What is Disaster Recovery

A disaster recovery plan enables businesses to respond quickly to a disaster and take immediate action to reduce damage, and resume operations as quickly as possible.

A disaster recovery plan typically includes:

- Emergency procedures staff can carry out when a disaster occurs
- Critical IT assets and their maximum allowed outage time
- Tools or technologies that should be used for recovery
- A disaster recovery team, their contact information and communication procedures (e.g. who should be notified in case of disaster)

I WAS JUST WONDERING, DO WE HAVE A DISASTER RECOVERY PLAN?
IT DEPT
© D.Fletcher for CloudTweaks.com

Causes for an IT disaster

There is a great number of IT disasters that can completely disturb an organization:

Minor disaster – Causes

- Simple human error
- Software error
- Loss of device

Operational disaster – Causes

- IT admin mistake
- Viruses
- Tech migration failure
- Hardware failure

Major disaster – Causes

- Hacking
- Natural disaster
- Theft of corporate data
- Employee malfeasance

"For security purposes, the information should make no sense at all to spies and hackers. We'll bring in someone later to figure out what you meant."

What is a security Model?

A **security model** is a framework in which a **security** policy is developed. The development of this **security** policy is geared to a particular setting or instance of a policy, for example, a **security** policy based upon authentication, but built within the confines of a **security model**. For example, designing a **security model** based upon authentication and authorization, one would consider the 4-factor **model** of **security**, that is, authentication, authorization, availability, and authenticity.

Service Levels for Disaster Recovery

Tier 0 - No off-site data. Recovery is only possible using on-site systems.

Tier 1 - Physical backup with a cold site. Data, likely on tape, is transported to an off-site facility that does not have the necessary hardware installed.

Tier 2 - Physical backup with a hot site. Data, likely on tape, is transported to an off-site facility that has the necessary hardware installed to support key systems of the primary site.

Tier 3 - Electronic vaulting. Data is electronically transmitted to a hot site.

Tier 4 - Point-in-time copies/active secondary site. Vital data is copied across the primary and secondary sites, each site backing up the other. Disk is often used in this tier.

Tier 5- Two-site commit/transaction integrity. Data is continuously transmitted across sites.

Tier 6 - Minimal to zero data loss. Recovery is instantaneous, often involving disk mirroring or replication.

Tier 7 - Later added to include automation, and it represents the highest level of availability in disaster recovery scenarios. In general, while the ability to recover improves with the next highest tier, costs also increase.

What is a disaster recovery plan?

A disaster recovery plan enables businesses to respond quickly to a disaster and take immediate action to reduce damage, and resume operations as quickly as possible.

A disaster recovery plan typically includes:

- Emergency procedures staff can carry out when a disaster occurs
- Critical IT assets and their maximum allowed outage time
- Tools or technologies that should be used for recovery
- A disaster recovery team, their contact information and communication procedures (e.g. who should be notified in case of disaster)

Why is Disaster Recovery Important?

Drafting a disaster recovery plan, and ensuring you have the right staff in place to carry it out, can have the following benefits:

- Minimize interruption – in the event of a disaster, even if it is completely unexpected, your business can continue operating with minimal interruption.
- Limit damages – a disaster will inevitably cause damage, but you can control the extent of damage caused. For example, in hurricane-prone areas, businesses plan to move all sensitive equipment off the floor and into a room with no windows.
- Training and preparation – having a disaster recovery program in place means your staff are trained to react in case of a disaster. This preparation will lower stress levels and give your team a clear plan of action when an event occurs.
- Restoration of services – having a solid disaster recovery plan means you can restore all mission critical services to their normal state in a short period of time. Your Recovery Time Objective (RTO) will determine the longest time you are willing to wait until service is restored.

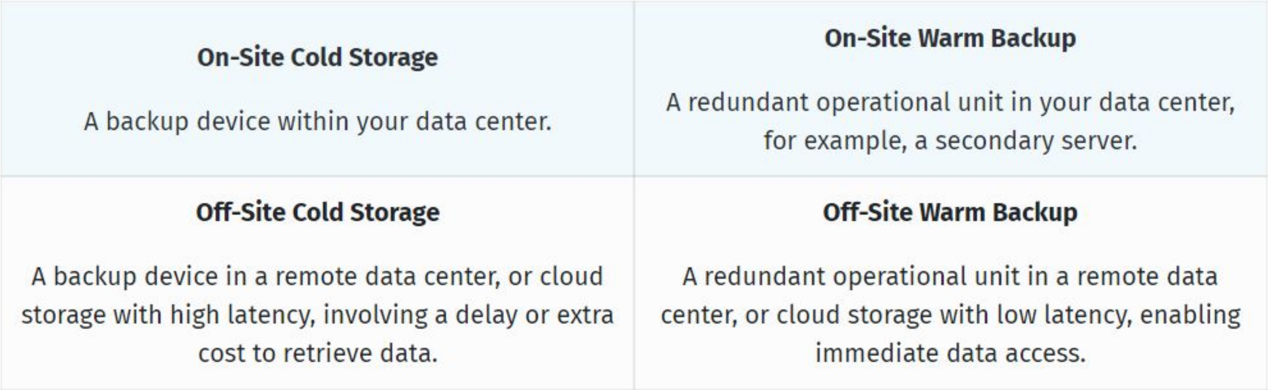
How Does disaster Recovery Work?

