identified, 4 aspects of emergency plans must be articulated

- The for aspects are
  1. Plan must show who is to be notified immediately when disaster occurs
  2. Plan must show the actions to be undertaken
  3. Plan must specify the evacuation procedures
  4. Plan must designate return procedures

Emergency Plans

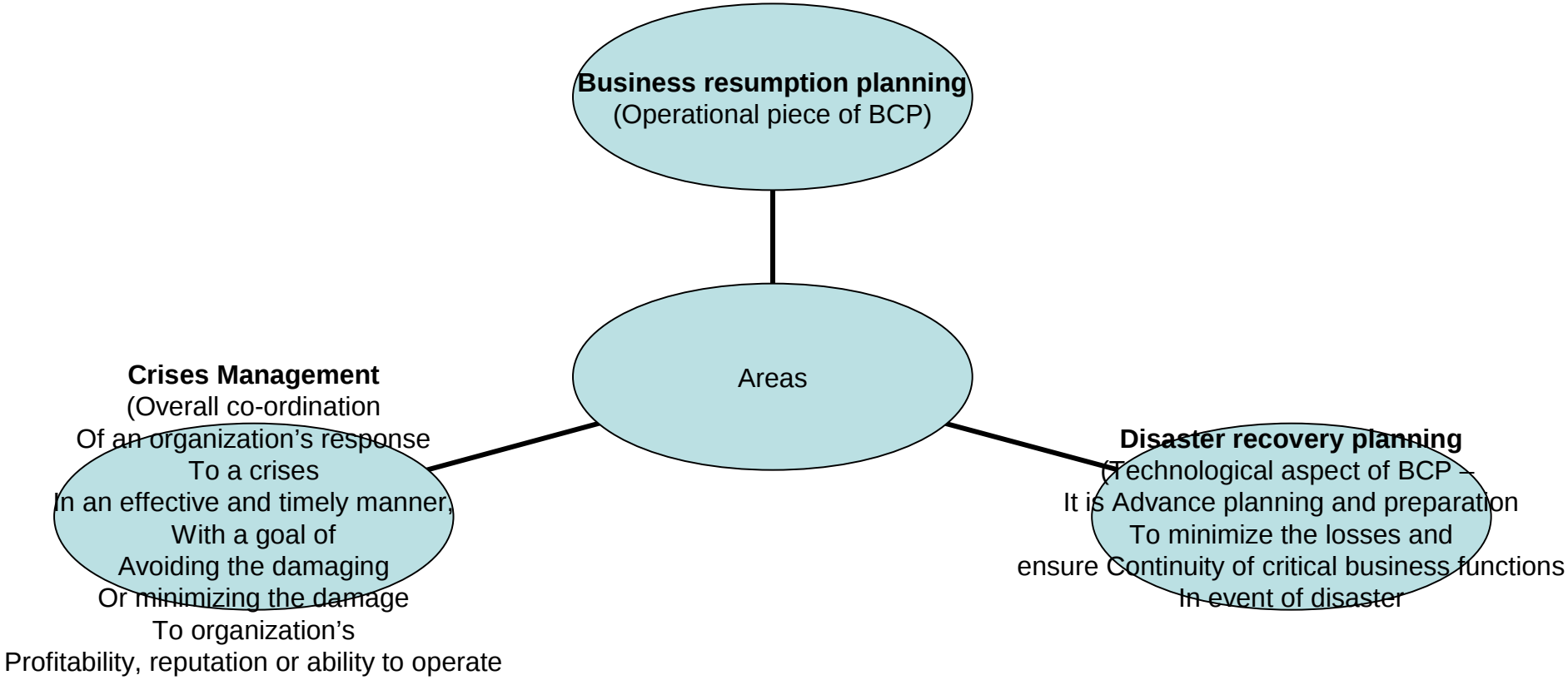


Planning and Business continuity planning

- Planning is an activity
- to be performed before the disaster occurs or
- it would be too late to plan an effective response.
- The resulting outage from such disaster can have a serious effects on
  - the viability of firm's operations,
  - profitability,
  - quality of service and
  - convenience.

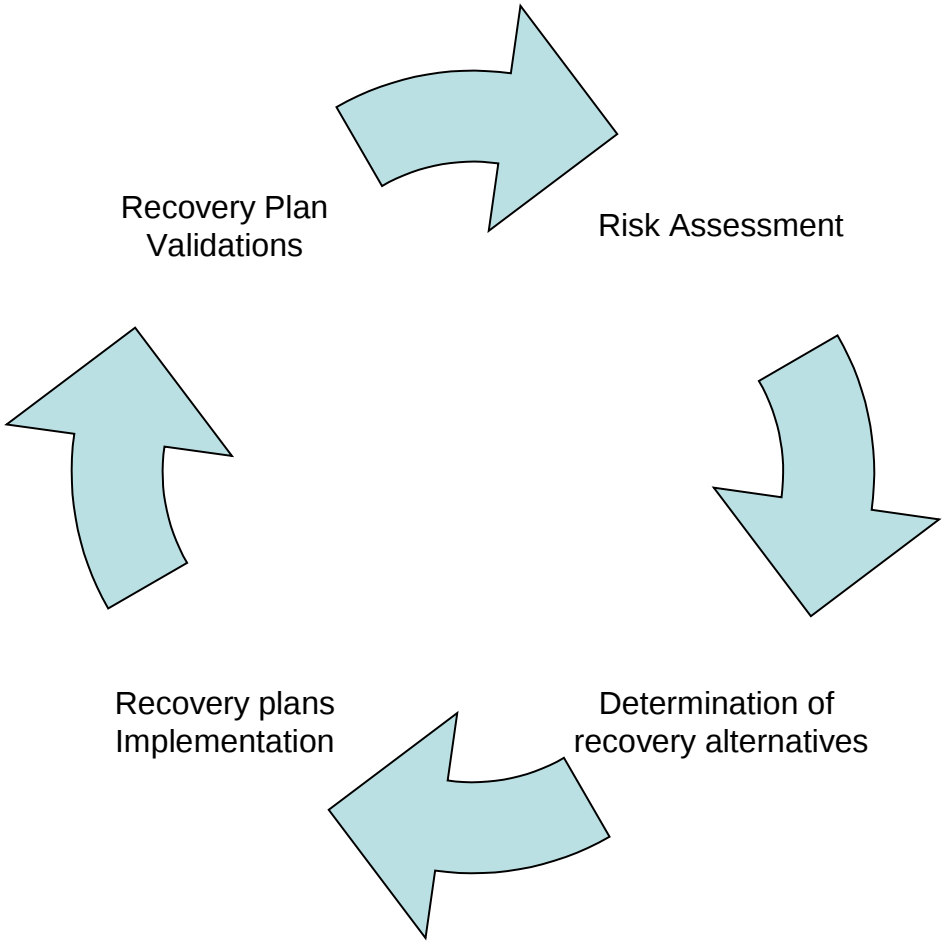
- Business continuity planning is
  - creation and
  - validation of practical logistical plans
  - for how an organization will
    - recover and
    - restore
      - partially or
      - completely the
        - » interrupted critical functions
        - » within pre-determined time after a disaster.

