Section - 4

Disaster Recovery and Business Continuity Planning

4.1 Introduction to Disaster Recovery (DR) and Business Continuity (BC)

Explanation:

- **Disaster Recovery (DR)** ensures systems can **recover quickly** after an unexpected event like hardware failures, cyberattacks, or natural disasters.

- **Business Continuity (BC)** ensures that **critical business operations** continue during and after such disruptions.

Key Goals:

- Minimize downtime
- Protect data
- Maintain customer trust

Real-world Example:

An online bank implements a disaster recovery site in another region to ensure customers can always access accounts even if the primary site is down.

4.2 Key Concepts: RPO and RTO

RPO (Recovery Point Objective):

- How much **data loss** is acceptable? (e.g., last 5 minutes, 1 hour)

RTO (Recovery Time Objective):

- How quickly must systems **be back online**? (e.g., 15 minutes, 2 hours)

Real-world Example:

A stock trading platform sets an RPO of 30 seconds (minimal data loss) and an RTO of 5 minutes (very fast recovery).

4.3 Types of Disaster Recovery Strategies

1. Backup and Restore:

- Simple backups (daily, weekly)
- Restores systems manually after a failure.

2. Pilot Light:

- Minimal version of environment always running.
- Quickly scale it up when disaster strikes.

3. Warm Standby:

- A scaled-down but **live** environment.
- Minimal time to switch.

4. Multi-site Active-Active:

- Fully running environments in **multiple locations**.
- Instant failover — expensive but highly resilient.

Real-world Example:

An airline uses a warm standby approach, running essential services at reduced capacity in a second region.

4.4 Google Cloud Tools for DR Planning

Tools:

- **Cloud Storage:** Object storage backups.
- **Cloud SQL Backups:** Automated backups for managed databases.
- **Compute Engine Snapshots:** VM disk backups.
- **Persistent Disk Replication:** Cross-zone and cross-region replication.

Real-world Example:

An online learning platform schedules daily snapshots of all production VMs and replicates them to another region.

4.5 Disaster Recovery Design Patterns

1. Regional Redundancy:

- Deploy workloads across multiple zones within a region.

2. Multi-Regional Redundancy:

- Deploy across entirely different Google Cloud regions.

3. Stateless Architectures:

- Use stateless microservices that can be restarted anywhere.

4. Data Replication:

- Ensure database replication across regions (Cloud Spanner, etc.)

Real-world Example:

A music streaming service uses Google Cloud Load Balancers to automatically route traffic to the nearest healthy regional deployment.

4.6 Business Continuity Planning

Steps for BC Planning:

- Identify critical processes
- Conduct risk assessment
- Prepare communication plans
- Document and test the BC Plan
- Update BC Plan regularly

Real-world Example:

A logistics company creates a BC Plan that includes alternative warehouses and transportation routes in case of regional disasters.

4.7 Testing and Validation of DR and BC Plans

Best Practices:

- Perform regular **failover drills**.
- Simulate different disaster scenarios.
- Test recovery of backup data.
- Measure RPO and RTO during drills.

Real-world Example:

A healthcare provider conducts quarterly disaster simulations including the failure of primary cloud services and successful failover to backups.