

MIS - BUSINESS CONTINUITY PLANNING

http://www.tutorialspoint.com/management_information_system/business_continuity_planning.htm

Copyright © tutorialspoint.com

Business Continuity Planning *BCP* or Business Continuity and Resiliency Planning *BCRP* creates a guideline for continuing business operations under adverse conditions such as a natural calamity, an interruption in regular business processes, loss or damage to critical infrastructure, or a crime done against the business.

It is defined as a plan that "identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity."

Understandably, risk management and disaster management are major components in business continuity planning.

Objectives of BCP

Following are the objectives of BCP:

- Reducing the possibility of any interruption in regular business processes using proper risk management.
- Minimizing the impact of interruption, if any.
- Teaching the staff their roles and responsibilities in such a situation to safeguard their own security and other interests.
- Handling any potential failure in supply chain system, to maintain the natural flow of business.
- Protecting the business from failure and negative publicity.
- Protecting customers and maintaining customer relationships.
- Protecting the prevalent and prospective market and competitive advantage of the business.
- Protecting profits, revenue and goodwill.
- Setting a recovery plan following a disruption to normal operating conditions.
- Fulfilling legislative and regulatory requirements.

Traditionally a business continuity plan would just protect the data center. With the advent of technologies, the scope of a BCP includes all distributed operations, personnel, networks, power and eventually all aspects of the IT environment.

Phases of BCP

The business continuity planning process involves recovery, continuation, and preservation of the entire business operation, not just its technology component. It should include contingency plans to protect all resources of the organization, e.g., human resource, financial resource and IT infrastructure, against any mishap.

It has the following phases:

- Project management & initiation
- Business Impact Analysis *BIA*
- Recovery strategies
- Plan design & development
- Testing, maintenance, awareness, training

Project Management and Initiation

This phase has the following sub-phases:

- Establish need *riskanalysis*
- Get management support
- Establish team *functional, technical, BCC – BusinessContinuityCoordinator*
- Create work plan *scope, goals, methods, timeline*
- Initial report to management
- Obtain management approval to proceed

Business Impact Analysis

This phase is used to obtain formal agreement with senior management for each time-critical business resource. This phase has the following sub-phases:

- Deciding maximum tolerable downtime, also known as MAO *MaximumAllowableOutage*
- Quantifying loss due to business outage *financial, extracostofrecovery, embarrassment, without* estimating the probability of kinds of incidents, it only quantifies the consequences
- Choosing information gathering methods *surveys, interviews, softwaretools*
- Selecting interviewees
- Customizing questionnaire
- Analyzing information
- Identifying time-critical business functions
- Assigning MTDs
- Ranking critical business functions by MTDs
- Reporting recovery options
- Obtaining management approval

Recovery Phase

This phase involves creating recovery strategies are based on MTDs, predefined and management-approved. These strategies should address recovery of:

- Business operations
- Facilities & supplies
- Users *workersandend – users*
- Network
- Data center *technical*
- Data *off – sitebackupsofdataandapplications*

BCP Development Phase

This phase involves creating detailed recovery plan that includes:

- Business & service recovery plans
- Maintenance plan
- Awareness & training plan
- Testing plan

The Sample Plan is divided into the following phases:

- Initial disaster response
- Resume critical business ops
- Resume non-critical business ops
- Restoration *return to primary site*
- Interacting with external groups *customers, media, emergency responders*

Final Phase

The final phase is a continuously evolving process containing testing maintenance, and training.

The testing process generally follows procedures like structured walk-through, creating checklist, simulation, parallel and full interruptions.

Maintenance involves:

- Fixing problems found in testing
- Implementing change management
- Auditing and addressing audit findings
- Annual review of plan

Training is an ongoing process and it should be made a part of the corporate standards and the corporate culture.

Loading [MathJax]/jax/output/HTML-CSS/jax.js