NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Disaster Recovery

Cloud Infrastructure Engineering

Nanyang Technological University & Skills Union - 2022/2023

Course Content

- Quick Check-In
- Dive into the basics of Disaster Recovery
- Explore why Disaster Recovery is important
- Create your own Disaster Recovery plan

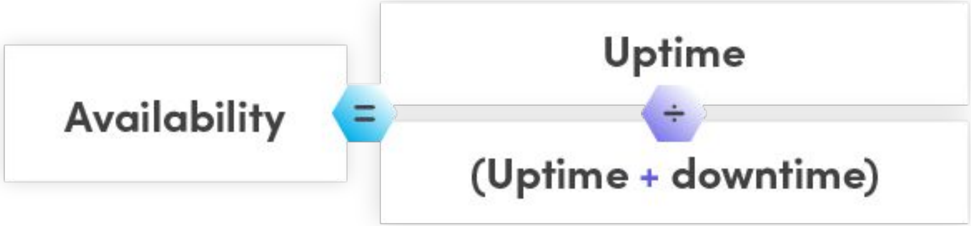
Time	What	How or Why
7:15pm - 7:30pm	Part 1 - Presentation	Disaster Recovery
7:30pm - 7:45pm	Part 2 - Presentation	Importance of Disaster Recovery
7:45pm - 7:55pm	Break	
7:55pm - 8:35pm	Group Assignment	
8:35pm - 9:00pm	Group Sharing	
9:00pm - 9:45pm	Summary	Summary of Module 1 and what to expect for Module 2
9:45pm - 10:00pm	Wrap Up	

Recap

- **Resiliency** - Ability of a storage system to self-heal, recover, and continue operating after encountering failure, outage, security incidents, etc
- **Reliability** - Probability that the storage system (hardware) will work as expected
- **Durability** - Continued persistence of data
- **Availability** - **Amount of time that a service is accessible** and the amount of time it takes for a system to **react to a user's request.**

Recap

- **Factors of HA**
  - Environment/ Location
  - Hardware
  - Software
  - Data
  - Network



$$\text{Availability} = \frac{\text{Uptime}}{(\text{Uptime} + \text{downtime})}$$

