

# Disaster recovery planning

*A documented structured approach.*

Given your organisations' dependencies on IT to run operations, a documented structured approach with instructions on how to respond to unplanned events is critical.

vCIO service from SevenC Computing will ensure a step by step plan is in place that consists of the necessary precautions to minimise the effects of a disaster and ensure the business can continue to operate or quickly resume mission critical functions.

This process starts with an analyses of business processes and continuity needs.

The correct strategy will then be implemented, that will define the organisations plans for responding to an incident.

In determining the correct strategy for your business, the following assessment and factors will be considered.

- Budget
- Resources – people and physical facilities
- Managements position on risks
- Technology
- Data
- Suppliers



## Checklist

- Establish the scope of the actual requirement
- Gather relevant network infrastructure documentation
- Identify the most serious threats and vulnerabilities, and the most critical assets
- Review the history of unplanned incidents and outages, and how they were handled
- Identify current DR strategies
- Identify the emergency response team
- Management review and approval of the plan
- Test the plan
- Update the plan
- Implement DR plan audit

*Having involvement at all levels, from Management to entry level employees will increase the value of the DR Plan.*

## Types of disaster recovery plans

### Virtualised disaster recovery plan

Virtualisation provides opportunities to implement disaster recovery in a more efficient way, a virtualised environment can spin up new virtual machines within minutes.

### Network disaster recovery plan

These are plans that involve the recovery of the network.

### Cloud disaster recovery plan

Ranging from file backups in the cloud to complete replication with automated failover.

### Data centre recovery plan

Key elements of data center DR is planning, analysing key components such as building location - power systems and protection, security systems and office space, and addressing a broad range of possible scenarios.



## The DR plan from SevenC will include:

- Statement, overview and objectives of the overall plan
- Contact details for all key disaster recovery personnel
- In depth analysis of emergency and routine response actions
- Details about recovery sites, including diagrams and illustrations
- Details of your business' most critical business assets and systems
- Up to date list of software, user accounts and license keys
- Technical information for third part vendors

## Ingredients of an effective DR plan

- Inventory of all hardware and software
- Define your tolerance for downtime and data loss
- A layout of who is responsible for what
- The creation of a communication plan
- Ensure all service level agreements include disaster/emergency references
- Include how to handle sensitive information
- Test the plan regularly