CHAPTER-4

Business Continuity Planning and Disaster Recovery Planning

Giridhar Dande
G's publiCAtions

key terms related to BCM -B^3

Business Contingency: A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions.

Such an event could be a

power outage,
hardware failure,
fire, or storm.

If the event is very destructive, it is often called a disaster.

BCP Process: BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.

The purpose of BCP is to ensure that vital business functions (critical business operations) are recovered and operationalized within an acceptable timeframe.

The purpose is to ensure continuity of business and not necessarily the continuity of all systems, computers or networks.

The BCP identifies the critical functions of the enterprise and the resources required to support them.

The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and incident response so as to ensure that the proper procedures will be carried out to ensure the timely restoration of services.

Business Continuity Planning (BCP): It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

It is imperative that every enterprise whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the enterprise.

It is not enough that enterprise has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the enterprise.

BCP Manual

A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

BCP is expected to provide:

1. Reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.

2. Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring ‘Continuous availability of all key services to clients.

BCM is business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

1. Proactively improves an enterprise's resilience against the disruption of its ability to achieve its key objectives

2. Provides a detailed method of restoring an enterprise's ability to supply its key products and services to an agreed level within an agreed time after a disruption, and

3. Delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

Advantages of Business Continuity

1. Is able to proactively assess the threat scenario and potential risks

2. Has planned response to disruptions which can contain the damage and minimize the impact on the enterprise, and

3. Is able to demonstrate a response through a process of regular testing and trainings.

BCM policy

Objective of this policy is to provide a structure through which

1.Critical services and activities undertaken by the enterprise operation for the customer will be identified.

2. Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.

3. Invocation of incident management and business continuity plans can be managed.

4. Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updating as required.

5. Planning and management responsibility are assigned to a member of the relevant senior management team.

Objectives and Goals of Business Continuity Planning

The key objectives of the contingency plan should be to:

1. Minimize the duration of a serious disruption to operations and resources (both information processing and other resources). **(G-2)**

2. Continue critical business operations.

3. Provide the safety and well-being of people on the premises at the time of disaster.

4. Minimize immediate damage and losses.

5. Establish management succession and emergency powers.

6. Facilitate effective co-ordination of recovery tasks. **(G-3)**

7. Identify critical lines of business and supporting functions.

8. Reduce the complexity of the recovery effort. **(G-4)**

Goals

Identify weaknesses and implement a disaster prevention program **(G-1).**

Developing a Business Continuity Plan

The methodology gives importance on the following:

1. Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan.

2. Obtaining commitment from appropriate management to support and participate in the effort.

3. Defining recovery requirements from the perspective of business functions.

4. Documenting the impact of an extended loss to operations and key business functions.

5. Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery.

6. Selecting business continuity teams that ensure the proper balance required for plan development.

7. Developing a business continuity plan that is understandable, easy to use and maintain.

8. Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Eight Phases

Phase-1. Pre-Planning Activities (Project Initiation)

used to obtain an understanding of the existing and projected computing environment of the organization.

This enables the project team to:

i. Refine the scope of the project and the associated work program.

ii. Develop project schedules.

iii. Identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase, a Steering Committee should be established.

The committee should have the overall responsibility for providing direction and guidance to the Project Team.

The committee should also make all decisions related to the recovery planning effort.

The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules.

Phase 2 – Vulnerability Assessment and General Definition of Requirements

This phase addresses measures to reduce the probability of occurrence.

This phase will include the following key tasks:

1. A thorough Security Assessment of the computing and communications environment including

physical security;
database security;
data and voice communications security;
systems and access control software security;
security planning and administration;
systems development and maintenance;
application controls; and

operating procedures;
personnel practices;
personal computers;
backup and contingency planning;
insurance.

2. The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and

to implement required emergency plans and disaster prevention measures where none exist.

3. 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.

4. Define the scope of the planning effort.

5. Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.

6. Develop a Plan Framework.

7.Assemble Project Team and conduct awareness sessions.

Phase 3 – Business Impact Assessment (BIA)

Enables the project team to:

1. identify critical systems, processes and functions.

2. assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities.

3. assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee.

This report identifies critical service functions and the timeframes 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.

Phase 4 – Detailed Definition of Requirements

A profile is developed by identifying resources required to support critical functions identified in Phase 3.

This profile should include hardware, software, documentation, outside support, facilities 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.

Phase 5 – Plan Development

During this phase, recovery plans components are defined and plans are documented.

This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations and the definition of Recovery Teams, their roles and responsibilities.

Recovery standards are also being developed during this phase.

Phase 6 – Testing Program

The plan Testing Program is developed during this phase.

Testing 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.

Phase 7 – Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery.

The plans must reflect changes to the environments that are supported by the plans.

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.