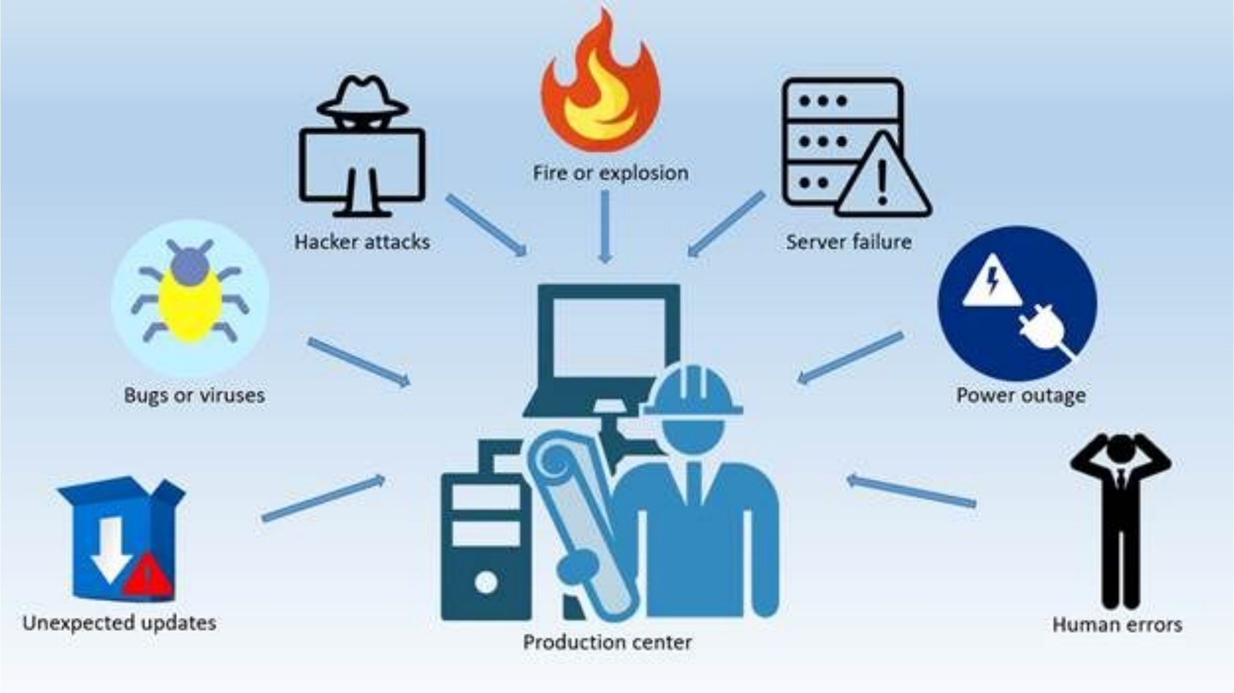
Disaster Recovery

To Begin…

IT infrastructure has become a critical component of today's business world.

As more organizations rely on computing power, storage, and applications, being without these mission-essential assets is an almost unfathomable thought, **underpinning the importance of investing in disaster recovery.**

What is DR?


Fire or explosion
Hacker attacks
Server failure
Bugs or viruses
Power outage
Unexpected updates
Production center
Human errors

What is DR?

Policy and/or process that is designed to assist an organization in **executing recovery processes** in response to a disaster to protect business IT infrastructure and more generally promote recovery.

Disasters take many shapes and forms and can include **cyber-attacks, natural disasters, theft or sabotage, power failures, IT network failures, events affecting an organization's reputation, and also outbreaks of diseases or infections** that impact operations.

What is DR?

Ask these questions:

1. Is my company prepared for a security attack on our servers?
2. Is my company prepared for a natural disaster in one of our data centres?
3. Is my company prepared for an unexpected power outage?
4. Is my company prepared for…….?

What is DR?

The purpose of a disaster recovery is to comprehensively explain the consistent actions that **must be taken BEFORE, DURING and AFTER the disaster** so that the entire team can take those actions.

Disaster recovery **should address and contains detailed instructions** on how to **respond to unplanned incidents** such as natural disasters, power outages, cyber attacks and any other disruptive events.

The plan contains strategies on minimizing the effects of a disaster, so an organization will continue to operate – or quickly resume key operations.

What is Business Continuity?

A very synonymous concept of DR is Business Continuity (COB, BC)

Business Continuity focuses on **keeping business operational** during a disaster, while Disaster Recovery focuses on **restoring data access and IT infrastructure** after a disaster.

What is Recovery Point Objective (RPO)

Describes the **interval of time** that might pass during a disruption before the **quantity of data** lost during that period **exceeds** the Business Continuity Plan’s **maximum allowable threshold** or “tolerance.”

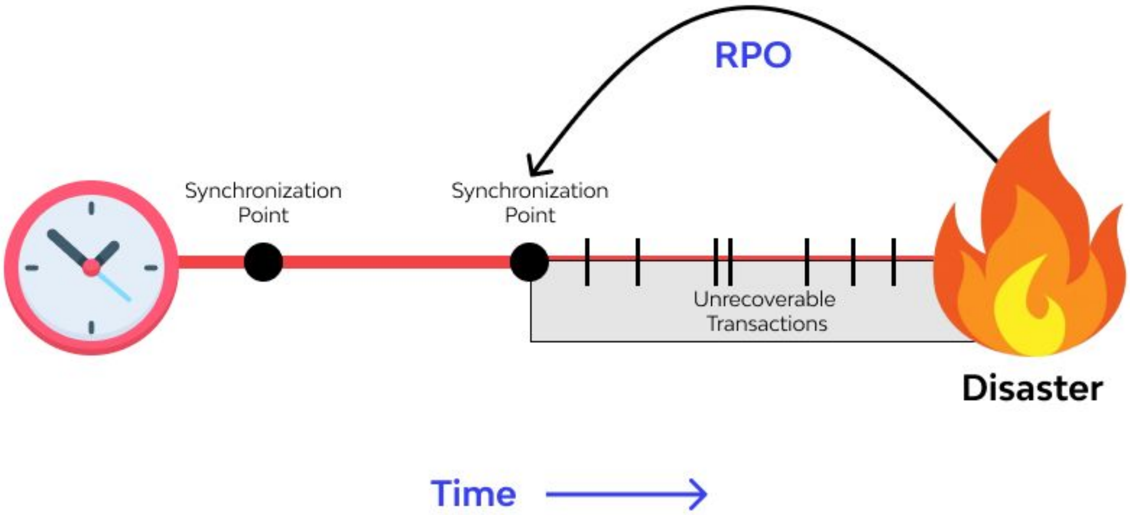
What is Recovery Point Objective (RPO)

Example:

If the last available good copy of data upon an outage is from **18 hours ago,** and the **RPO for this business is 20 hours** then we are still within the parameters of the Business Continuity Plan’s RPO.

