



Business Continuity Plan

A business continuity plan is to be prepared in light of the guidelines of SBP on the subject and among others, also to include the following points;

1. Scope and Objective of BCP
2. Board and senior management responsibilities
 - Allocating sufficient resources and knowledgeable personnel to develop the BCP ensuring participation from all concerned
 - Detailed descriptions of roles and responsibilities of the people responsible for BCP
 - Reviewing BCP test results
 - Updating and approving the BCP on an annual basis
 - Ensuring that the concerned employees are trained and aware of their role in implementation of BCP.
 - Putting up to board the annual review and test results by senior management
 - Evaluating the adequacy and periodic testing of BCP in case of outsourced operations/service providers
3. Succession plans for critical staff and senior management
4. Detailed program for the development, implementation, and maintenance of BCP
5. Identification of
 - Organization which will handle the emergency
 - Critical (time sensitive) functions
 - Location & suitability of operations back-up site and availability of necessary facilities and accessibility/movement plan.
 - Critical documents / data
6. Program for training and awareness of staff
7. Coordination with external parties and maintenance contracts / service level agreements
8. Business Continuity Planning Process
 - Maintaining, resuming, and recovering the business, not just the recovery of the technology conducted on an enterprise-wide basis.
 - A thorough business impact analysis including:
 - Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers;
 - Consideration of all departments and business functions, not just data processing; and
 - Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses
 - Risk assessment including
 - A prioritizing of potential business disruptions and critical business lines based upon severity and likelihood of occurrence;
 - A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives;



- An analysis of threats based upon the impact on the institution, its customers, and the financial markets, not just the nature of the threat.
 - Recovery time targets
 - Risk monitoring through
 - Validation through testing or practical application.
 - Independent audit and its review by the board of directors in addition to the role of internal audit.
 - Periodical updation to reflect and respond to changes in the financial institution or its service provider(s).
9. Arrangement of storage of backups; emergency call tree and evacuation plans
10. Plans to deal with technology based products, geographic concentrations & centralization of operations
11. Testing, updation and improvement of BCP and its frequency
12. BCP is:
- Disseminated
 - Specific regarding what conditions should prompt implementation of the plan;
 - Specific regarding what immediate steps should be taken during a disruption;
 - Flexible to respond to unanticipated threat scenarios and changing internal conditions;
 - Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption; and
 - Effective in minimizing service disruptions and financial loss.
13. Contingency plan exist for outsourced operations/service providers and their compatibility
14. Major failures during the period and steps taken
15. A resilient Disaster Recovery Plan specifically covering:
- Steps to be taken during a disaster situation
 - How to get the business restored smoothly in the event that a specific facility or function is disrupted
 - Ensures the reliability of standby systems
 - Establishes priorities for processing and continuity of operations in disaster situations
 - Sets recovery time targets in case of disaster situation
 - Provides a standard for testing the plan and defines testing criteria and procedures
 - Minimizes decision-making during a disaster
 - Identification of Disaster Recovery Plan (DRP) site.
