

Disaster Recovery Planning

All businesses rely heavily on information and depend on the computer systems that gather, store and process that information. The loss of access to these systems for even a few days can cause severe financial loss and even threaten the survival of the business.

What is a Disaster Recovery Plan?

A Disaster Recovery Plan is a document that clearly sets out what is to be done to prevent and prepare for disasters. If a disaster does occur, the plan outlines what needs to be done to restore normal business operations. The emphasis is placed on both prevention and business resumption with minimal cost and inconvenience to customers, suppliers and the business itself.

Why do I need a plan?

A Disaster Recovery Plan aims to eliminate the most common and preventable disasters (viruses, disk crash, backup failure, data loss) and to reduce the impact of disasters that we cannot control (fire, flood, earthquake, storm).

Benefits of a Disaster Recovery Plan

- A plan saves time and money in the recovery phase as necessary equipment and skills can be quickly assembled and put into action.
- When you are in the middle of a disaster it is difficult to make decisions that normally take considerable skill, research and forward planning. Often hasty judgements are made, leading to costly mistakes and making the disaster worse.
- To protect the investment in Information Technology and in turn get a higher return on investment (ROI) by greater system availability.
- To reduce insurance premiums.
- To minimise legal and regulatory liabilities.
- To meet quality assurance standards.

What should the plan include?

The plan should identify the key business processes, key people and resources required, identify the threats and vulnerabilities of the business processes, identify controls and procedures to mitigate the risks and have a clear action plan for the recovery and resumption of each business process.

How is the plan developed?

The plan is developed by gaining management support, conducting an audit of all business processes, prioritising these processes, identifying the key staff and skills required for these processes, identifying likely threats to these processes, identifying vulnerabilities of these processes, developing controls and procedures to mitigate these threats and vulnerabilities, developing procedures for the Emergency, Backup and Recovery phases, regularly testing and evaluating the plan.

Disaster Recovery Planning

Disaster Recovery and Business Resumption

Business Resumption is the ability to conduct critical business processes as soon as possible after the disaster (eg from temporary premises). Business Resumption is a very customer focussed viewpoint and needs to occur as soon as possible after the disaster. For example – following a factory fire, take the customer orders over a mobile phone in a temporary office, arrange temporary warehousing and arrange suppliers to deliver new stock.

Disaster Recovery refers to completing the whole process back to full normal operations and is more supplier focussed.

Business Processes and Information Systems

There is a clear distinction between a business process and an information system. It is important to be aware that the business process is the more critical system to the business. For example it is more important to accept a customer order and have to write it on a scrap of paper than to decline the order because your computerised ordering system is down. Taking customer orders is a business process; the computerised ordering system is an information system for order taking and many other associated processes. The backup system for the example above may have required the order taker to look up a printed catalogue for pricing details and to use a calculator to total the order. The business process may have been delayed but the business continued to operate relatively normally.

Business Process

The following are examples of typical Business Processes - taking customer orders, placing orders with suppliers, checking inventory, doing banking, preparing payroll, answering mail, paying accounts, receiving customer payments, communicating with customers and suppliers, marketing and advertising.

Information System

Examples of Information Systems include – the company email system, computerised accounting system, online ordering system, web site, library system, word processing, databases, spreadsheets, fleet management system, payroll, etc.

Disaster Recovery Planning

Threats, Vulnerabilities and Controls

Most disasters are caused by relatively small local incidents that can be identified and in most cases eliminated entirely. By identifying both the threats and vulnerabilities to business processes, a plan of controls can be developed to reduce or eliminate the risks so the business can be protected against potential disasters.

Threats

Typical threats to business processes include:

- Human Error
- Fire
- Fraud
- Theft
- Flooding
- Burst water pipes
- Computer virus
- Computer hacking / attack
- Loss of data/records
- Corrupted data
- Damaged/lost/corrupted backups
- Equipment failure
- Electrical supply failure
- Electrical storm damage
- Telecommunications failure
- Internet service disruption
- Negative publicity
- Environmental hazards
- Vandalism / wilful damage
- Bushfire
- Earthquake
- Hurricane / Cyclone
- Terrorism

Vulnerabilities

Vulnerabilities are things that make the system prone to disasters such as:

- Poor computer security
- Lack of planning and change control
- Poor physical security
- Inadequate documentation / vendor support
- Inadequate staff identification / security
- Inadequate fire protection systems
- Lack of surge protection devices

Disaster Recovery Planning

- Poorly maintained Uninterruptible Power Supplies & generators
- Procedures not being followed
- Lack of training
- Lack of backup systems
- Poor testing procedures
- Inadequate accounting and control measures

Controls

Controls are countermeasures for vulnerabilities and can be identified into four main groups:

- a) deterrent controls – to reduce likelihood of a disaster;
- b) preventative controls – prevent the disaster where possible;
- c) corrective controls – what to do in effect of a disaster;
- d) detective controls - discover attacks and trigger preventative or corrective controls.

Disaster Phases

Emergency Phase

The initial response to the disaster. Emergency and Disaster Recovery Plans to be initiated. Recover Team appointed. Senior Management briefed on required actions.

Backup Phase

Initiate the recovery of the critical business applications and get the alternative site/equipment operational. Less critical applications brought online as time/resources permit.

Recovery Phase

Complete recovery of all systems and full normal operations back in the existing site (if practical).