ONE PAGE SUMMARY

IT & Software › Cloud Computing › Disaster Recovery

Introduction to Disaster Recovery

Disaster Recovery: Safeguarding Your Data in the Cloud

DEFINITION

> Disaster recovery is a strategy to restore IT systems and data after a disruption. It ensures business continuity by minimizing downtime and data loss.

KEY CONCEPTS

Backup Solutions

These are methods used to create copies of data to restore in case of loss.

Recovery Time Objective (RTO)

RTO defines the maximum acceptable time to restore services after a disaster.

Recovery Point Objective (RPO)

RPO indicates the maximum acceptable amount of data loss measured in time.

Disaster Recovery Plan (DRP)

A DRP is a documented process to recover and protect a business IT infrastructure.

Cloud-Based Recovery

This involves using cloud services to store backups and facilitate quick recovery.

EXAMPLES

→ A company uses cloud backups to recover data after a server failure.

→ A business restores its operations within 4 hours after a natural disaster.

→ A firm implements a DRP to ensure data is backed up every hour.

MEMORY TIPS

★ Remember RTO as 'Return Time Objective' for quick recovery.

★ Think of RPO as 'Recent Point Objective' to minimize data loss.

★ Use the acronym DRP to recall 'Disaster Recovery Plan' easily.

COMMON MISTAKES

✗ Neglecting to regularly test the disaster recovery plan.

✗ Underestimating the importance of RTO and RPO.

✗ Failing to update backups after significant data changes.

QUICK RECAP

Disaster recovery is essential for maintaining data integrity and business operations after disruptions. Key concepts include RTO, RPO, and having a solid DRP in place. Regular testing and updates are crucial for effective recovery strategies.