In other words it answers the question – “Up to what point in time could the business process’ recovery proceed tolerably given the volume of data lost during that interval?”

What is Recovery Point Objective (RPO)



What is Recovery Time Objective (RTO)

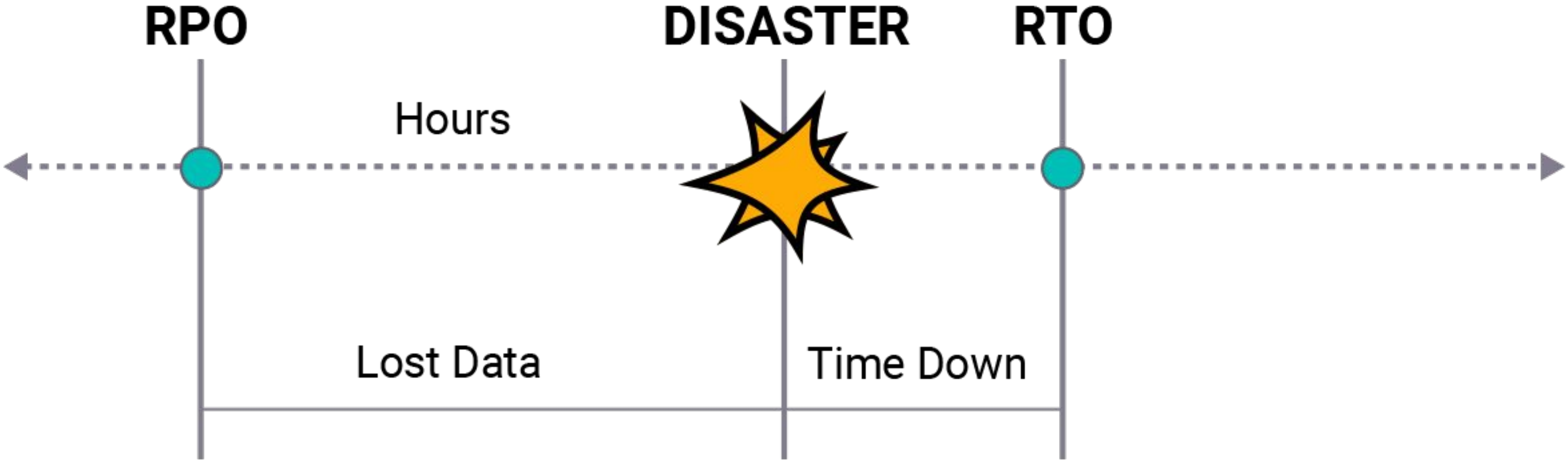
Describes the **duration of time** and a **service level** within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity

What is Recovery Time Objective (RTO)

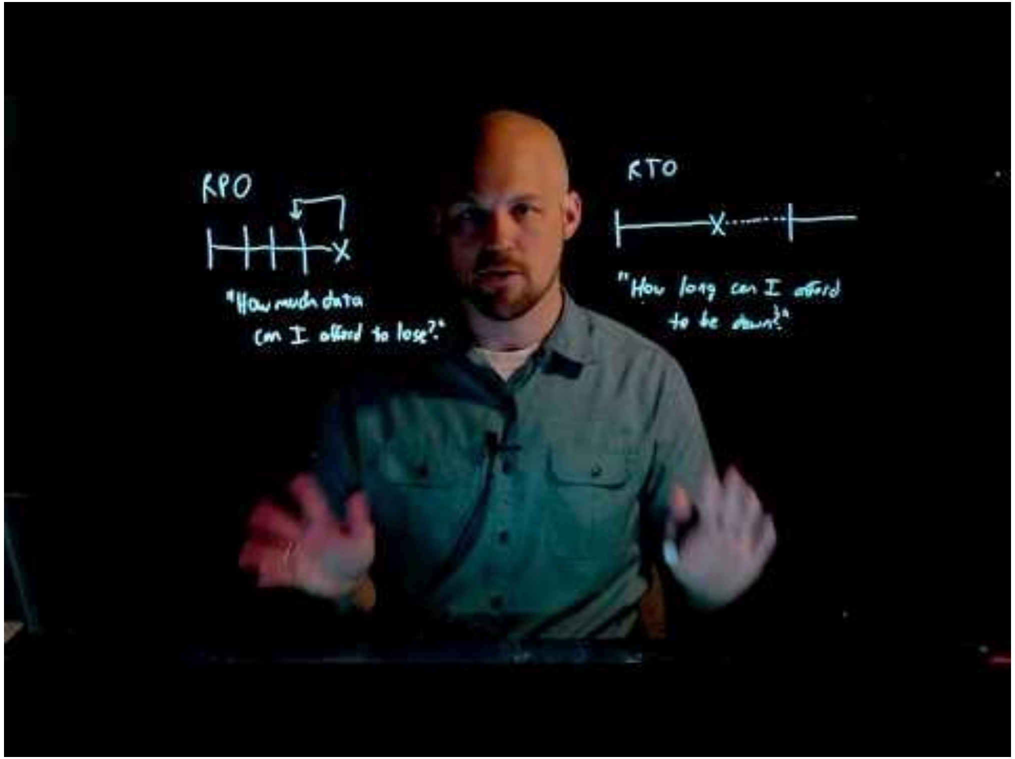
Example:

