huonit

10-Point Scoping Guide for Disaster Recovery:

Choose the right solution for your business

DID YOU KNOW?

Company survival rates after catastrophic data loss are slim:

- Only *6%* recover
- *43%* do not reopen
- *51%* fail within the next two years

-AM Best

With so many disaster recovery options available, finding the right solution for your business can be complicated depending on your budget, levels of acceptable risk, and recovery requirements.

The following 10 point guide will help you quickly scope out a DR solution, or to simply validate your existing strategy…

1. Level of Disaster Recovery

First and foremost, determine what level of Disaster Recovery your business needs. These differ by levels of service, costs and effort required to implement each.

- **Hot Site** – A synchronous mirrored system for almost immediate cutover.
- **Warm Site** – The secondary site holds an up to date copy of your system on standby infrastructure, ready to be activated within minutes or hours.
- **Cold Site** – Data is backed up periodically. In the event of a disaster, hardware is not readily available and would need to be procured, rented or repurposed. This process is the slowest, taking weeks or even months.

2. Types of Disaster Scenarios

Consider the different types of scenarios in which your business may require DR, such as:

- **Physical Disaster** – Your office is out of commission, due to a fire or power failure etc. Staff cannot work in the building.
- **System Disaster** – Your office is intact, but your IT system is offline due to a critical hardware failure etc, so your staff can keep working in the building but IT is unavailable.

3. Define & Prioritise Your Business Needs

Now, clarify exactly how quickly you need your systems up and running in the event of a disaster. Compile a full list of every physical and virtual machine in your system, and determine for each:

- **Recovery Point Objective (RPO)** – The maximum tolerable period in which data might be lost due to a major incident (i.e. this is usually the time between the failure and your last successful backup).
- **Recovery Time Objective (RTO)** – How long after a disaster does your IT system need to be restored?

4. Solution Design – Replication

There are various types of replication, depending on what infrastructure you use and what your goals are. Some common types are:

- **Host-Based Replication** – The virtual machine disks are replicated via the hypervisor, negating the need to have the same storage vendor at both DR and production sites.
- **Storage Layer Replication** – The SAN replicates the data to an identical SAN at the DR site, which is more efficient as it takes advantage of storage level de-duplication and compression.
- **Virtual Machine Replication** – Data is replicated using a third party software on a per VM basis.
- **Application Based Replication** – The application handles the replication. This is more complex to setup with slightly higher costs, however has the advantage of hot standby and high availability.

5. Retention

This is the grey area between backup and disaster recovery. Whilst most disaster recovery systems should hold a replication of your current system, some may offer archival (depending on how comprehensive your backup system is). Determine how many point in time backups you want retained.

6.

Network Design & Rate of Change

The internet links you use for your disaster recovery system are absolutely crucial.

Consider the following points when designing your network:

- **Link Capacity** – Understand your data set size and expected rate of change to determine link capacity.
- **Redundancy** – There should be no single points of failure in your network, including dual firewalls, backup wireless links, etc.

7.

Failing Over – How will your staff work again?

After a disaster is declared and your system is restored in the DR environment, how will your staff work?

- **Logging in** – Do you have virtual desktop or remote desktop solution such as Citrix XenDesktop or XenApp, VMware View or Microsoft Remote Desktop Services, etc?
- **Physical Devices** – What devices will staff use to log in if your building is out of commission? Do they have laptops or home PCS, or will you lease devices? Remember peripherals such as printers, too.
- **Location** – Where will staff actually work from? Some businesses rent temporary offices, while others elect for staff to work from home.

8.

DR site security and sovereignty

The location, reliability and security of your secondary site are absolutely crucial.

For a business-grade solution, determine what features you expect:

- **Security** – 24x7 surveillance and strict access controls.
- **Multi-tenancy Segregation** – How is your data separated from other parties.
- **Power and Air Conditioning** – Monitoring and redundancy.
- **Certifications** – Varying ISO and Government certification levels.
- **Location** – Does your provider back your data up to other locations. Locally or overseas?

9.

Cost Model for Scalability

Initial quotes may not always remain static. Be sure to understand the cost model upfront and consider its scalability and as your dataset grows. Some different types of cost variables may be:

- **Resource usage (per GB, VM, physical servers etc)**
- **Storage Layer Replication**
- **Hourly usage**
- **Licensing**
- **Bandwidth and cross connects**
- **Rack space and power costs**
- **Associated labour services**

10.

Ongoing maintenance, reporting and ‘bubble’ testing

Once you establish your disaster recovery solution, it is certainly not a ‘set and forget’ system. Ensure your forward plan addresses:

- **Reporting** – What type and frequency of reports do you need to confirm that replications are successful?
- **Maintenance** – Establish a routine schedule of maintenance and configuration

> **“Before Huon IT it could have taken days to get up and running in the event of system failure. Now we can do it in one hour.”**
>
> - Brad Allen, IT Director
> McCabes Lawyers

Is your organisation prepared for a disaster?

Speak to an expert at Huon IT about your Disaster Recovery requirements before it’s too late.

huonit

W www.huonit.com.au | **E** info@huonit.com.au

SYDNEY **MELBOURNE** **1300 HUON IT**