Areas covered by business continuity



Business continuity life cycle

(With each of these sections applicable resource sets [information, technology, telecommunication, process, people and facilities] are manipulated to provide best mix at optimal cost with minimum losses

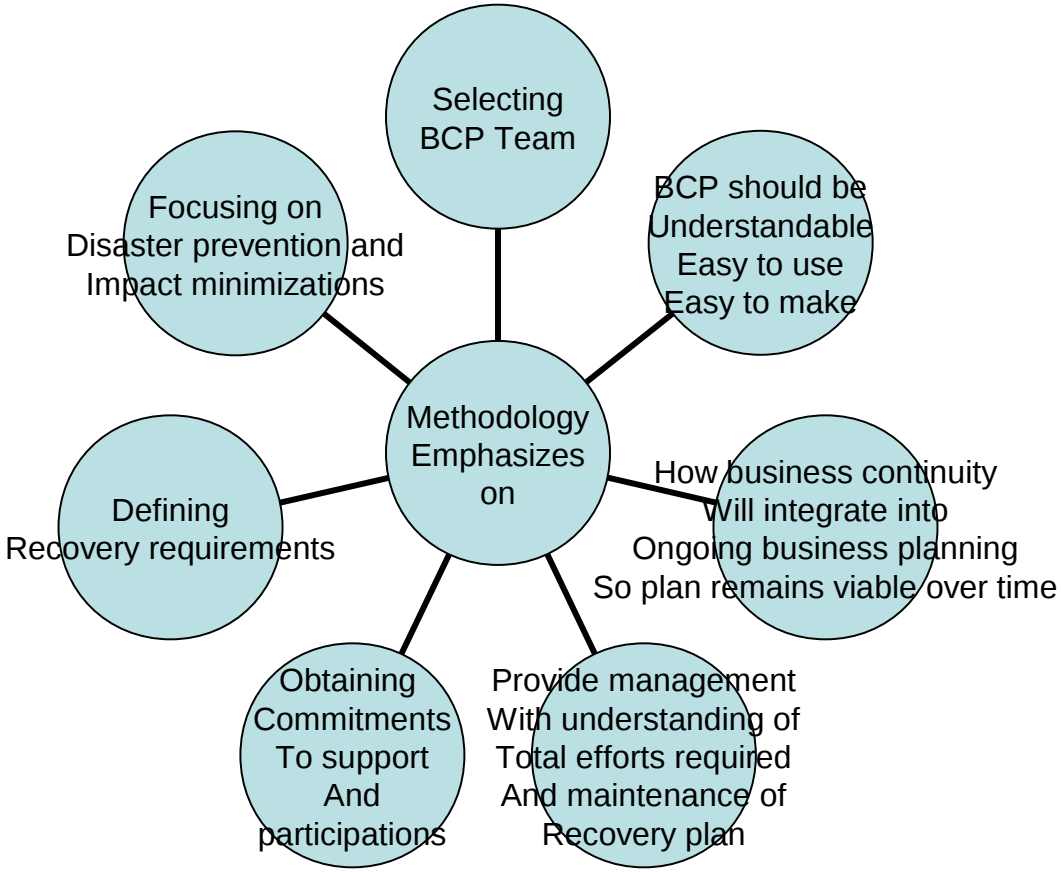


Objectives and Goals of BCP

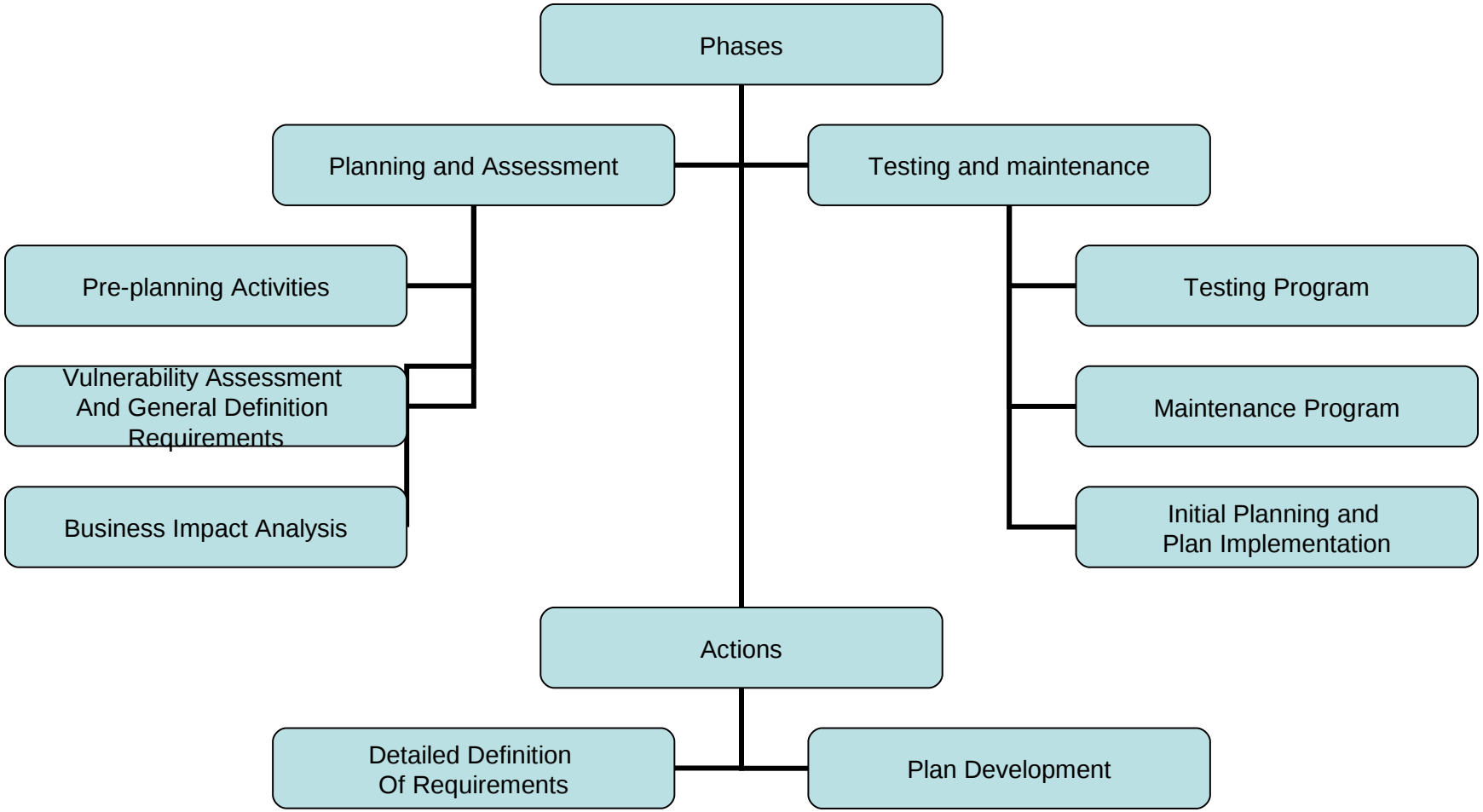
[Primary objective is to minimize losses by minimizing the cost associated with disruption and enable organization to survive the disaster and establish normal business functions]

- Key objectives are
  - Identification of critical business functions
  - Continuation of critical business functions after disaster
  - Minimize duration of serious disruption
  - Provide safety and well being of people at the time of disaster
  - Minimize immediate damage and immediate losses
  - Facilitate effect co-ordination of recovery tasks
  - Establish Management succession and emergency powers
  - Reduce complexity of recovery effort.
- Goals of BCP
  - Identify weakness and develop disaster recovery plan
  - Minimize duration of serious disruption
  - Facilitate effect co-ordination of recovery tasks
  - Reduce complexity of recovery effort

Methodology of BCP emphases on



Phases of BCP



Pre-planning activities

1. Obtain understanding of
    1. Existing and
    2. Projected system's environment of organization
2. This enables us to
    1. Refine the scope of
        1. BCP and
        2. Associated work program
    2. Develop schedules
    3. Identify and address the issues that could have impact on delivery and success of plan