A **2-hour RTO** means that you give responsible personnel two hours to bring your services back up again. If you managed to recover within 1.5 hours, then you are within the Business Continuity Plan’s RTO.

RTO vs RPO



RTO & RPO


RPO
"How much data can I afford to lose?"
RTO
"How long can I afford to be down?"

BREAK TIME

DR Importance

Why is DR Important?

Disaster recovery offers organizations a means of salvaging their operational capacity and can save them from devastating losses that could lead to a complete shutdown.

By investing in disaster recovery, organizations can **build more resilience** and a **stronger competitive advantage**.

Why is DR Important?

Prevent Revenue Loss

As more businesses rely on technology to operate, IT infrastructure holds tremendous value.

Without an operational IT infrastructure, businesses can suffer significant revenue losses.

Why is DR Important?

Enhance Resilience

Committing to disaster recovery can be costly, however, it **improves** an organization’s **ability to quickly return to business** as usual after a disaster.

Through regular DR testing, organizations developed the resiliency they need to limit the effects of disasters on their operations.

Why is DR Important?

Maintain Customer Satisfaction

DR plans tested **develop resilience** that pays dividends over time. It’s a well-known fact that customer acquisition costs exceed customer retention costs.

By being prepared for disasters, customer attrition is limited if not averted altogether.

Why is DR Important?

Improve Partner Confidence

Due to the connectedness of organizations and their reliance on partner resources and infrastructure, **investing in DR can improve relationships and confidence.**

Why is DR Important?

Overcome Hardware Failure

IT hardware is machinery and, therefore, prone to breakdown and failure. Having a DR plan accounts for outages and prevents unnecessary downtime.

Why is DR Important?

Compliance

As security and privacy grow in importance, new regulations are introduced to protect sensitive information. Investing in a DR plan ensures that you stay ahead of compliance requirements.