Many recovery software products take this requirement into account.

Phase 8 – Initial Plan 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 – **(DI-SCAM)**

o **D**efining the test purpose/approach;
o **I**dentifying test teams.
o **S**tructuring the test.
o **C**onducting the test.
o **A**nalyzing test results.
o **M**odifying the plans as appropriate.

Components of BCM Process – 5 STAGES

BCM – Information Collection Process
BCM – Strategy Process
BCM – Development and Implementation Process
BCM – Testing and Maintenance Process
BCM – Training Process

BCM Information Collection Process – STAGE-1

- Business Impact Analysis (BIA)
- Classification of Critical Activities
- Risk Assessment

The pre-planning phase of Developing the BCP also involves collection of information.

It enables us to refine the scope of BCP and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan.

Two other key deliverables of that phase are:

the development of a policy to support the recovery programs; and

an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

The process used for the development of both Business Impact Analysis and the Risk Assessment

Both the BIA and Risk Assessment will be reviewed as part of the annual BCM management review or following a change to the operation, its processes or associate risks.

Business Impact Analysis (BIA)

BIA is essentially a means of systematically assessing the potential impacts resulting from various events or incidents.

The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services.

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.

For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

assess	-the impacts that would occur if the activity was interrupted over a period of time. -the minimum level at which the activity needs to be performed on its resumption.
identify	-the maximum time period after the start of an interruption within which the activity needs to be resumed. -critical business processes. -the length of time within which normal levels of operation need to be resumed. -any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

Classification of Critical Activities – if possible see Study Material

BCP leader and BCP team leaders in consultation with respective function owner shall carry out BIA for infrastructure and business transactions.

BIA will result in

business categorization (like Vital, Desirable and Essential)
disaster scenarios (Catastrophic, major, minor trivial)

for various disaster causes (fire, flood, system failure etc.),

Risk Assessment

The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as

people,
process,
technology,
information,
infrastructure supplies and stakeholders.

The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality.

It is the decision of the enterprise to select a risk assessment approach, but it is important that it is suitable and appropriate to address all of the enterprise's requirements.

Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.

Vulnerabilities might occur as weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.

The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist.

This is similar to vulnerability assessment phase of developing a BCP.

As a result of the BIA and the risk assessment, the enterprise should identify measures that:

- reduce the likelihood of a disruption
- shorten the period of disruption
- limit the impact of a disruption on the enterprise's key products and services.

BCM Strategy Process – STAGE-2

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources.

For example, one common preparation is to establish procedures for backing up files and applications.

Another is to establish contracts and agreements, if the contingency strategy calls for them.

Existing service contracts may need to be renegotiated to add contingency services.

Another preparation may be to purchase equipment, especially to support a redundant capability.

The enterprise may adopt any strategy but it should take into account the implementation of appropriate measures to reduce the likelihood of incidents and/ or reduce the potential impact of those incidents and resilience and mitigation measures for both critical and non-critical activities.

BCM Development and Implementation Process – STAGE-3

The enterprise should have an exclusive organization structure,

Incident Management Team / Crisis management team

for an effective response and recovery from disruptions. In the event of any incident, there should be a structure to enable the enterprise to: **C^5**

- **c**onfirm Impact of incident
- **c**ontrol of the situation
- **c**ontain the incident
- **c**ommunicate with stakeholders
- **c**oordinate appropriate response.

The Incident Management Plan (IMP)

To manage the initial phase of an incident, the crisis is handled by IMP.

The IMP should have top management support with appropriate budget for development, maintenance and training.

They should be flexible, feasible and relevant; be easy to read and understand; and provide the basis for managing all possible issues, including the stakeholder and external issues, facing the enterprise during an incident.

The Business Continuity Plan (BCP)

To recover or maintain its activities in the event of a disruption to a normal business operation, the BCP are invoked to support the critical activities required to deliver the enterprise's objectives. They may be invoked in whole or part and at any stage of the response to incident.

The recovery strategies may be two-tiered:

1.Business: Logistics, accounting, human resources, etc.

2.Technical: Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).

The plan development phase also includes the implementation of changes to use procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of recovery teams, their roles and responsibilities.

Recovery standards are also developed during this phase.

The organization's recovery strategy needs to be developed for the recovery of the many business processes.

BCM Implementation

Repeat phase-8 – if you have doubt plz check the study material.

BCM Testing and Maintenance Process – STAGE- 4

BCM Testing

A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation.

Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovative solutions.

BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.) and technology and telecommunications recovery, including the availability and relocation of staff.

The frequency of testing should depend upon both the enterprise's needs, the environment in which it operates, and stakeholder requirements.

However, the testing program should be flexible, taking into account the rate of change within the enterprise, and the outcome of previous one.

