

# Business Continuity Planning & Disaster Recovery



## Contents

- 1 Introduction
- 2 Analysis
  - 2.1 Impact analysis
  - 2.2 Threat analysis
  - 2.3 Definition of impact scenarios
  - 2.4 Recovery requirement documentation
- 3 Solution design
- 4 Implementation
- 5 Testing and organizational acceptance
- 6 Maintenance
  - 6.1 Information update and testing
  - 6.2 Testing and verification of technical solutions
  - 6.3 Testing and verification of organization recovery procedures
  - 6.4 Treatment of test failures
- 7 Business Data protection
  - 7.1 Events that necessitate disaster recovery
  - 7.2 Prevention against data loss
- 8 Disaster recovery planning

**Eagle Cap Communications, Inc.** offers the following services to help you and your business stay prepared in the event of a hardware failure or a natural disaster.

**Secure offsite Data Storage, Automated Data Backup and Recovery Services**

**Document Duplication (Copy) Services**

**Document Imaging (Scanning) Services**

# Business Continuity Planning & Disaster Recovery



## Introduction

**Business Continuity Planning (BCP)** methodology is scalable for an organization of any size and complexity. Even though the methodology has roots in regulated industries, any type of organization may create a BCP manual, and arguably every organization *should* have one in order to ensure the organization's longevity. Evidence that firms do not invest enough time and resources into BCP preparations is evident in these disaster survival statistics.

*Fires permanently close 44% of the business affected. In the 1993 World Trade Center bombing, 150 businesses out of 350 affected failed to survive the event. Conversely, the firms affected by the Sept 11 attacks with well-developed and tested BCP manuals were back in business within days.*

A BCP manual for a small organization may be simply a printed manual stored safely away from the primary work location, containing the names, addresses, and phone numbers for crisis management staff, general staff members, clients, and vendors along with the name, phone number, contact person and location of the offsite data backup, copies of insurance contracts, and



other critical materials necessary for organizational survival. At its most complex, a BCP manual may outline a secondary work site, technical requirements and readiness, regulatory reporting requirements, work recovery measures, the means to reestablish physical records, the means to establish a new supply chain, or the means to establish new production centers. Firms should ensure that their BCP manual is realistic and easy to use during a crisis.

The development of a BCP manual has five main phases: analysis, solution design, implementation, testing and organization acceptance, and maintenance.

## Analysis

The analysis phase in the development of a BCP manual consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

## Impact analysis

An impact analysis results in the differentiation between critical and non-critical organization functions. A function may be considered critical if the implications for stakeholders of damage to the organization resulting are regarded as unacceptable. Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law. Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

## Business Continuity Planning & Disaster Recovery



- The time frame in which the critical function must be resumed after the disaster
- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function

### Threat analysis

After defining recovery requirements, documenting potential threats is recommended to detail a specific disaster's unique recovery steps. Some common threats include the following:

- Disease
- Earthquake
- Fire
- Flood
- Cyber attack
- Hurricane
- Utility outage
- Terrorism

All threats in the examples above share a common impact - the potential of damage to organizational infrastructure - except one (disease). The impact of diseases is initially purely human, and may be alleviated with technical and business solutions. During the 2002-2003 SARS outbreak, some organizations grouped staff into separate teams, and rotated the teams between the primary and secondary work sites, with a rotation frequency equal to the incubation period of the disease.

The organizations also banned face-to-face contact between opposing team members during business and non-business hours. With such a split, organizations increased their resiliency against the threat of government-ordered quarantine measures if one person in a team contracted or was exposed to the disease.

Damage from flooding also has a unique characteristic. If an office environment is flooded with non-salinated and contamination-free water (e.g.m, in the event of a pipe burst), equipment can be thoroughly dried and may still be functional.

### Definition of impact scenarios

After defining potential threats, documenting the impact scenarios that form the basis of the business recovery plan is recommended. In general, planning for the most wide-reaching disaster or disturbance is preferable to planning for a smaller scale problem, as almost all smaller scale problems are partial elements of larger disasters. A typical impact scenario like 'Building Loss' will most likely encompass all critical business functions, and the worst potential outcome from any potential threat. A business continuity plan may also document additional impact scenarios if an organization has more than one building. Other more specific impact scenarios - for example

## **Business Continuity Planning & Disaster Recovery**



a scenario for the temporary or permanent loss of a specific floor in a building - may also be documented.

### **Recovery requirement documentation**

After the completion of the analysis phase, the business and technical plan requirements are documented in order to commence the implementation phase. For an office-based, IT intensive business, the plan requirements may cover the following elements which may be classed as ICE (In Case of Emergency) Data:

- The individuals involved in the recovery effort along with their contact and technical details
- The numbers and types of desks, whether dedicated or shared, required outside of the primary business location in the secondary location
- The numbers and types of computer systems and networking equipment required to run the critical business operations
- The critical software and company data required to continue business operations.
- The applications and application data required from the secondary location desks for critical business functions
- The manual workaround solutions
- The peripheral requirements like printers, copier, fax machine, calculators, paper, pens etc.

Other business environments, such as production, distribution, warehousing etc will need to cover these elements, but are likely to have additional issues to manage following a disruptive event.

### **Solution design**

The goal of the solution design phase is to identify the most cost effective disaster recovery solution that meets two main requirements from the impact analysis stage. For IT applications, this is commonly expressed as:

1. The minimum application and application data requirements
2. The time frame in which the minimum application and application data must be available

Disaster recovery plans may also be required outside the IT applications domain, for example in preservation of information in hard copy format, or restoration of embedded technology in process plant. This BCP phase overlaps with Disaster recovery planning methodology. The solution phase determines:

- the crisis management command structure
- the location of a secondary work site (where necessary)
- telecommunication architecture between primary and secondary work sites

## **Business Continuity Planning & Disaster Recovery**



- data replication methodology between primary and secondary work sites
- the application and software required at the secondary work site, and
- the type of physical data requirements at the secondary work site.