- Two key deliverables are

1. Development of policy to support the recovery program
2. Awareness program to educate the management and senior who will be required to participate in BCP

Vulnerability Assessment and General definition of requirements

- **Its is preferable to**
  - concentrate activities that have the effect of reducing the possibility of disaster occurrence
  - rather than concentrating on minimizing the impact of actual disaster
- **Thus this phase addresses** the measures to reduce the probability of occurrence

- **The tasks undertaken are**

1. Assemble BCP team and conduct awareness program
2. Develop a plan framework
3. Define the scope
4. Analyze and purchase recovery planning and maintenance software
5. A through security assessment of system and communication environment which will enable the BCP team to improve existing emergency plans and disaster prevention plans and implement those which do not exist
6. Present the findings and recommendations to Steering Committee

Business Impact Analysis

- It means a systematically assessing the potential impacts resulting from various incidents
- It is intended to help understand the degree of potential loss that could occur
- This will cover not only direct financial loss but others issues like reputation
- **Ways to obtain information in this phase are**
  - Questionnaires
  - Workshops
  - Interviews
  - Examination of documents

- **The tasks undertaken are**

1. Identify
   1. organizational risk including single point failure and infrastructure risk
   2. critical business processes
   3. dependencies and interdependencies of critical business processes
   4. type and quality of resources required
2. Identify and quantify threats to critical business processes in terms of outage and financial impact
3. Determine maximum allowable downtime for each business process
4. Identify the Determine the impact to organization in event of disaster

Detailed definition requirements

- A profile of recovery requirements is developed
- It is used as a basis for analyzing alternative recovery strategies
- Key deliverables are definition of
  - Plan
  - Scope
  - Objectives and
  - Assumptions

- The profile should include (for each business unit)

1. Hardware
2. Software
3. Documentation
4. Outside support

Plan Development

- The objective is to determine the available options and formulation of appropriate alternative recovery strategies to provide timely recovery for all critical processes and their dependencies
- Organization's recovery strategy has to be developed for recovery of core business processes
- In event of disaster, it is survival and not business as usual

- Recovery strategies are two tired

1. Business
    1. Logistics
    2. Accounting
    3. Human Resource

2. Technical
    1. Information Technology

Testing the plan

- Unless plan is tested on a regular basis, there is no assurance that in the event of disaster the plan is activated and the organization will survive the disaster

- Objectives of BCP tests are

1. Recovery procedure are complete and workable
2. Competence of personnel in their performance can be evaluated
3. Resources are obtainable and operational to perform recovery process
4. Manual recovery process are operational
5. Success or failure of BCP training is monitored

Maintenance Program

- It is critical that existing change management process are revised to take recovery plan maintenance into account
- Where change management does not exist, change management procedures should be recommended and implemented

- The tasks undertaken are

1. Determine ownership and maintenance of BCP
2. Identify BCP maintenance triggers communication of change management
3. Determine
    1. maintenance regime
    2. maintenance process
4. Determine Implement version control procedures so that plan is maintained up-to-date

Testing and Implementation

- Testing largely depends upon recovery strategies
- It is conducted so that written plans are comprehensive and accurate
- Activities for this stage are
  - Defining the test
  - Identifying the test team
  - Structuring the test
  - Conducting the test
  - Analyzing the test results
  - Modifying the plans as appropriate