DR Importance

Prevent Revenue Loss

Enhance Resilience

Maintain Customer Satisfaction

Improve Partner Confidence

Overcome Hardware Failure

Compliance

Preparing for DR

Preparing for DR

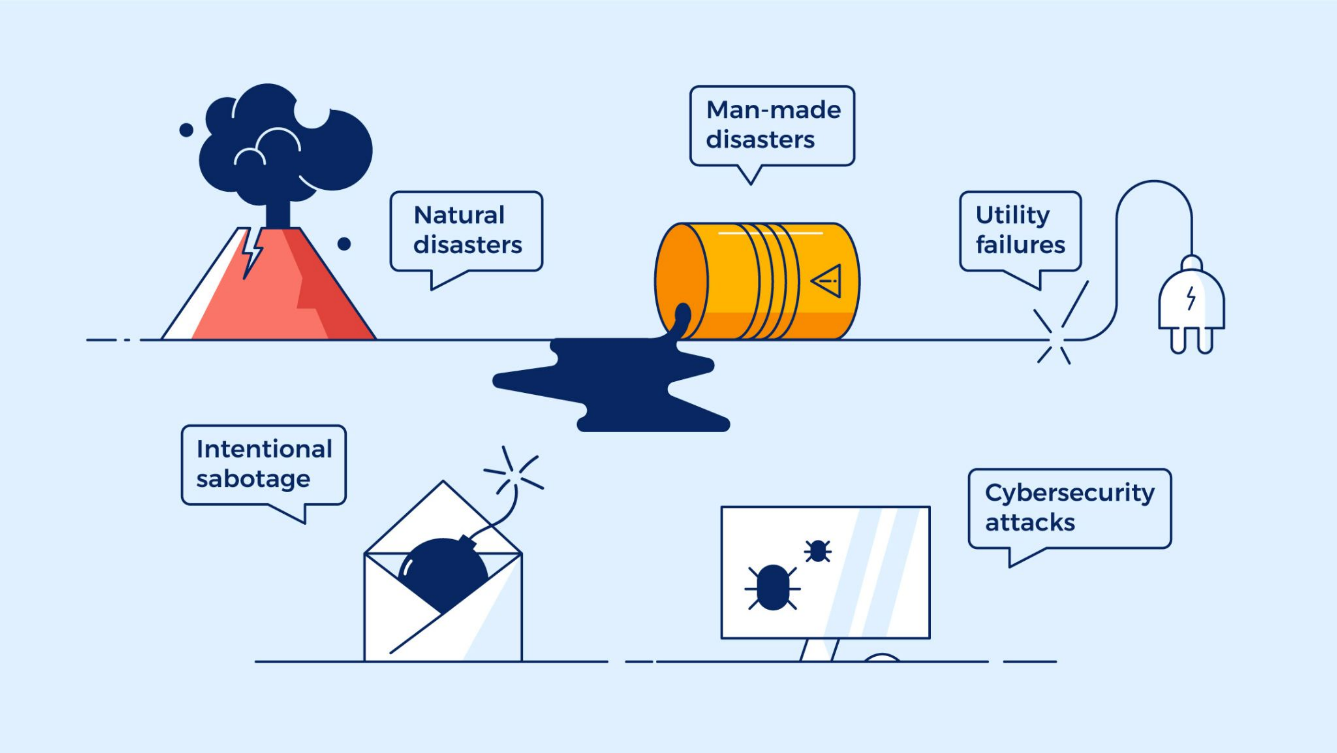
Know Your Company’s Threats

Learn about the history of your business, the industry and the region, and **map out the threats** you are most likely to face.

Threats include natural disasters, geopolitical events like wars or civil unrest, failure to critical equipment like servers, Internet connection or software, and cyber attacks that are most likely to affect your type of business.

Ensure your **disaster recovery plan is effective against all**, or at least the most likely or most significant threats. If necessary, develop separate DR plans or separate sections within your DR plan for specific types of disasters.

Know Your Company’s Threats



Know Your Company’s Assets

Get your team together and make a big list of all the assets that are important for the day-to-day operations of your business.

In the IT sphere this includes network equipment, servers, workstations, software, cloud services, mobile devices, and more.

Know Your Company’s Assets

Critical assets your business cannot operate without – for example, an email server

Important assets that can seriously hamper some activities – for example, a projector used for presentations