1. Know Your Threats

2. Know Your Assets

3. Define Your RTO and RPO Define your Recovery Time Objective (RTO) for critical assets. What period of downtime can you sustain? The term recovery point objective (RPO) refers to the maximum age of files the organization must recover from backup storage to resume normal operations after a disaster occurs.

4. Set Up Disaster Recovery Sites



On-Site Cold Storage A backup device within your data center.	**On-Site Warm Backup** A redundant operational unit in your data center, for example, a secondary server.
Off-Site Cold Storage A backup device in a remote data center, or cloud storage with high latency, involving a delay or extra cost to retrieve data.	**Off-Site Warm Backup** A redundant operational unit in a remote data center, or cloud storage with low latency, enabling immediate data access.

5. Test Backups and Restor of Services

Disaster Recovery Planning

Business impact analysis

The creation of a comprehensive disaster recovery plan begins with business impact analysis. When performing this analysis, you'll create a series of detailed disaster scenarios that can then be used to predict the size and scope of the losses you'd incur if certain business processes were disrupted.This will allow you to identify the areas and functions of the business that are the most critical and enable you to determine how much downtime each of these critical functions could tolerate. With this information in hand, you can begin to create a plan for how the most critical operations could be maintained in various scenarios.

Risk analysis

Assessing the likelihood and potential consequences of the risks your business faces is also an essential component of disaster recovery planning. As cyberattacks and ransomware become more prevalent, it's critical to understand the general cybersecurity risks that all enterprises confront today as well as the risks that are specific to your industry and geographical location.

Ask yourself the following questions:

- What financial losses due to missed sales opportunities or disruptions to revenue-generating activities would you incur?
- What kinds of damage would your brand’s reputation undergo? How would customer satisfaction be impacted?
- How would employee productivity be impacted? How many labor hours might be lost?
- What risks might the incident pose to human health or safety?
- Would progress towards any business initiatives or goals be impacted? How?

Prioritizing applications

Not all workloads are equally critical to your business’s ability to maintain operations, and downtime is far more tolerable for some applications than it is for others. Separate your systems and applications into three tiers, depending on how long you could stand to have them be down and how serious the consequences of data loss would be.

- Mission-critical: Applications whose functioning is essential to your business’s survival.
- Important: Applications for which you could tolerate relatively short periods of downtime.
- Non-essential: Applications you could temporarily replace with manual processes or do without.

Documenting dependencies

The next step in disaster recovery planning is creating a complete inventory of your hardware and software assets. It’s essential to understand critical application interdependencies at this stage. If one software application goes down, which others will be affected?

Designing resiliency—and disaster recovery models—into systems as they are initially built is the best way to manage application interdependencies. It’s all too common in today’s microservices-based architectures to discover processes that can’t be initiated when other systems or processes are down, and vice versa.

Regulatory compliance issues

All disaster recovery software and solutions that your enterprise have established must satisfy any data protection and security requirements that you’re mandated to adhere to. This means that all data backup and failover systems must be designed to meet the same standards for ensuring data confidentiality and integrity as your primary systems.

At the same time, several regulatory standards stipulate that all businesses must maintain disaster recovery and/or business continuity plans.

Choosing technologies

Backups serve as the foundation upon which any solid disaster recovery plan is built. In the past, most enterprises relied on tape and spinning disks (HDD) for backups, maintaining multiple copies of their data and storing at least one at an offsite location.

In today's always-on digitally transforming world, tape backups in offsite repositories often cannot achieve the RTOs necessary to maintain business-critical operations. Architecting your own disaster recovery solution involves replicating many of the capabilities of your production environment

Choosing recovery site locations

Building your own disaster recovery data center involves balancing several competing objectives. On the one hand, a copy of your data should be stored somewhere that's geographically distant enough from your headquarters or office locations that it won't be affected by the same seismic events, environmental threats, or other hazards as your main site.

Continuous testing and review

Simply put, if your disaster recovery plan has not been tested, it cannot be relied upon. All employees with relevant responsibilities should participate in the disaster recovery test exercise, which may include maintaining operations from the failover site for a period of time.

If performing comprehensive disaster recovery testing is outside your budget or capabilities, you can also schedule a "tabletop exercise" walkthrough of the test procedures, though you should be aware that this kind of testing is less likely to reveal anomalies or weaknesses in your DR procedures—especially the presence of previously undiscovered application interdependencies—than a full test.

What is Disaster Recovery Policy?

The purpose of a disaster recovery policy is to identify critical business assets, and define activities needed to ensure their continuity in a disaster. The policy can cover any assets essential for business operations—equipment, software, physical facilities, and even employees—and determines what steps the business will take to protect and recover them.