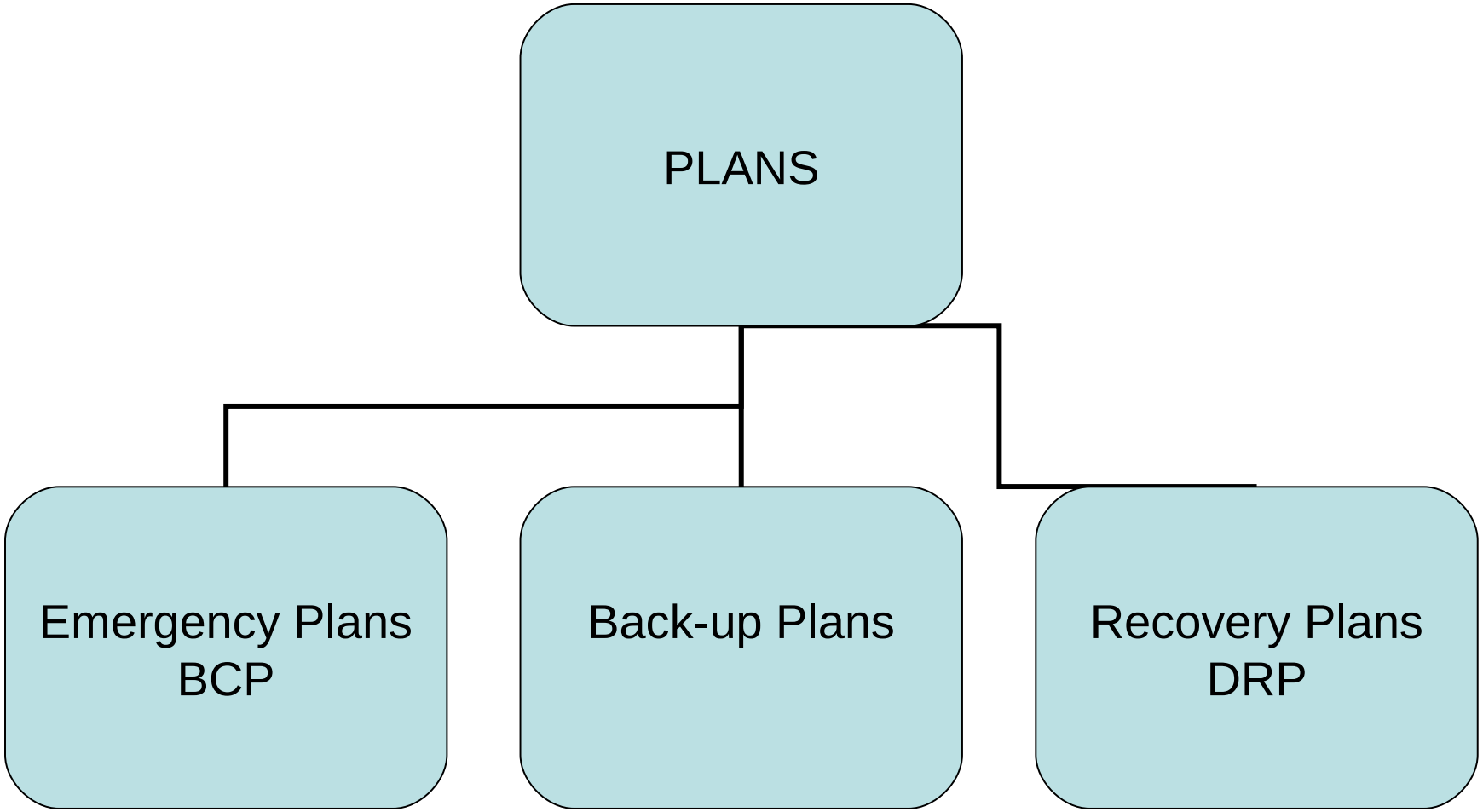
BCP and DRP

Chapter 6.3

Contents

- Types of plans
  - Back-up plans

Types of plans



Back-up Plans

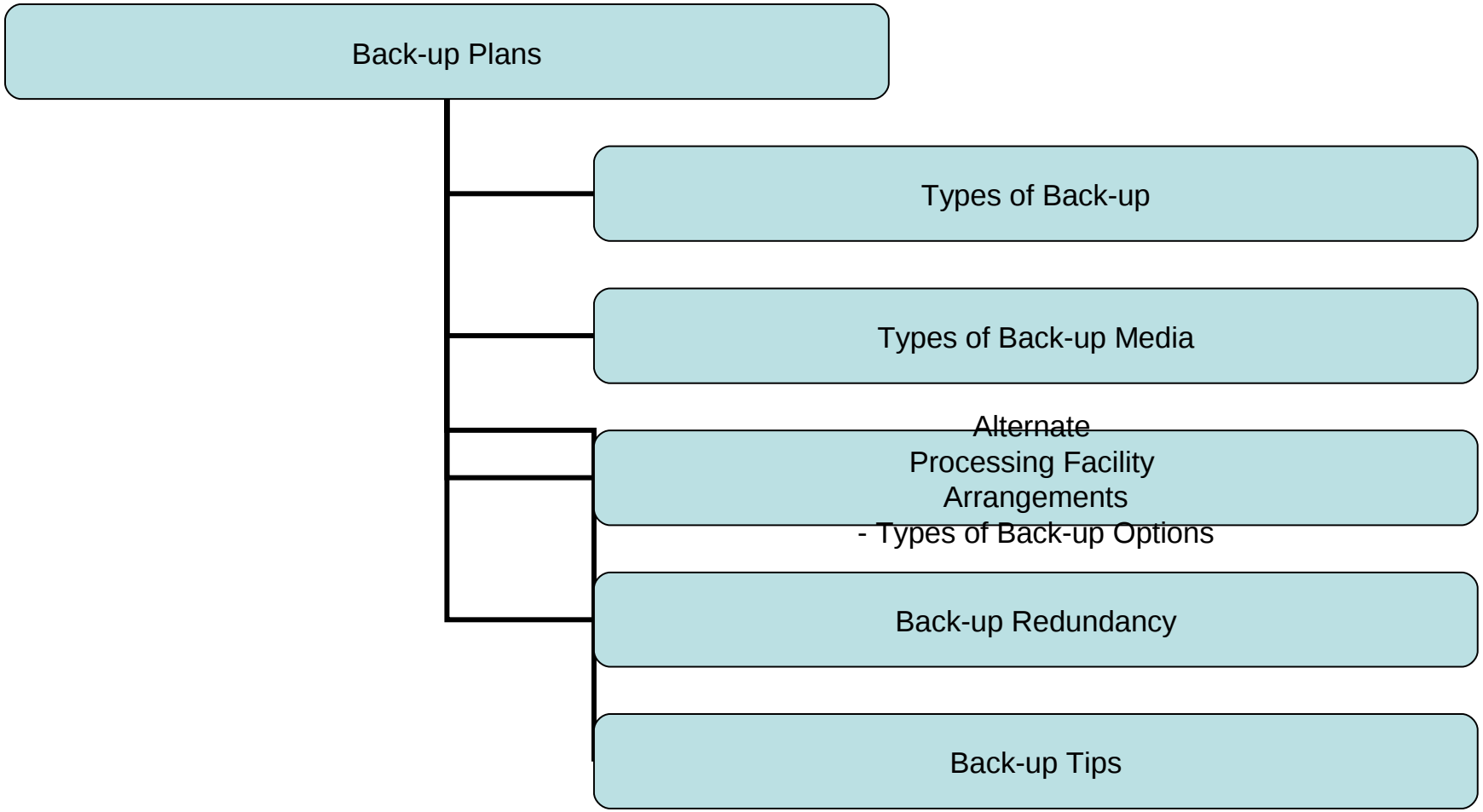
- **It should specify**

1. They type of back-up to be kept
2. Frequency with which back-up is to b undertaken
3. Procedures for making back-up
4. Location of back-up resources
5. Site where these resources can be assembled
6. Personnel responsible for back-up of resources and restarting of operations
7. Priorities to restarting the operations
8. Time frame for recovery

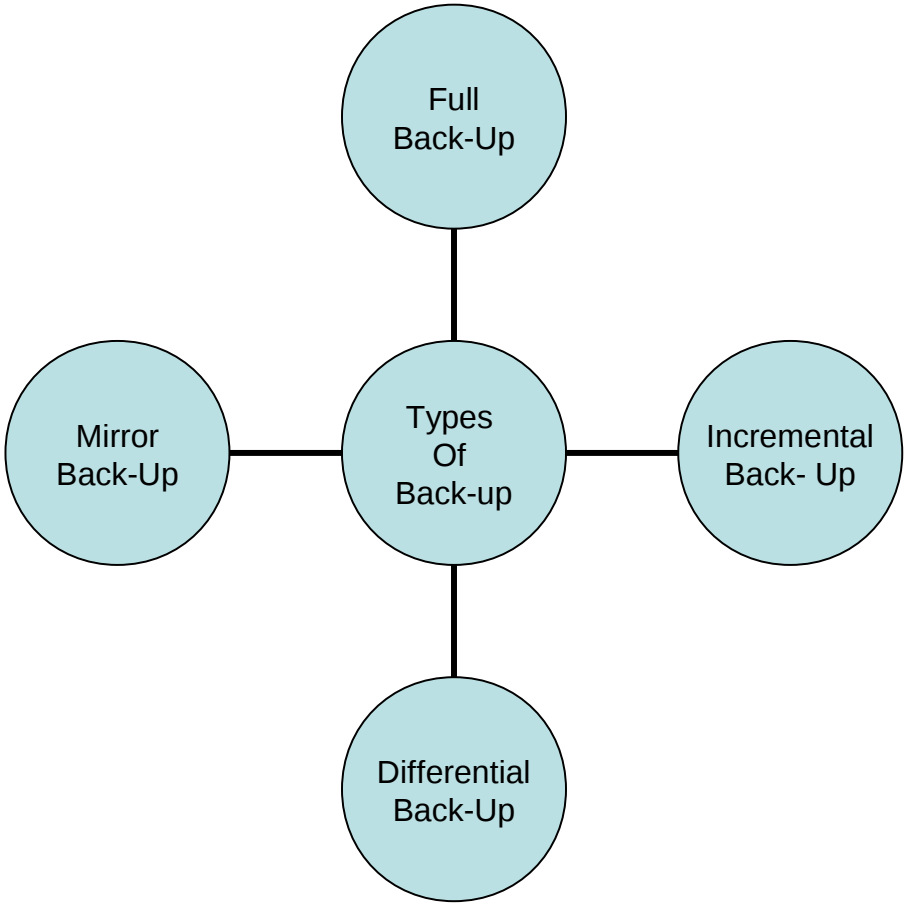
- **Perhaps most critical part is to ensure that all critical resources are backed-up. Some of them are**

1. Hardware and Facilities
    1. *Arrangement with others for provision of*
        1. Hardware
        2. Software
        3. Personnel and their training and rotation of duties
2. Others
    1. *Inventory of those securely stored on-site and off-site like that of*
        1. System software
        2. Files stored
        3. Documentation
        4. Critical supplies
        5. List of vendors who provide all supplies

Back-up Plans



Types of Back-up



Types of System back-up

Full Back-up –

- It captures all files and data
- Every back-up generation contains every file in back-up set
- Amount of time and space prevents its from being realistic proposition for backing up large amount of data

Incremental Back-up –

1. It captures the files that were crated or changed since the last back-up
2. This is most economical and saves lot of back-up time and space
3. However it is difficult to restore since we will have to recover

- Last full back-up and
- Every incremental back-up

Differential Back-up –

1. It stores files that have changed since the last back-up
2. Compared with Full back- up it is faster and economical
3. Restoring has two steps

