PROJECT PHASE 3

PROJECT TITLE : Disaster recovery with IBM cloud servers

Phase 3: Development part 1

- **Introduction :**

Disaster recovery (DR) planning is a critical component of any business's IT strategy, and when you're working with IBM Cloud servers, there are several steps you can take to ensure that your applications and data are protected in the event of a disaster. This is part 1 of a guide on disaster recovery with IBM Cloud servers, focusing on the development and planning stages.

1. Define Your Recovery Objectives:

Determine your Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum allowable downtime, while RPO is the maximum amount of data loss acceptable.

2. Assess Your Infrastructure:

Document your existing infrastructure, including IBM Cloud server configurations, data center locations, and network topology.

3. Identify Critical Applications and Data:

Identify which applications and data are critical to your business operations. Prioritize them for recovery.

4. Backup and Replication Strategy:

Implement a backup and replication strategy for your IBM Cloud servers. IBM offers services like IBM Cloud Object Storage and IBM Cloud Virtual Servers that can assist with this.

5. Choose a DR Solution:

Evaluate IBM Cloud's DR services like IBM Cloud Virtual Servers for VPC (Virtual Private Cloud) and IBM Cloud Resiliency Orchestration for automated recovery options.

6. Create a Disaster Recovery Plan:

Develop a comprehensive DR plan that outlines the steps to take in the event of a disaster. Ensure that it's well-documented and easily accessible to your IT team.

7. Test Your DR Plan:

Regularly test your DR plan to ensure that it works as expected. Simulate disaster scenarios to validate recovery procedures.

8. Data Replication and Synchronization:

Implement data replication and synchronization between your primary and secondary data centers or IBM Cloud regions to maintain up-to-date copies of your critical data.

9. Consider Geographical Diversity:

If possible, choose IBM Cloud data centers or regions that are geographically diverse to minimize the impact of localized disasters.

10. Security and Compliance:

Ensure that your DR plan adheres to security and compliance requirements, especially if you deal with sensitive data.

11. Disaster Recovery Team:

Appoint a dedicated team responsible for DR. Define roles and responsibilities, and ensure team members are trained for their roles.

12. Communication Plan:

Develop a communication plan to keep stakeholders, employees, and customers informed during a disaster event.

13. Documentation and Reporting:

Keep detailed records of all DR activities, including tests, failovers, and recoveries. These records are invaluable for auditing and improving your DR strategy.

14. Regular Updates and Maintenance:

Your DR plan should be a living document that's regularly updated to reflect changes in your infrastructure, applications, and business needs.

This is Part 1 of the disaster recovery guide for IBM Cloud servers. Part 2 will cover the implementation and ongoing management of your disaster recovery strategy using IBM Cloud services. Remember that disaster recovery is an ongoing process, and it's essential to adapt and improve your plan as your business evolves.