### **Implementation**

The implementation phase, quite simply, is the execution of the design elements identified in the solution design phase. Work package testing may take place during the implementation of the solution, however; work package testing does not take the place of organizational testing.

### **Testing and organizational acceptance**

The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors. Testing may include:

- Crisis command team call-out testing
- Technical swing test from primary to secondary work locations
- Technical swing test from secondary to primary work locations
- Application test
- Business process test

At minimum, testing is generally conducted on a biannual or annual schedule. Problems identified in the initial testing phase may be rolled up into the maintenance phase and retested during the next test cycle.

### **Maintenance**

Maintenance of a BCP manual is broken down into three periodic activities. The first activity is the confirmation of information in the manual. The second activity is the testing and verification of technical solutions established for recovery operations. The third activity is the testing and verification of documented organization recovery procedures. A biannual or annual maintenance cycle is typical.

### **Information update and testing**

All organizations change over time, therefore a BCP manual must change to stay relevant to the organization. Once data accuracy is verified, normally a call tree test is conducted to evaluate the notification plan's efficiency as well as the accuracy of the contact data. Some types of changes that should be identified and updated in the manual include:

## **Business Continuity Planning & Disaster Recovery**



- Staffing changes
- Staffing persona
- Changes to important clients and their contact details
- Changes to important vendors/suppliers and their contact details
- Departmental changes like new, closed or fundamentally changed departments.

### **Testing and verification of technical solutions**

As a part of ongoing maintenance, any specialized technical deployments must be checked for functionality. Some checks include:

- Virus definition distribution
- Application security and service patch distribution
- Hardware operability check
- Application operability check
- Data verification

### **Testing and verification of organization recovery procedures**

As work processes change over time, the previously documented organizational recovery procedures may no longer be suitable. Some checks include:

- Are all work processes for critical functions documented?
- Have the systems used in the execution of critical functions changed?
- Are the documented work checklists meaningful and accurate for staff?
- Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

### **Treatment of test failures**

As suggested by the diagram included in this article, there is a direct relationship between the test and maintenance phases and the impact phase. When establishing a BCP manual and recovery infrastructure from scratch, issues found during the testing phase often must be reintroduced to the analysis phase.

# Business Continuity Planning & Disaster Recovery



## Business Data Protection

With the rise in information technology and the reliance on business-critical data, the landscape has changed in recent years in favor of protecting irreplaceable data. This is especially evident in information technology, with most large computer systems backing up digital information to limit data loss and to aid data recovery.

It is believed that some companies spend up to 25% of their budgets on disaster recovery planning; this is to avoid larger losses. Of companies that had a major loss of computerized records, 43% never reopen, 51% close within two years, and only 6% will survive long-term.

The current data protection market is characterized by:

- Rapidly changing customer needs that are driven by data growth, regulatory issues and the growing importance to access data quickly by retaining it online.
- An ever-shrinking time frame for backing up data, which is burdening conventional tape backup technologies.

## Events That Necessitate Disaster Recovery

There are many different risks that can negatively impact the normal operations of an organization. A risk assessment should be performed to determine what constitutes a disaster and which risks a specific company is susceptible to, including:

- Natural disasters
- Fire
- Power failure
- Terrorist attacks
- Organized or deliberate disruptions
- Theft
- System and/or equipment failures
- Human error
- Computer viruses
- Legal issues
- Worker strikes

## Preventions Against Data Loss

- Backups sent off-site automatically and in regular intervals
  - Includes software as well as all data information, to facilitate recovery
  - Use a Remote backup facility to minimize data loss
- Surge Protectors - to minimize the effect of power surges on delicate electronic equipment
- Uninterruptible Power Supply (UPS) and/or Backup Generator

## Business Continuity Planning & Disaster Recovery



- Fire Preventions - more alarms, accessible extinguishers
- Anti-virus software and other security measures

### Disaster Recovery Planning

Disaster recovery planning falls into the realm of Business Continuity Planning, as well as Risk management. The planning process consists of the following steps:

- Assess business impact and risk. This should include an assessment of the business unit's function and, preferably, a business impact analysis (BIA). The purpose of the assessment is to determine the business unit's relative contribution to the larger organization (monetary and functional).
- Develop a Disaster Recovery framework. Data should be categorized by importance. Two measures of importance are used, RTO and RPO. Recovery Time Objective (RTO) is the acceptable amount of time between the disaster and the post-disaster resumption of function (how long can we wait to restore data?). Recovery Point Objective (RPO) is the acceptable data roll-back (how current does the data have to be?).
- Adjust information systems to make Disaster Recovery easier. This includes consolidating servers and data, perhaps with a Storage Area Network or other archival storage method.
- Address other technical issues. Maintaining logical integrity between data and applications that may be interdependent is not a trivial matter. The business may consider the use of applications that have recovery built in to their capabilities.

A good plan takes into account many different factors. The most important are:

- Communication
  - Personnel - notify all key personnel of the problem and assign them tasks focused toward the recovery plan.
  - Customers - notifying clients about the problem minimizes panic.
- Recall backups - If backup tapes are taken offsite, these need to be recalled. If using remote backup services, a network connection to the remote backup location (or the Internet) will be required.
- Facilities - having backup hot sites or cold sites for larger companies. Mobile recovery facilities are also available from many suppliers.
- Knowledge Workers - during a disaster, employees are required to work longer, more stressful hours, and a support system should be in place to alleviate some of the stress.
- Business Information - backups should be stored in a completely separate location from the company. Security and reliability of that data is key.