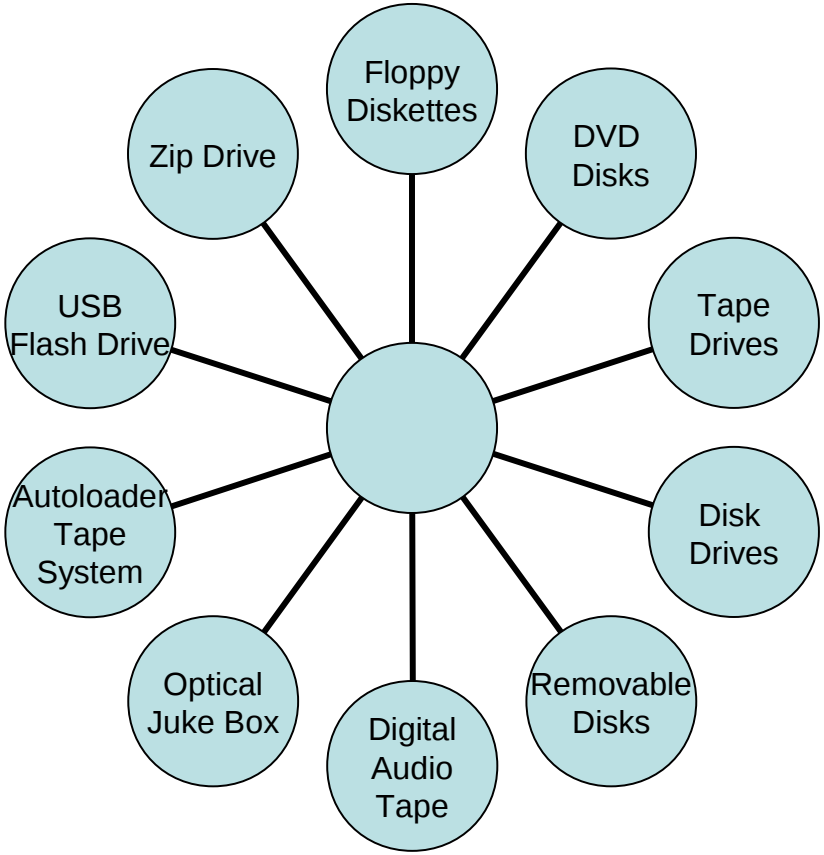
- Restore from the last full back-up
- Restore appropriate differential back-up

1. Downside is that of duplication of files in various differential back-up

Mirror Back-up –

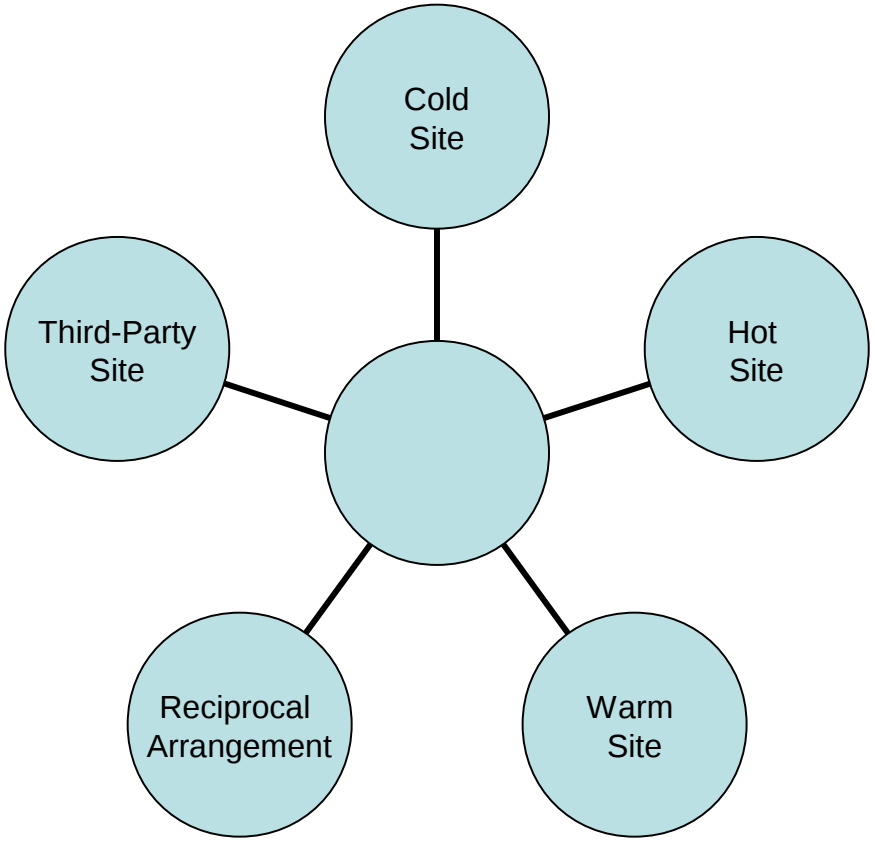
1. It is identical to full back-up
2. But files are not compressed in zip files
3. Hence they cannot be protected by password
4. It is used to create an exact copy of data

Types of Back-up Media



Five fundamental factors that should base you decision in selecting the Back-up Media	
Speed	How fast can you back-up and restore the data using the media type used
Reliability	Can you risk purchasing the media that has reduced reliability to save cost
Capacity	Is the media big enough for your back-up load
Extensibility	If the amount of data grows, will the media support this demand
Cost	Does the solution you want fit into your budget

Alternate Processing Facility Arrangements - Types of Back-up Options to be considered by Security Administrators



Security administrator should consider following alternative processing facility arrangements

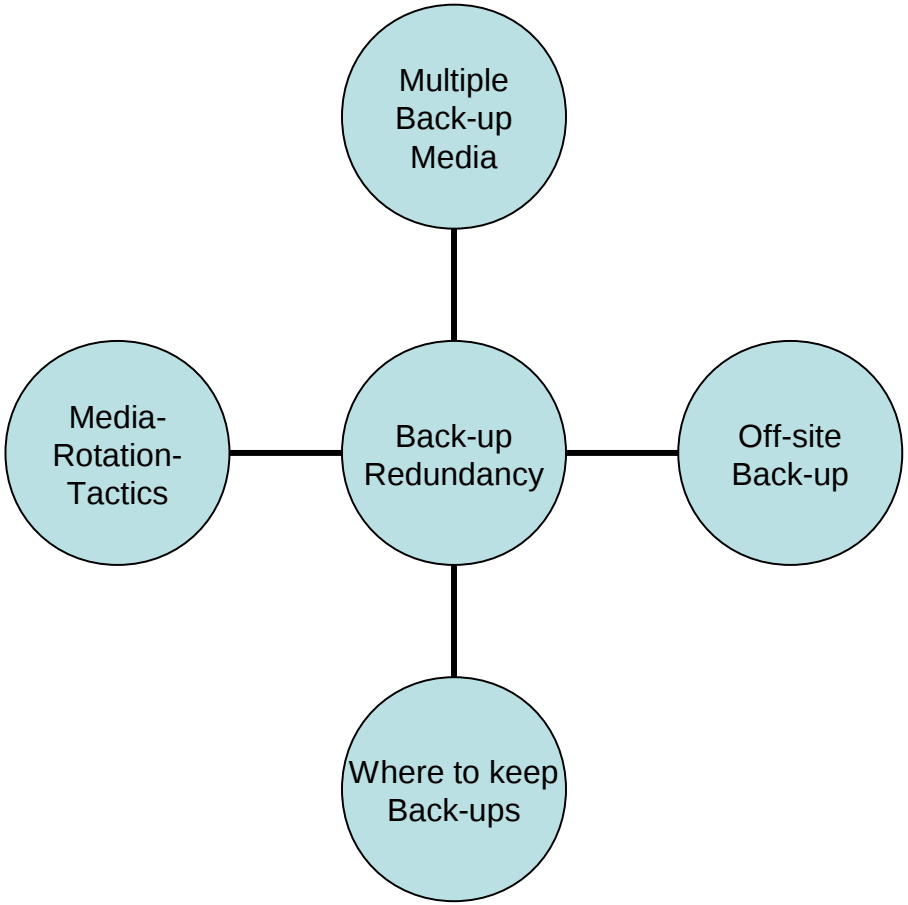
Cold Site – 1. Useful if organization can tolerate some down-time 2. It has all the facilities needed to install a mainframe system 3. An organization can establish its own cold-site facility or can enter into arrangement with another organization to provide cold-site facility	Hot Site – 1. Useful if fast recovery is critical for organization 2. All hardware and operations facilities will be available 3. It is expensive to maintain 4. The are usually shared with other organizations
Warm Site – 1. It provides an intermediate level of back-up 2. It has • All cold site facilities • Also hardware that might be difficult to obtain and install	Reciprocal Arrangement – 1. Two or more organization might agree to provide back-up to each other in the event of one suffering a disaster 2. This option is relatively cheap 3. Each participant has to maintain sufficient capacity to operate another's critical system

