# DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVICES

**OBJECTIVES:**

The IBM Cloud service level objectives documentation provides links to the available high availability, DR, and backup information for the IBM Cloud services that can be used as reference documentation in designing and implementing the DR plan. To minimize interruptions to normal operations. To limit the extent of disruption and damage. To minimize the economic impact of the interruption. To establish alternative means of operation in advance.

**Problem Definition:**

The project involves creating a disaster recovery plan using IBM Cloud Virtual Servers. The objective is to safeguard business operations by developing a plan that ensures continuity for an on-premises virtual machine in unforeseen events. This plan will include setting up backup strategies, configuring replication, testing the recovery process, and guaranteeing minimal downtime. The project encompasses defining the disaster recovery strategy, implementing backup and replication, validating recovery procedures, and ensuring business continuity.

**Design Thinking:**

Disaster Recovery Strategy: Define the disaster recovery strategy and objectives, including recovery time objectives (RTO) and recovery point objectives (RPO).

Backup Configuration: Configure regular backups of the on-premises virtual machine to capture critical data and configurations.

Replication Setup: Implement replication of data and virtual machine images to IBM Cloud Virtual Servers to ensure up-to-date copies.

Recovery Testing: Design and conduct recovery tests to validate the recovery process and guarantee minimal downtime.

Business Continuity: Ensure that the disaster recovery plan aligns with the organization's overall business continuity strategy.

Typically, disaster recovery involves securely replicating and backing up critical data and workloads to a secondary location or multiple locations—disaster recovery sites. A disaster recovery site can be used to recover data from the most recent backup or a previous point in time.

Main Disaster Recovery techniques are three:

 synchronous replication, asynchronous replication and mixed technique

The first step to create a disaster recovery plan for cloud is to assess your risks and requirements. You need to identify the potential threats and scenarios that could affect your cloud infrastructure, such as natural disasters, cyberattacks, human errors, or vendor failures.

Disaster recovery (DR) typically refers to ability to restart IT services from a different geographic location and infrastructure. To implement DR, you need a set of data, compute, and network capabilities in the alternative location and the ability to operate and manage them.

Data can be continuously replicated or periodically refreshed. The time difference between the time of disaster and the age of the data images on the DR site is known as the recovery point objective (RPO). The recovery time objective (RTO) is the time to take the copies of data, associate compute and network, and reprovision the IT service from the alternative location.

Accessibility:

Cloud-based applications and data are accessible from virtually any internet-connected device. Speed to market: Developing in the cloud enables users to get their applications to market quickly. Data security: Hardware failures do not result in data loss because of networked backups.