

6. Business Continuity Planning and Disaster Recovery Planning

Business Continuity Planning

Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Planning is an activity to be performed before the disaster occurs or it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business continuity covers the following areas:

- *Business resumption planning*: the operation's piece of business continuity planning.
- *Disaster recovery planning*: the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- *Crisis Management*: the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

Objectives and Goal of Business Continuity Planning

The primary objective of a BCP is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to reestablish normal business operations.

➤ Objectives

1. Provide for the safety and well-being of people on the premises at the time of disaster;
2. Continue critical business operations;
3. Minimize the duration of a serious disruption to operations and resources;
4. Minimize immediate damage and losses;
5. Establish management succession and emergency powers;
6. Facilitate effective co-ordination of recovery tasks;
7. Identify critical complexity of the recovery effect;
8. Reduce the complexity of the recovery effort;

➤ Goals

1. Identify weaknesses and implement a disaster prevention program;
2. Minimize the duration of a serious disruption to business operations;
3. Facilitate effective co-ordination of recovery tasks; and
4. Reduce the complexity of the recovery effort

Developing a business continuity plan

The methodology for developing a business continuity plan can be sub-divided into eight different phases.

1. *Pre-panning activities*: Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
2. *Vulnerability assessment and general definition of requirements*: Obtaining commitment from appropriate management to support and participate in the effort;
3. *Business impact analysis*: Defining recovery requirements from the perspective of business functions;
4. *Detailed definition of requirement*: Documenting the impact of an extended loss to operations and key business functions;
5. *Plan development*: Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;

6. *Testing Program*: Selecting business continuity teams that ensure the proper balance required for plan development;
7. *Maintenance program*: Developing a business continuity plan that is understandable, easy to use and maintain;
8. *Initial plan testing and plan implementation*: Define how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Pre-Planning Activity:

We obtain an understanding of the existing and projected systems environment of the organization. This enables us to refine the scope of business continuity planning and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan.

Two key deliverables of this phase are: the development of policy to support the recovery programs; and awareness program to educate management and senior individuals who will be required to participate in the business continuity planning.

Vulnerability assessment and definition of requirement:

Security and control within an organization is a continuing concern. It is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence. Following activities are included in this phase;

1. A thorough security assessment of the system and communication environment.
2. Improve existing emergency plan and disaster prevention measures and implement new emergency plan
3. Define the scope of planning effort;
4. Purchase recovery planning and maintenance software;
5. Develop a plan framework;
6. Assemble business continuity team and conduct awareness sessions.

Business impact analysis (BIA):

BIA is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions.

The business impact analysis is intended to help understand the degree of potential loss and various other unwanted effects which could occur. This will cover not just financial loss, but other issues, such as reputation damage, regulatory effects etc.

Tasks that performed in this phase are as follows

1. Identify organizational risks
2. Identify critical business processes
3. Identify and quantify threats/risks to critical business process and the order in which they must be restored.
4. Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
5. Determine the maximum allowable downtime for each business process.
6. Identify the type and the quantity resources required for recovery.
7. Determine the impact to the organization in the event of a disaster.

Plan development:

The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies.

Testing the Plan:

The objective of performing BCP tests are to ensure that:

- The recovery procedures are complete and workable.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- The resources such as business processes, IS systems, Personnel, facilities and data are obtainable and operational to perform recovery processes.
- The manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- The success or failure of the business continuity training program is monitored.

Types of Plan

1. Emergency Plan:

The emergency plan specifies the action to be undertaken immediate when a disaster occurs. Management must identify those situations that require the plan to be invoked for example fire, terrorist attack, damage etc.

2. Back-up Plan:

The back-up plan specifies the type of back-up to be kept, frequency with which backup is to be undertaken, procedures for making back-up, location of backup resource, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system.

3. Recovery Plan:

The backup plan is intended to restore operations quickly so the information system functions can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specific of the recovery to be undertaken.

Threats and Risk Management

The *Various threats* to computer system are discussed as under

1. Lack of integrity
2. Lack of Confidentiality
3. Lack of system availability
4. Unauthorized users attempt to gain access to the system and system resources
5. Disgruntled employees
6. Hacker and computer crimes
7. Terrorism and industrial espionage

The *objectives of risk assessment* are to

- Identify information technology risks
- Determine the level of risk
- Identify the risk factors
- Develop risk mitigation strategies

The **benefits** of performing risk assessment are:

- A business drives process to identify, quantify and manage risks while detailing future suggestions for improvement in technical delivery.
- A framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle.
- Interpretations and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable risk.
- Implementation of strict disciplines for active management during the project lifecycle.

Types of Back-ups

1. Full Backup: captures all files on the disk or within the folder selected for backup
2. Incremental Backup: captures file that were created or changed since the last backup, regardless types of backup.
3. Differential Backup: stores the files that have changed since the last full backup.
4. Mirror back-up: is identical to full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password.

Alternate Processing Facility Arrangements

Security administrations should consider the following backup options:

1. Cold Site: if an organization can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system raised floors, air conditioning, power, communication lines, and so on.
2. Hot Site: if fast recovery is critical, an organization might need hot site backup.
3. Warm Site: a warm site provides an intermediate level of backup. It has all cold-site backup facilities plus hardware that might be difficult to obtain or install.
4. Reciprocal agreement: two or more organizations might agree to provide backup facilities to each other in the event of disaster.

Types of Back-up Media

1. Floppy diskettes
2. DVD
3. Tape drives
4. Disk Drives
5. Removable disks
6. DAT (Digital Audio tape)
7. Optical Jukeboxes
8. Autoloader tape systems
9. USB flash drives
10. Zip Drive

Backup tips

1. Draw up a simple plan of who will do what in the case of an emergency
2. Keep a record of what was backed up, when it was backed up and which backup media contains what data.
3. Utilize the volume shadow copy service in windows server 2003.
4. Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.
5. Create a reference point where you know everything is working properly.
6. Select the option to restrict restoring data to owner or administrator and also set the domain group policy to restrict the restore privilege to administrators only.
7. Create a step-by-step guideline clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

Disaster Recover Procedural Plan

- The condition for activating the plans, which describes the process to be followed before each plan, are activated.
- Emergency procedures, which describe the situation for emergency procedures to be applied and followed.
- A fallback procedure which describes the actions to be taken to move essential business activities or support service to alternate temporary locations, to bring business process back into operation in the required time scale.
- Resumption procedures, which describes the actions to be taken to return normal business operations.
- A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintain the plan.
- Awareness and education activities, which are designed to understanding of business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedures.
- List of vendors doing business with the organization, their contact number and address for emergency purpose.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone number of employees on event of emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location etc.
- Medical procedures to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms
- Primary computer centered hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

Testing Methodologies and Checklist

With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests:

1. Hypothetical: this test is an exercise to verify the existence of all necessary procedures and actions specified within the recovery plan and to prove the theory of those procedures.
2. Component: is the smallest set of instruction within the recovery plan which enables specific processes to be performed. This testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods.
3. Module: a module is a combination of components. The ideal method of testing is that each component be individually tested before being included in module. The aim of the module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined.
4. Full: the full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective detailed in the recovery plan.

Audit tools and techniques

The best audit tool and techniques is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meeting, questionnaires and documentation reviews. These tools and techniques are categorized as under:

- I. **Automated tools:** make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.
- II. **Internal Control Auditing:** this includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- III. **Disaster and Security Checklists:** a checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline.
- IV. **Penetration Testing:** penetration testing can be used to locate vulnerabilities.