The Institute of Cost Accountants of India

INFORMATION SYSTEM SECURITY AUDIT

BATCH: 5

DISSA
INFORMATION SYSTEM SECURITY AUDIT

Elocutionist: Dr. Saurabh Maheshwari

Chapter - 3

BUSINESS CONTINUITY AND DISASTER RECOVERY

WHAT IS BCP OR DRP?

Technically the Business Continuity Plan (BCP) refers to how the loss of business may be avoided and it ought to define the business requirements for the continuity of operations. And the Disaster Recovery Plan (DRP) deals with restoring computer systems with all attendant software and connections to full functionality under various damaging or interfering external conditions.

WHY A BCP OR DRP?

- Manage the risks which could lead to disastrous events.
- Reduce the time taken to recover when an incident occurs and
- Minimize the risks involved in the recovery process.
- Reduce the costs involved in reviving the business from the incident.
- Reduce the likelihood of a disruption occurring that affects the business through a risk management process.
- Enhances the organization’s ability to recover following a disruption to normal operating conditions.
- Minimize the impact of that disruption, should it occur.
- Protect staff and their welfare and ensure staff knows their roles and responsibilities.
- Tackle potential failures within the organization’s Information System Environment
- Protect the business.
- Preserve and maintain relationships with customers.
- Mitigate negative publicity.
- Safeguard the organization’s market share and/or competitive advantage.
- Protect the organization’s profits or revenue and avoid financial losses.
- Prevent or reduce damage to the organization’s reputation and image.

KEY TERMS

- BCP – Business Continuity Planning: A documented collection of procedures and information that is developed compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level.
- DRP – Disaster Recovery Plan: disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
- BIA – Business Impact Analysis: A business analysis is a structured process your organization uses to determine and evaluate the potential impacts of an interruption to critical business operations, due to disasters, accidents or emergencies.
- MBCO – Minimum Business Continuity Objective: This refers to the minimum level of services and/or products that is acceptable / required to the organization to achieve its business objectives during an incident, emergency or disaster.
- MAO – Maximum Acceptable Outrage: This refers to the maximum period of time that an organization can tolerate the disruption of a critical business function, before the achievement of objectives is adversely affected. MAO is also known as Maximum Tolerable Outage (MTO), Maximum Allowable Downtime (MAD).
- IR Plan – Incident Response Plan: IR Plan includes tasks like incident planning, incident detection, incident reaction, incident recovery etc. Incident Response plan gives an entity a set of procedures and guidelines that is needed by an entity to handle an incident.
- Recovery Time Objective (RTO): The pre-determined time at which a product, service, or activity must be resumed, or resources must be recovered
- Recovery Point Objective (RPO): Maximum data loss, i.e., minimum amount of data used by an activity that needs to be restored
- Resilience: The ability of an organization to resist being affected by the incident.

BCP

- Phases of BCP
  - Business Impact Analysis
  - Risk Assessment
  - Planning & Design of BCP
  - Testing of BCP
  - Training of Staff
  - Maintenance of BCP
- After all phases are executed properly, a BCM manual is prepared for future reference.
- 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. A BCP manual consists of the Business Continuity Plan and the Disaster Recovery Plan. The primary objective of preparing the BCP manual is to provide reasonable assurance to senior management of the organization about the capability of the organization to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact. Further, the BCP should be comprehensive and 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. The BCP Manual is expected to specify the responsibilities of the BCM team.

TESTING OF BCP

- Desk Test
- Structural Walkthrough
- Simulation Test
- Parallel Test
- Full Interruption Test [Acid Test / Mock Drill]

DRP

Phases of DRP

- Crises Phase: This phase is under the overall responsibility of the Incident Control Team (ICT). It comprises the first few hours after a disruptive event starts or the threat of such an event is first identified
- Emergency Response Phase: This phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the crisis Phase if there has been one, or when a potentially threatening situation is identified. During the Emergency Response Phase, the Business Continuity Team (BCT) will assess the situation; and decide if and when to activate the BCP.
- Recovery Phase: The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate. During the recovery phase, essential operations will be restarted (this could be at temporary premises) by one or more recovery teams using the BCP; and the essential operations will continue in their recovery format until normal conditions are resumed.
- Restoration Phase: This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the restoration phase, any damage to the premises and facilities will be repaired.

