DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

Problem statement:

* Safeguard business operations with IBM Cloud Virtual Servers. Create a disaster recovery plan for an on-premises virtual machine, ensuring continuity in unforeseen events.
* Test and validate the recovery process to guarantee minimal downtime. Become the guardian of business continuity, securing the future of your organization!

PHASE 1: Problem Definition and Design Thinking (Assignment 1)

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.

1.Disaster Recovery Strategy:

**Assessment**: Begin by thoroughly assessing your existing IT infrastructure, identifying critical assets, and evaluating potential risks or vulnerabilities.

 RTO and RPO: Determine your Recovery Time Objective (RTO), which is the maximum tolerable downtime, and your Recovery Point Objective (RPO), indicating how much data loss is acceptable.

**Cloud Resources**: Select the specific IBM Cloud virtual servers, services, and resources that will be part of your disaster recovery plan.

**Communication Plan**: Create a well-defined communication plan that outlines how your team will be notified and how stakeholders will be informed during a disaster event.

2.Backup Configuration:

**Data Backup**: Regularly back up your critical data, configurations, and system settings. These backups should be stored securely on IBM Cloud Object Storage or another reliable storage solution.

**Automation:** Employ automation tools to schedule and manage backups. Automation helps ensure consistency and minimizes the risk of human error.

**Encryption**: Implement encryption for your backup data to maintain its confidentiality and integrity.

3. Replication Setup:

**Data Replication**: Set up data replication mechanisms between your primary and secondary IBM Cloud virtual servers. Real-time or near-real-time replication helps keep data consistent between locations.

**Load Balancing**: Configure load balancing to distribute incoming traffic evenly between primary and secondary servers, enhancing efficiency and resilience.

**Failover Mechanism**: Establish automatic failover processes to seamlessly redirect traffic to secondary servers in the event of a disaster, reducing downtime.

4. Recovery Testing:

**Regular Testing**: Conduct periodic disaster recovery tests to validate the effectiveness of your plan. This involves simulating various disaster scenarios.

**Testing Scenarios**: Create and execute testing scenarios that mimic different types of disasters, such as hardware failures, data corruption, or network outages.

    Documentation**: Document the results of your recovery tests, including any issues** encountered. Use these findings to improve and refine your disaster recovery procedures.

5. Business Continuity:

**Redundancy:** Ensure redundancy for critical components of your virtual server infrastructure to minimize single points of failure.

**Geographic Diversity:** Deploy your virtual servers in multiple IBM Cloud regions to achieve geographic diversity, reducing the risk of regional disasters impacting your operations.

**Monitoring:** Implement continuous monitoring and alerting to detect potential issues proactively, allowing you to take corrective action before they affect business operations.

**Training:** Provide training for your IT staff to ensure they are proficient in executing the disaster recovery plan effectively during high-pressure situations.