If third party sites are used for back-up and recovery purpose

- Security administrator must ensure that a contract covers

1. The period during which the site can be used
2. The conditions under which the site can be used
3. The facilities and services that the site provider agrees to make available
4. Controls that will be placed while working at off-site facility
5. How soon site will be made available subsequent to disaster
6. Number of organization that will be allowed to use the site in the event of disaster
7. The priority to be given to the concurrent users in the event of common disaster

Back-up Redundancy



Back-up Redundancy

Multiple Back-up – 1. For data of high importance it is unacceptable to have a situation of data loss 2. Hence single point of failure should be eliminated	Off Site Back-up – 1. It is done to keep at least one copy of redundant back-up in an alternate location 2. A practical solution would be to take a back-up on removable back-up disk which will be shuttled out of your site into a secure location
Where to keep the Back-Ups – 1. A secure off-site location is the best	Media Rotation Tactics – 1. Rotate the active back-up media with the one of the offsite stored media 2. This will update the offsite media with the latest media changes 3. To reduce the data loss in case of disaster it is recommended to daily switch the active back-up media with the one stored

Back-up Tips

1. Draw up a simple plan of who will do in case of an emergency
2. Be organize as to what was backed-up, when it was backed-up, which media was used
3. Use Volume Shadow Copy service in Windows Server 2003 which allows us to create a point in time copies of data that can be restored and reverted to at any time
4. Select the option of verify the back-up
5. Create a reference point where you know everything is working properly
6. Select the option to restrict data to owner/administrator
7. Set a Domain Group Policy to restrict the Restore privilege to Administrators only
8. Create a step by step guideline clearly outlining the sequence for retrieval and restoration of data.

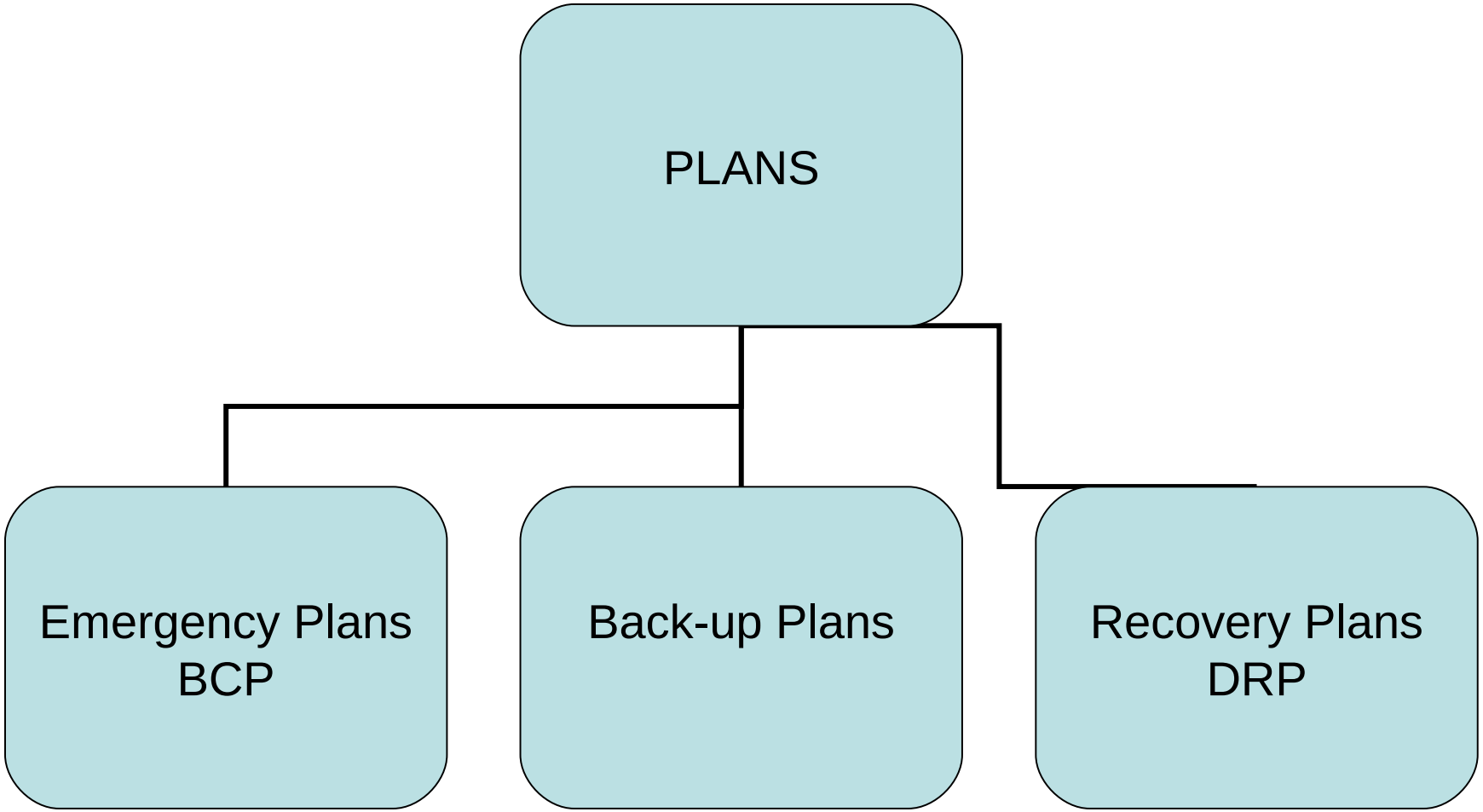
BCP and DRP

Chapter 6.4

Contents

- Types of plans
  - Recovery Plans
  - DRP
  - Testing Methodology
  - Audit tools