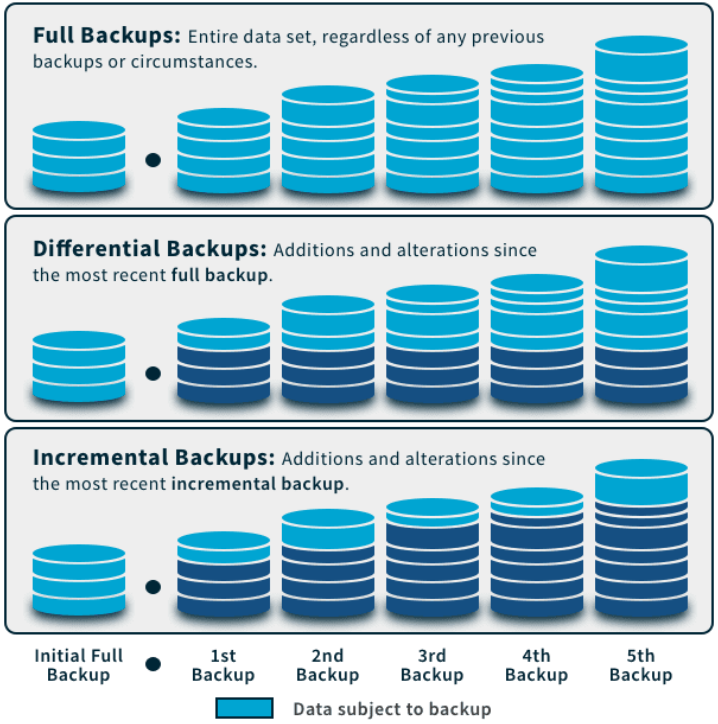
TYPES OF BACKUP AND RECOVERY SITES

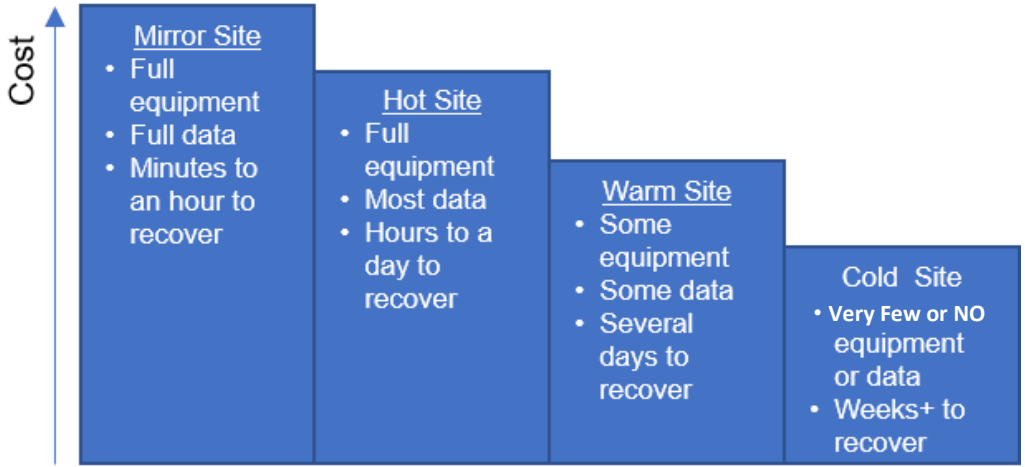
Types of Backup

- Full Backup
- Incremental Backup
- Differential Backup
- Mirror Backup

Recovery Sites

- Mirror Site
- Hot Site
- Warm Site
- Cold Site
- Reciprocal Site
- Outsources Site


Full Backups: Entire data set, regardless of any previous backups or circumstances.
Differential Backups: Additions and alterations since the most recent full backup.
Incremental Backups: Additions and alterations since the most recent incremental backup.
Initial Full Backup
1st Backup
2nd Backup
3rd Backup
4th Backup
5th Backup
Data subject to backup


Cost
Mirror Site
• Full equipment
• Full data
• Minutes to an hour to recover
Hot Site
• Full equipment
• Most data
• Hours to a day to recover
Warm Site
• Some equipment
• Some data
• Several days to recover
Cold Site
• Very Few or NO equipment or data
• Weeks+ to recover

DOCUMENTATIONS

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities are undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plan;
- SLA with alternate site/mirror site with switchover plans;
- Change control, preventative action, corrective action, document control, and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training Program

10 CHALLENGES IN BUSINESS CONTINUITY MANAGEMENT AND HOW TO OVERCOME THEM

1. **Some business unit heads may not completely understand what a process is.**
   The best way to address this is to look at the organizational procedures or website of the particular business unit and go to the BIA interview or meeting with a prior understanding of the high-level processes. This will make the discussion process-focused
2. **Impacts are not captured properly and priorities are misjudged.**
   Often the first BIA does not go to plan and it may be a good idea to repeat the BIA at least once soon after the first attempt. After the first round, there will be a much better understanding of the processes, applications, and other resources, as well as their interdependencies. This will enable a focused discussion in the second round.
3. **Interdependency may not be captured in the first round of BIA.**
   The best way to address this is to talk about “what happens next” and “what happens before.”
4. **Common applications and online systems such as the intranet, file storage, and email can be easily missed in a BIA where ownership is not defined.**
   This needs to be captured by asking intelligent questions or with the discussion within the IT section.