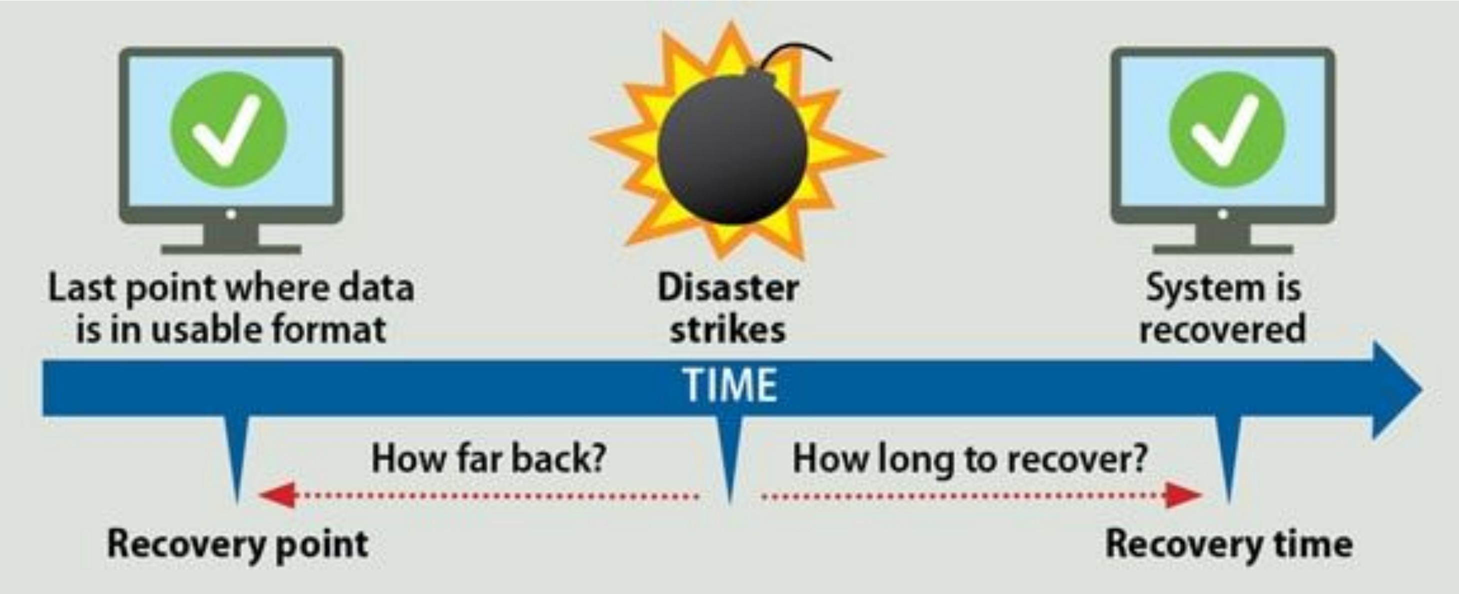
Other assets that will not have a major effect on the business – for example, a recreational system used by employees on their lunch break

Define Your Company’s RPO/ RTO

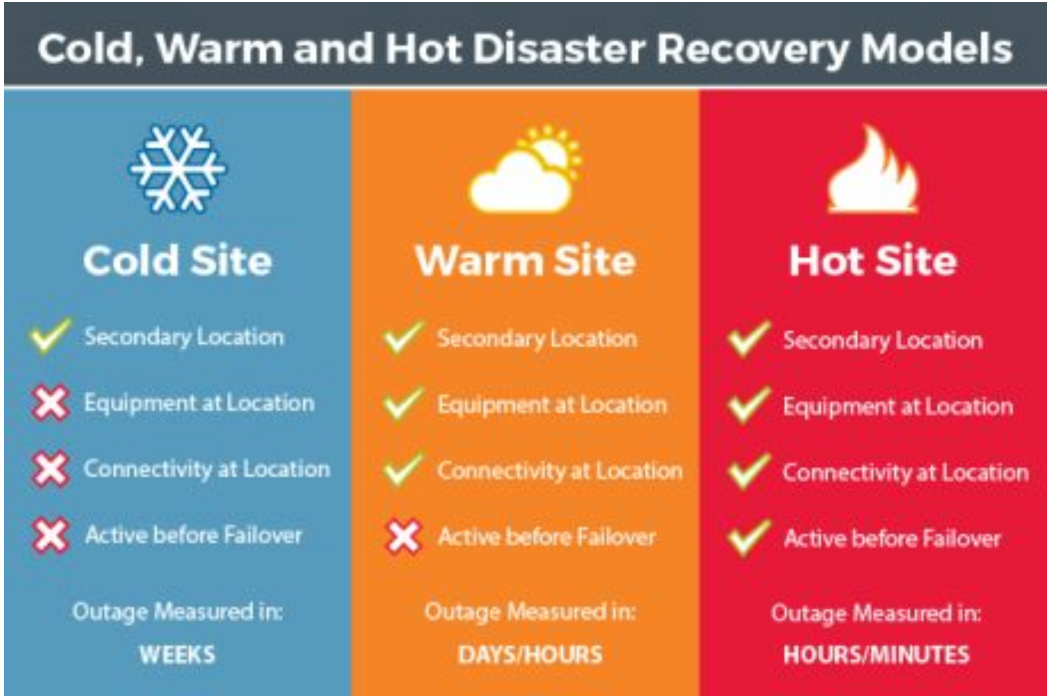
Define your RTO for critical assets. What **period of downtime** can you sustain? Build a process and obtain technological means that can help you bring operations back online within the RTO.

Define your RPO. Organizations use RPO to **determine the minimum frequency of backups**. For example, a four-hour RPO requires backing up at least every four hours.