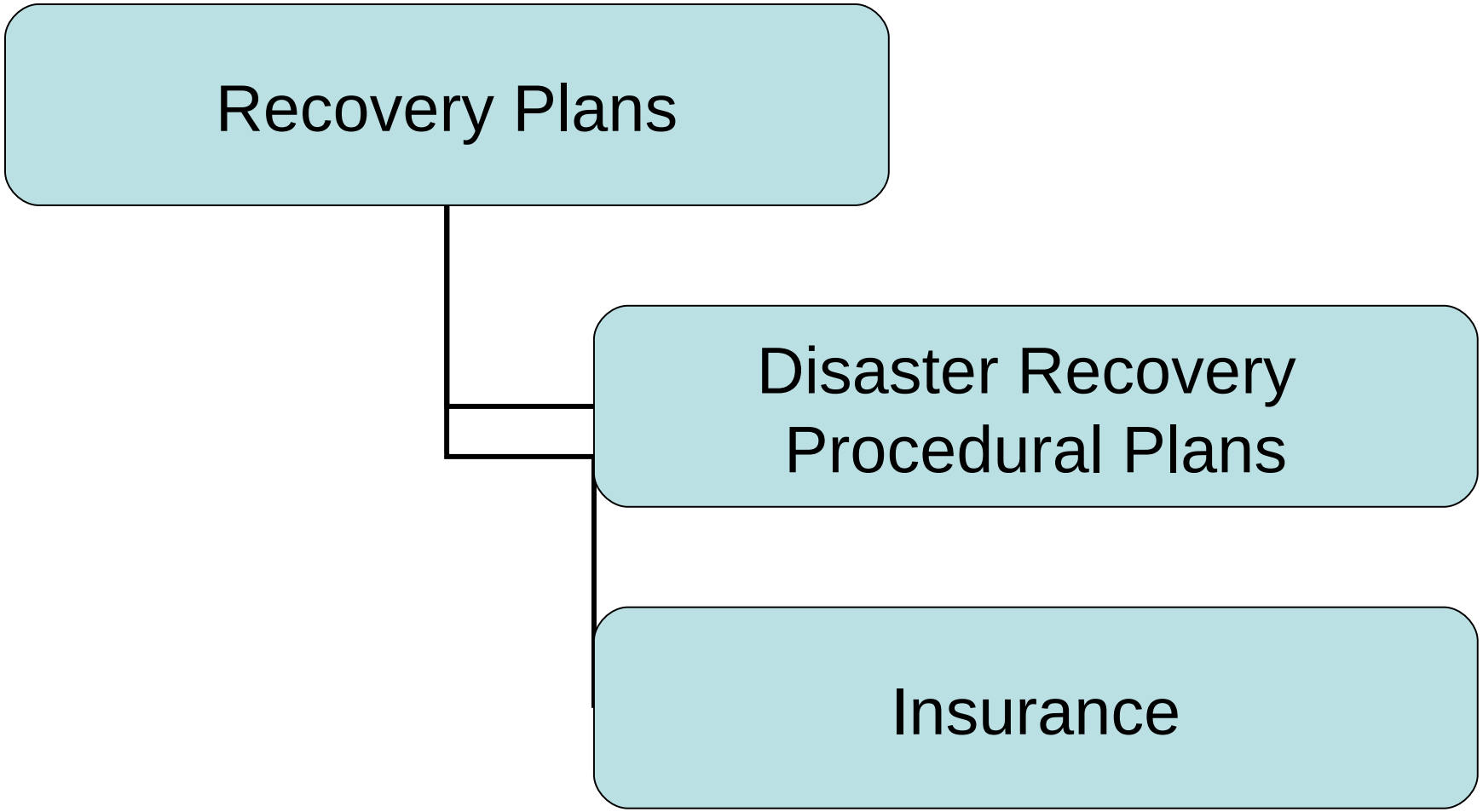
Types of plans



Recovery Plan

- They set out the procedures to restore full information system capabilities
- They identify the recovery committee that will be responsible for working out the specifics
- The plan should specify the responsibilities of the committee and provide a guidelines on priorities to follow
- It might also indicate the applications to be recovered first
- Members of recovery committee must
  - Understand their responsibilities
  - Review and practice by executing their responsibilities
  - Appoint new members and brief them if the old members lave