… … CONTD

5. **In general, finding an impact on revenue or profit is difficult unless it is a retail sales process.**
   Having financial details and budgetary information and analyzing them prior to a BIA discussion will be useful to help the business unit estimate the financial impacts, especially on revenue or profit.
6. **Interpolation and extrapolation often cause difficulties.**
   Simplification is often necessary for this area. For example, consider impacts for one day or three days, depending on the overall organizational criticality. If overall impacts are high, select a shorter duration such as one day. If impacts are low, choose three or five days. It is easier for the business unit to assess what the impacts would be if their unit shuts down for two days than it is for the business unit to estimate the impact as time changes. After assessing the impact for a particular duration, then interpolation and extrapolation could be done using mathematical formulae or otherwise. However, such interpolation and extrapolation (linear or non-linear) need to be realistic and validated by the business unit.
7. **Key man dependency is something used by the staff as a weapon to address job security.**
   The BIA should identify this risk, but addressing it may well be challenging in small functional areas.

… … CONTD

8. **Single points of failure should be identified in the BIA using the resources that are required for a particular process.**
   The identification of single points of failure can be difficult and asking questions such as “What do you use for this?” or “What are your dependencies?” could be helpful. This should be followed by a risk assessment to further understand single points of failure and their hidden components.
9. **The final review of the business impact analysis should have a good distribution of the priority of processes.**
   Although there is no specific limit defined, and the levels of criticality could vary, it is ideal to have four-five levels of criticality, with the top priorities not exceeding 25%. Anything more than that will not result in the processes being effectively restored (or exercised) as the focus will be lost.
10. **It is important not to spoil the relationship with the business units as the BIA is only the first step in the business continuity process.**
    The support of business units is essential in a successful business continuity implementation. In some cases, if an agreement cannot be reached about prioritization, some tactics need to be used.

SECURITY OF BCP/DRP PLAN

- Secrecy of plan documentation
- Secrecy of recovery sites
- Rights of backup and recovery execution
- Securing ‘Data Vaults’
- Avoiding exposure to SPOF
- Keeping ‘Version Control’

AUDITING BCP/DRP

In a BCP / DRP Audit, the IS auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for the continuity of business operations and IS processing in the event of a disruption.

The BCP / DRP review aims to assess the organization's ability to continue all critical operations during a contingency and recover from a disaster / interruption within the defined critical recovery period.

IS Auditor is expected to identify residual risks which are not identified and provide recommendations to mitigate them. A BCP / DRP audit also assesses the plan of action for each type of expected contingency and its adequacy in meeting contingency requirements.

The BCP / DRP of an organization is also to be reviewed to a limited extent for the assessment of an auditee organization from the perspective of going concerned.

OPPORTUNITIES FOR AN IS AUDITOR

- Management Consultancy Services in providing guidance in drafting of a BCP/DRP
- Management Consultancy Services in designing and implementing a BCP/DRP
- Designing Test Plans and Conducting Tests of the BCP/DRP
- Consultancy Services in revising and updating the BCP/DRP
- Conducting Pre-Implementation Audit, Post Implementation Audit, General Audit of the BCP/DRP
- Consultancy Services in Risk Assessment and Business Impact Analysis
- You can be involved in any/all areas of BCP implementation or review

ISO 22301 : 2019

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise. The requirements specified in ISO 22301 are generic and intended to apply to all organizations (or parts thereof), regardless of the organization’s type, size, and nature. The extent of application of these requirements depends on the organization's operating environment and complexity. The new structure of ISO 22301 is organized into the following main clauses:

- Normative references
- Terms and definitions
- Context
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

SUMMARY

Business continuity planning is the process of preparing for the unexpected. The result is a plan to respond to partially or completely interrupted access to information and information technology initiated by various causes such as natural disasters, accidents, equipment failures, or malicious activity. The goal is to ensure the availability of critical information resources and the continuity of operations. Information and IT-related business continuity plan should be based on risk and focus on key information and information technology assets in the context of business needs. Business continuity planning will promote the rapid recovery of the university in the face of an adverse event, minimize the impact of such events, and improve the organization’s ability to cope with the unexpected.

Two-thirds of the Earth is covered with Water and the rest one-third is covered with Auditors from different verticals evaluating the business operations from different angles.

- Dr. Saurabh Maheshwari

THANKS!

Any questions?