Disaster recovery policies should not be confused with disaster recovery plans:

- A disaster recovery plan is a comprehensive program that covers the widest possible scenario, addressing risks such as lack of connectivity, destruction of hardware, data corruption, and cyber attacks.
- A disaster recovery policy defines, concretely, how the organization will behave when a disaster occurs. A disaster recovery plan alone cannot guarantee business continuity without a practical policy that is well understood and practiced by all relevant stakeholders.

Why is Disaster Recovery Policy Important?

In today’s highly digitized world, organizations have become highly reliant on high availability. Downtime is rarely tolerated. And when it comes to mission-critical systems—downtime is not tolerated at all. When disasters strike—a power outage, a ransomware attack, a malicious insider—organizations that are not prepared might suffer significant damage.

The repercussions of a data loss and a successful breach may be different depending on the business and industry. A financial institution handling funds may face not only loss of customer trust but also fines imposed by regulatory entities. When a healthcare facility suffers from downtime or data loss, lives may be in mortal danger.

This is where a disaster recovery policy comes in—this outlines all of the procedures and tools that must be put into place in case of a disaster. Typically, creating a disaster recovery policy involves the use of two important metrics:

YOU'D BETTER INFORM THE BOSS THAT WE'VE GOT A DATA BREACH!
© D.Fletcher for CloudTweaks.com

- Recovery point objective (RPO)—the amount of time that may transpire until recovery from backup repositories during downtime. These files are critical to ensure normal operations. The RPO helps in determining the minimum frequency of backups.

- Recovery time objective (RTO)—the maximum downtime the organization is capable of sustaining. During this time the organization can recover files from local and off-site backup repositories and maintain normal operations.

Types of Disaster Recovery Policies

Virtualized Disaster Recovery

A virtualized environment can help you quickly spin up new virtual machine (VM) instances. This can occur within the span of minutes, ensuring high availability for application recovery. A virtualized disaster recovery policy often provides a high level of efficiency.

Network Disaster Recovery

A network disaster recovery policy can be as complex as the recovered network. This is why the policy should be highly detailed, including a step by step breakdown of all recovery procedures. It is also important to test the policy and keep it up to date.

Cloud Disaster Recovery

There are several ways to use the cloud for disaster recovery. You can back up files in the cloud or maintain complete replicas, enabling you to transition operations to remote cloud resources in case of a disaster. Cloud DR offers compelling advantages, including costs reduction and improved resilience, compared to disaster recovery based on company-owned resources.

© Randy Glasbergen / glasbergen.com

"I used to bury my bones.
Now I upload them to the cloud."

Data Center Disaster Recovery

A data center disaster recovery policy is designed especially for the local facility and its infrastructure. To create a relevant policy, you need to do an operational risk assessment, which analyzes components of the data center. For example, an analysis of the power systems, the location of the facility, the office space, and overall security.

3 Key Elements of Disaster Recovery Policy

The Scope of Your Policy

There are many types of crises that may affect an organization, and in each disaster scenario, every aspect of the organization’s critical assets needs to be protected. However, the exact scope of the policy is limited by the disaster recovery plan. The policy should closely follow the disaster recovery plan, and define specific rules and procedures for each asset that needs to be protected.

Organisational Roles and Responsibilities

To recover from a disaster, you need a disaster recovery team that is familiar with your organization’s documented recovery process. The responsibilities of the recovery team should include immediate actions when a disaster occurs, and post-disaster activities. It should be very clear who is responsible for what—and individuals with certain responsibilities should have the relevant skills and training to perform them. It is important to provide emergency procedures that take into account failure of certain parts of the business infrastructure—for example, how to communicate if there is no cellular connectivity.

A Communication Plan

A disaster recovery policy must include a detailed communication plan, with a list of contacts of people who need to be notified about the disaster. The plan should include precise information protocols—what information to convey, over what channel and in what format, to save time and reduce confusion during a crisis.

Best Practices for a Successful Disaster Recovery Policy

Prepare an Inventory of Assets

You need to understand the hardware, software, and data that are critical to your business. Go over server rooms, data centers, virtual machines (VMs) based on-premises and in the cloud, and endpoints like employee workstations. Review networks, applications, and data stores.

Pay special attention to the configuration of networks, hypervisors and servers that will need to be restored in case of a disaster.

Review Backup Processes

Ensure that each sensitive system has a working backup system, that backups are regularly performed, and there is a tested procedure for recovering these systems from backup. Assess the risk that some systems will not be able to recover from backup, and develop appropriate replacement strategies.

Calculate the Cost of Downtime

Downtime can not only disrupt productivity and cause revenue loss, but also damage a company's reputation and result in legal and compliance violations. Calculating the cost of a potential failure can help you determine your investment in preventive measures.

Regularly Update the Policy

Disaster recovery policies must evolve. You'll need to update it whenever organizational structure, infrastructure, applications or data structure changes. Run regular drills to see if your policy still holds up, or if there are unanticipated changes to systems that need to be accounted for.