In addition, it might lead to the improvement of BCM capability by:

1. Practicing the enterprise's ability to recover from an incident.

2. Verifying that the BCP incorporates all enterprise critical activities and their dependencies and priorities.

3. Highlighting assumptions, which need to be questioned.

4. Injecting confidence amongst exercise participants.

5. Raising awareness of business continuity throughout the enterprise by publicizing the exercise.

6. Validating the effectiveness and timeliness of restoration of critical activities.

7. Demonstrating competence of the primary response teams and their alternatives.

In case of Development of BCP, the objectives of performing BCP tests are to ensure that:

1. The recovery procedures are complete and workable.

2. The competence of personnel in their performance of recovery procedures can be evaluated.

3. There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.

4. The manual recovery procedures and IT backup system/s are current and can either be operational or restored.

5. The success or failure of the business continuity training program is monitored.

BCM Maintenance

BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program.

the key people who are to implement the BCM strategy and plans are trained and competent.

the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

Similarly, the maintenance tasks undertaken in Development of BCP are to:

Determine	- the ownership and responsibility for maintaining the various BCP strategies within the enterprise. - the maintenance regime to ensure the plan remains up-to-date. - the maintenance processes to update the plan.

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.
Implement	-version control procedures to ensure that the plan is maintained up-to-date

Reviewing BCM Arrangements

An audit or self-assessment of the enterprise's BCM program should verify that:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy.

enterprise's	-BCM policy, strategies, framework and plans accurately reflect its priorities and requirements. -BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident. -BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise. -BCM maintenance and exercising programs have been effectively implemented. -has an ongoing program for BCM training and awareness
BCM	-strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program. -procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities.

-Change control processes are in place and operate effectively.

BCM Training Process – STAGE- 5

An enterprise with BCM uses training as a tool to **initiate a BCM culture** in all the stakeholders by:

-Developing a BCM program more efficiently.

-Providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions.

-Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels.

-Minimizing the likelihood and impact of disruptions.

Development of a BCM culture is supported by: - **(LAASE)**

-**L**eadership from senior personnel in the enterprise
-**A**ssignment of responsibilities
-**A**wareness raising
-**S**kills training
-**E**xercising plans.

Training, Awareness and Competency

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined.

These are consistent with the competencies required by the organization of the relevant role and are given as follows:

1.Actively listens to others, their ideas, views and opinions;
2.Provides support in difficult circumstances.
3.Responds constructively to difficult circumstances.
4.Adapts leadership style appropriately to match the circumstances.
5.Promotes a positive culture of health, safety and the environment.
6.Recognizes and acknowledges the contribution of colleagues.
7.Encourages the taking of calculated risks, and actively responds to new ideas.
8.Consults and involves team members to resolve problems.
9.Demonstrates personal integrity.
10.Challenges established ways of doing things to identify improvement opportunities.

Types of Plans - EBRT

There are various kinds of plans that need to be designed.

Emergency Plan	Back-up Plan	Recovery Plan	Test Plan

Emergency Plan

The emergency plan specifies the actions to be undertaken immediately when a disaster occurs.

Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack.

The actions to be initiated can vary depending on the nature of the disaster that occurs.

If an enterprise undertakes a comprehensive security review program(CSRP), the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, **four** aspects of the emergency plan must be articulated.

First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'.	**Second**, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.	**Third**, any evacuation procedures required must be specified.	**Fourth**, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated.

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.

For example
microcomputer users might be advised to make backup copies of critical files and store them off site.

In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain.

For example

it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire.

The backup plan needs continuous updating as changes occur.

For example
as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly.

Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs.

Recovery Plan

The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities.

Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken.

The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed and might also indicate which applications are to be recovered first.

Members of a recovery committee must understand their responsibilities.

Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur.

If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

Test Plan

The final component of a disaster recovery plan is a test plan.

The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster.

It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory.

Periodically, test plans must be invoked.

Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted.

They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a phased approach can be adopted.

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

Types of Back-ups – FIDM

Full Backup	Incremental Backup	Differential Backup	Mirror Backup

Full Backup

A Full Backup captures all files on the disk or within the folder selected for backup.

With a full backup system, every backup generation contains every file in the backup set.

At each backup run, all files designated in the backup job will be backed up again.

This includes files and folders that have not changed.

It is commonly used as an initial or first backup followed with subsequent incremental or differential backups.

After several incremental or differential backups, it is common to start over with a fresh full back up again.

Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space.

The Windows operating system lets us to copy a full back up on several DVD disks.

Any good backup plan has at least one full backup of a server.

For example - Suppose a full backup job or task is to be done every night from Monday to Friday.

The first backup on Monday will contain the entire list of files and folders in the backup job.

