**Chapter 3 - Business Continuity Planning**

* Business continuity activities are typically strategically focused at a high level and center themselves on business processes and operations.
* Disaster recovery plans tend to be more tactical and describe technical activities such as recovery sites, backups, and fault tolerance.
* The top priority of BCP and DRP is always people. The primary concern is to get people out of harm’s way; then you can address IT recovery and restoration issues.
* The BCP process has four main steps:

■ Project scope and planning

■ Business impact analysis

■ Continuity planning

■ Approval and implementation

* Project Scope and Planning
  + **Organizational Review** - Identify core services, critical departments, key individuals and senior executives responsible. Lays the foundation for forming the BCP team and remainder of the BCP process.
  + **BCP Team Selection** - should include (functional and representative) members from all departments
  + **Resource Requirements** - it needs to be finalized for training and periodic drills
  + **Legal and Regulatory Requirements** - Any legal or contractual requirement from govt or client which needs to be adhered
* Business Impact Analysis
  + **Identifying Priorities** - create a comprehensive list of critical business functions and rank them in order of importance. Qualitative and Quantitative analysis can be used for prioritizing. Key terms used in quantitative analysis are
    - MTD / MTO - Maximum Tolerable Downtime/ Outage is the maximum length of time a business function can tolerate a disruption before suffering irreparable harm
    - RTO - The recovery time objective (RTO) is the amount of time in which you think you can feasibly recover the function in the event of a disruption
    - RPO - The recovery point objective (RPO) is the maximum data an organization may lose after recovering from an incident using the backups
  + **Risk Identification** - Identify all the risks. Risks usually come in two forms: natural risks and person-made risks.
  + **Likelihood Assessment** - Annualized rate of occurrence (ARO) is computed for all risks using historical and statistical data
  + **Impact Analysis** - Assess the impact based on quantitative (compute ALE) & qualitative aspects (high, medium, low)
  + **Resource Prioritization** - prioritize based on Impact Analysis. Certain things can be taken parallely depending upon the resources availability
* Continuity Planning
  + Focuses on developing and implementing a continuity strategy to minimize the impact. The goal of this process is to create a continuity of operations plan (COOP).
  + **Strategy Development** - The BCP team should look back to the MTD estimates created during the early stages and determine which risks are deemed acceptable and which must be mitigated
  + **Provisions and Processes** - the BCP team designs the specific procedures and mechanisms that will mitigate the risks deemed unacceptable. Three categories of assets must be protected through BCP provisions and processes: people, buildings/facilities, and infrastructure.
* Plan Approval and Implementation
  + BCP Plan should be endorsed by the top executive in your business (CEO). This gives it much greater weight and credibility in the eyes of other senior managers.
* People with direct BCP responsibilities should be trained and evaluated on their specific BCP tasks. Backup person should be trained for redundancy.
* Documentation is a critical step in the business continuity planning process.
* The BCP documentation should also outline a vital records program for the organization. This document states where critical business records will be stored and the procedures for making and storing backup copies of those records.