Define Your Company’s RPO/ RTO



Setup DR Sites



Cold, Warm and Hot Disaster Recovery Models

	Cold Site	Warm Site	Hot Site
Secondary Location	✓	✓	✓
Equipment at Location	✗	✓	✓
Connectivity at Location	✗	✓	✓
Active before Failover	✗	✗	✓
Outage Measured in:	WEEKS	DAYS/HOURS	HOURS/MINUTES

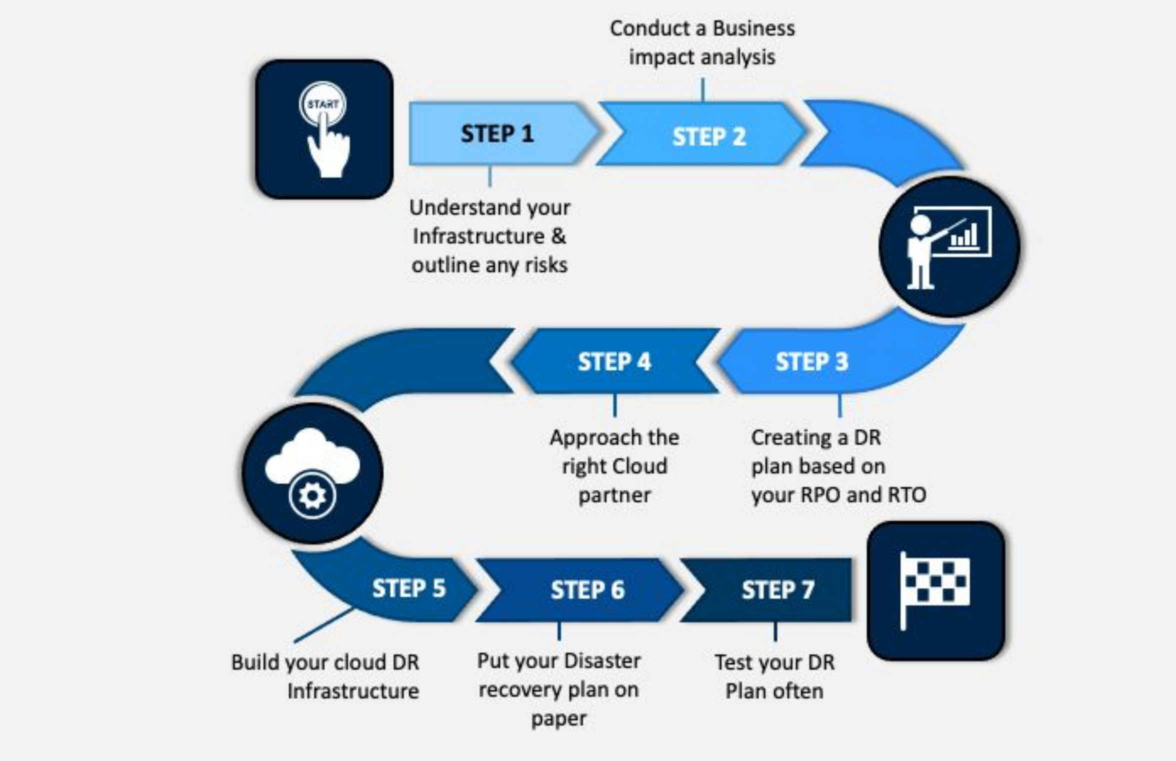
Test Backup & Recovery

An inseparable part of any disaster recovery plan is to **test that data is being replicated correctly to the target location**.

It's just as important to **test that it's possible to restore data** back to your production site.

These **tests must be conducted once**, when you set up your disaster recovery apparatus, and repeated periodically to ensure the setup is still working.

Test Backup & Recovery



START
STEP 1
Understand your Infrastructure & outline any risks
STEP 2
Conduct a Business impact analysis
STEP 3
Creating a DR plan based on your RPO and RTO
STEP 4
Approach the right Cloud partner
STEP 5
Build your cloud DR Infrastructure
STEP 6
Put your Disaster recovery plan on paper
STEP 7
Test your DR Plan often

Summary

- Know Your Company's Threats
- Know Your Company's Assets
- Define Your Company's RTO/RPO
- Setup DR Sites
- Test Backup & Recovery

Summary

Activity Briefing

Group Activity

Work with your group to answer the 2 questions below:

1. What are the differences between HA and DR?
2. What are the similarities between HA and DR?

What’s Next?