On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

Advantages	Dis-Advantages
1. Restores are fast and easy to manage as the entire list of files and folders are in one backup set. 2. Easy to maintain and restore different versions.	1.Backups can take very long as each file is backed up again every time the full backup is run. 2. Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

Incremental Backup

An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type.

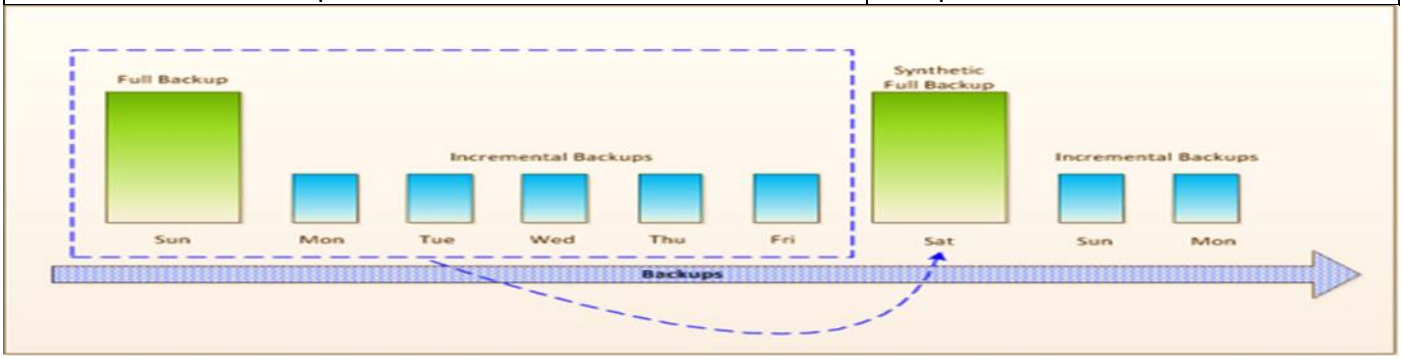
The last backup can be a full back up or simply the last incremental backup.

With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

For example

Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full back up since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Advantages	Dis-Advantages
1. Much faster backups 2. Efficient use of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.	1. Restores are slower than with a full back up and differential backups. 2. Restores are a little more complicated.



Differential Backup

Differential backups fall in the middle between full backups and incremental backup.

A Differential Backup stores files that have changed since the last full backup.

With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up.

Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation:

Restoring from the last full back up; and then restoring the appropriate differential backup.

The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

For example

Suppose a differential backup job or task is to be done every night from Monday to Friday.

On Monday, the first backup will be a full back up since no prior backups have been taken.

On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders.

On Wednesday, the files changed and files added since Monday's full backup will be copied again.

While Wednesday's backup does not include the files from the first full back up, it still contains the files backed up on Tuesday.

Advantages	Dis-Advantages
1. Much faster backups then full backups. 2. More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run. 3. Faster restores than incremental backups.	1. Backups are slower then incremental backups. 2. Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup. 3. Restores are slower than with full backups and are a little more complicated than full backups but simpler than incremental backups.

Mirror back-up

Mirror backups are, as the name suggests, a mirror of the source being backed up.

With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup.

Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well.

Some do not consider a mirror to be a backup.

Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password.

A mirror backup is most frequently used to create an exact copy of the backup data.

For example

Many online backup services offer a mirror backup with a 30 day delete.

This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted.

This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive.

Many backup software utilities do provide support for mirror backups.

Advantages	Dis-Advantages
The backup is clean and does not contain old and obsolete files.	There is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.

Alternate Processing Facility Arrangements -CHWR

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.

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 in addition to the hardware that might be difficult to obtain or install.

For example

a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

Reciprocal Agreement

Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster.

This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

If a 3rd-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

1. how soon the site will be made available subsequent to a disaster.

2. the number of organizations that will be allowed to use the site concurrently in the event of a disaster.

3. the priority to be given to concurrent users of the site in the event of a common disaster.

4.the period during which the site can be used.

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

6.the facilities and services the site provider agrees to make available.

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

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

- Identification and prioritization of the activities, which are essential to continue functioning.

- Operations managers and key employees participated in the development of the plan.

The plan	-is based upon a BIA that considers the impact of the loss of essential functions. -identifies the resources that will likely be needed for recovery and the location of their availability. -is simple and easily understood so that it will be effective when it is needed. -is realistic in its assumptions.

Information Technology

Determine	-if the plan reflects the current IT environment. -if the plan includes prioritization of critical applications and systems. -if the plan includes time requirements for recovery of each critical system, and that they are reasonable. -if a testing schedule exists and is adequate. -if weaknesses identified in the last tests were corrected.

Verify the date of the last test.

Is there a plan for alternate means of data transmission if the computer network is interrupted?

Has the security of alternate methods been considered?

Does the business resumption plan include arrangements for emergency telecommunications?