Recovery Plans

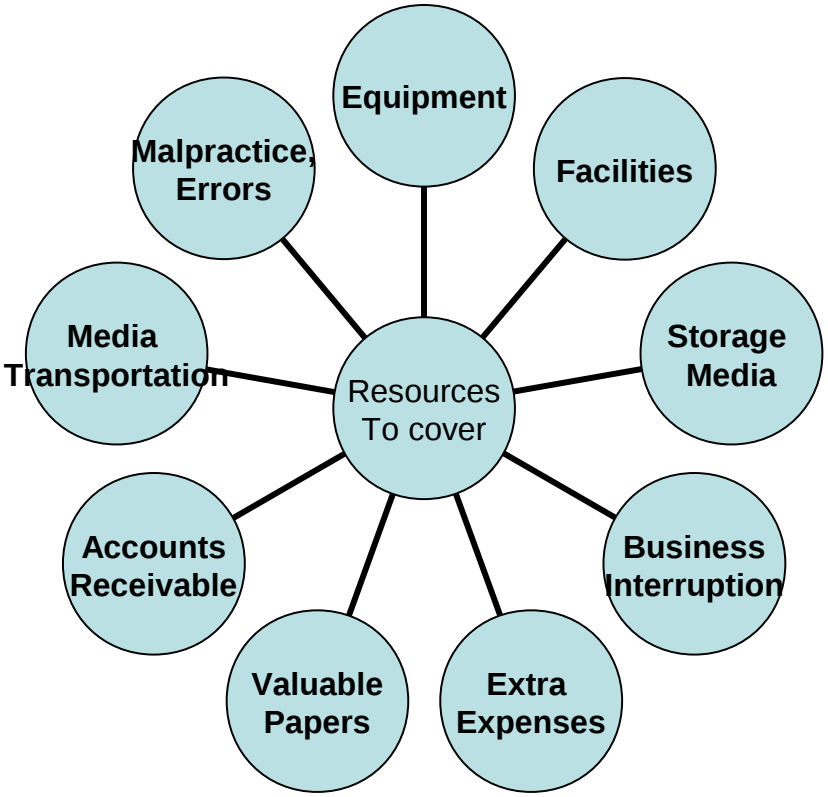


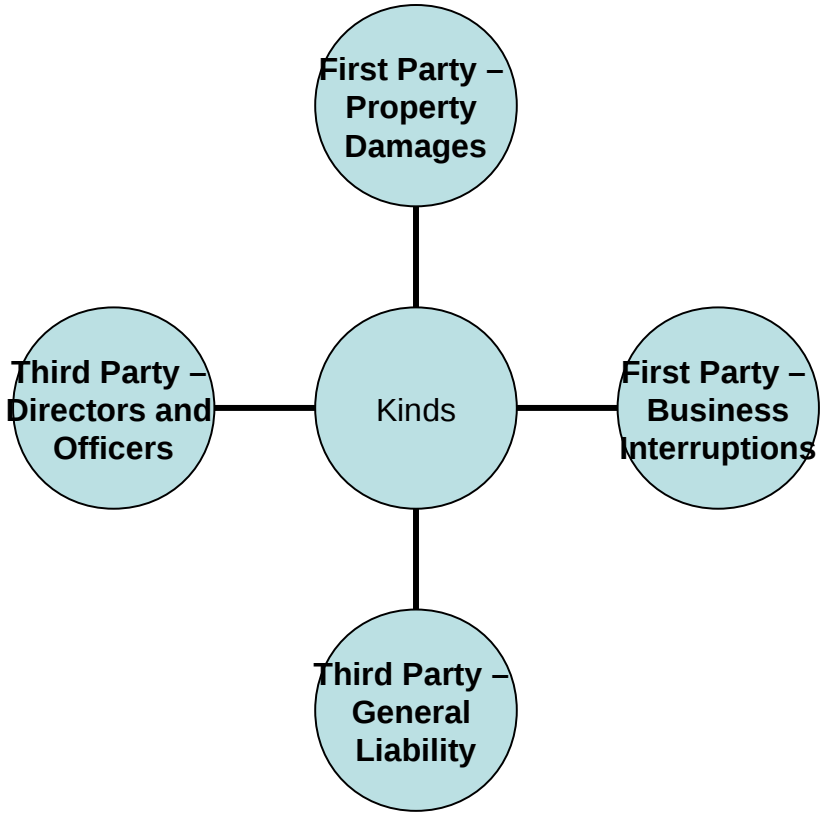
Disaster Recovery
Procedural Plans

- It may include

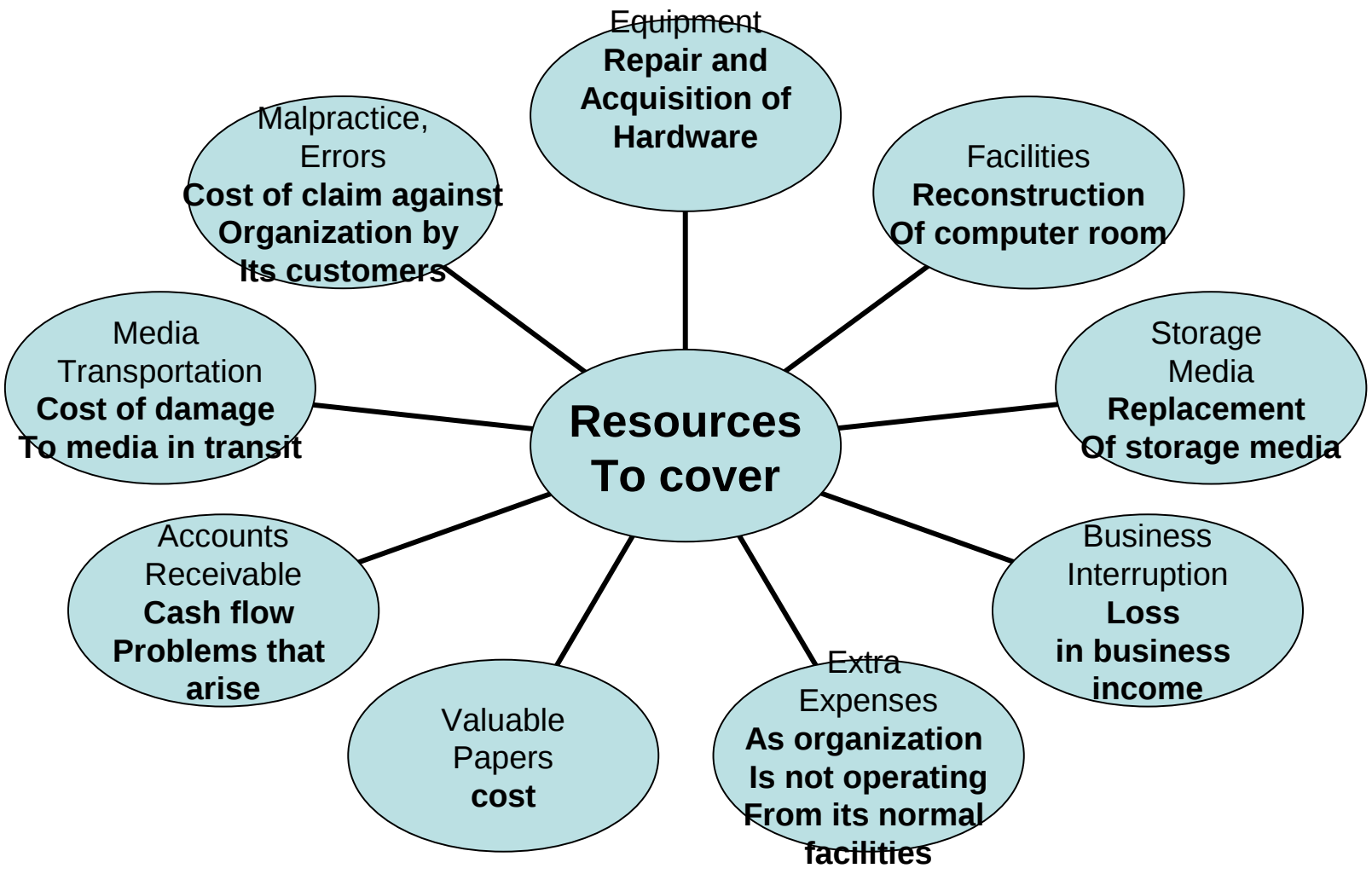
1. Description of purpose and scope
2. Conditions for activating the plan
3. Emergency procedures i.e.
    1. the actions to be taken following the incident
4. Fall back procedures i.e.
    1. the actions to be taken to move essential business activities to alternate temporary locations
5. Resumption procedures i.e.
    1. actions to be taken to return to normal business operations
6. Maintenance schedules
7. Awareness and education activities
8. Responsibilities of individual for executing the plans
9. Emergency phone list
10. Medical procedure to be followed
11. Insurance papers and claim plans
12. Alternate manual procedures

Insurance


Resources To cover
Equipment
Malpractice, Errors
Facilities
Media Transportation
Storage Media
Accounts Receivable
Business Interruption
Valuable Papers
Extra Expenses


Kinds
First Party – Property Damages
Third Party – Directors and Officers
First Party – Business Interruptions
Third Party – General Liability

Insurance


Equipment
Repair and Acquisition of Hardware
Malpractice, Errors
Cost of claim against Organization by Its customers
Facilities
Reconstruction Of computer room
Media Transportation
Cost of damage To media in transit
Resources To cover
Storage Media
Replacement Of storage media
Accounts Receivable
Cash flow Problems that arise
Business Interruption
Loss in business income
Valuable Papers
cost
Extra Expenses
As organization Is not operating From its normal facilities

Kinds of insurance

First Party Insurance – It identifies claims by policy holder against their own insurance	Third Party Insurance – It is designed to protect the policy holders and insurers from the wrong committed by policyholder
First Party Insurance – Property Damages 1. It is designed to protect the insured against the loss and destruction of property 2. It defines loss as/of • Physical injury to or destruction of tangible property • Use of tangible property which has not been physically injured or destroyed 1. They are known as • All risks • Defined Risks • Causality Insurance	Third Party Insurance – General Liability 1. Its is in parts based on legal theory of torts 2. Torts are civil wrongs and of three categories 3. Intentional torts are excluded from the liability of insurance policies and Strict liability torts are covered by specialized liability insurance 4. Generally liability policies include comprehensive and excess liability policies
First Party Insurance – Business Interruptions 1. If insured company fails to perform its contractual obligations because of loss of information system, data or communication, it is liable to customer for breach of contract 2. Hence some business and insurance industry have attempted to mitigate this risk by including information technology in BCP and DRP	Third Party Insurance – Directors and Officers 1. Protection from liability arising from failure to meet appropriate standards of care is Error and Omission Insurance 2. The two common forms are Directors and Officers which is designed to protect the officers as individuals from the liability arising out of the wrongful act committed in course of their duties and they compensate to officer's companies for any losses payable by them 3. The other form is professional laibility

Testing Methodology for Recovery Plans

Hypothetical It is a test exercised to verify •the existence of all procedures and actions specified in DRP and to •Prove the theory of those procedures	**Component** It is the smallest set of instructions within the DRP which enables specific processes to be performed It is designed to verify •the detail and accuracy of individual procedures in DRP and •can be used when no additional system can be made available
Module It is a combination of component The aim is to verify •the validity and functionality of the DRP when multiple components are combined. If one is able to test all modules, even is unable to perform full test, then one can be confident that business will survive	**Full** It verifies each component within the module so as to satisfy the strategy and recovery time objective in DRP Two main objectives are •To confirm the total time elapsed meets the recovery time objective •To prove the efficiency of recovery plan to ensure a smooth flow from module to module

Audit tools for DRP