**Disaster Recovery Implementation Plan with IBM**

**Cloud virtual servers**

**1. Introduction**

1.1 Purpose

The purpose of this plan is to ensure the availability and continuity of critical virtual servers in the event of a disaster or system failure within the IBM Cloud Foundry environment.

1.2 Scope

This plan covers the implementation of disaster recovery procedures for virtual servers hosted on the IBM Cloud Foundry platform, including the setup, configuration, and testing of the recovery processes.

**2. Business Impact Analysis**

2.1 Critical Systems and Applications

Identify the critical virtual servers and their associated applications that require a robust disaster recovery solution to minimize downtime and data loss.

2.2 Potential Risks and Vulnerabilities

Evaluate potential risks and vulnerabilities that could impact the availability and integrity of the virtual servers within the IBM Cloud Foundry environment.

2.3 Impact Analysis

Assess the potential impact of server downtime and data loss on business operations, customer experience, and overall organizational productivity.

**3. Disaster Recovery Strategy**

3.1 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Define the acceptable duration of downtime (RTO) and the maximum tolerable data loss (RPO) for each virtual server to determine the appropriate disaster recovery strategy.

3.2 Backup and Replication Strategy

Implement a robust backup and replication strategy using IBM Cloud Foundry's built-in tools to ensure the continuous synchronization of data between primary and secondary environments.

3.3 Failover and Failback Procedures

Establish clear failover and failback procedures to enable a seamless transition to the secondary environment during a disaster and ensure a smooth return to the primary environment once it's restored.

**4. IBM Cloud Foundry Setup and Configuration**

4.1 Overview of IBM Cloud Foundry

Provide an overview of the IBM Cloud Foundry platform, including its features, capabilities, and how it facilitates the deployment and management of virtual servers.

4.2 Setting Up Virtual Servers in IBM Cloud Foundry

Detail the steps involved in setting up virtual servers within the IBM Cloud Foundry environment, including server provisioning, network configuration, and resource allocation.

4.3 Configuring High Availability and Redundancy

Configure high availability and redundancy settings for critical virtual servers to minimize the risk of downtime and ensure continuous availability of services.

**5. Disaster Recovery Implementation**

5.1 Establishing a Secondary Data Center

Set up a secondary data center within the IBM Cloud environment to serve as a failover location for critical virtual servers in case of a disaster or system failure.

5.2 Configuring Replication between Primary and Secondary Data Centers

Configure data replication mechanisms between the primary and secondary data centers to ensure data consistency and integrity across both environments.

5.3 Testing the Failover Procedures

Regularly test the failover procedures to validate the effectiveness of the disaster recovery plan and identify any potential issues or shortcomings that need to be addressed.

**6. Maintenance and Testing**

6.1 Regular Maintenance Checks and Updates

Perform regular maintenance checks and updates on the disaster recovery infrastructure to ensure its readiness and reliability in the event of a disaster.

6.2 Testing the Disaster Recovery Plan

Conduct periodic tests of the disaster recovery plan to verify its effectiveness and make necessary adjustments based on the test results and feedback from the testing process.

6.3 Documenting and Reporting Test Results

Document all testing activities, including test results, observations, and recommendations, and report the findings to the relevant stakeholders for review and further action.

**7. Communication Plan**

7.1 Stakeholder Communication Strategy

Develop a communication strategy to keep stakeholders informed about the disaster recovery plan, including their roles and responsibilities during a disaster event.

7.2 Communication Channels during Disasters

Establish communication channels that enable effective and timely communication among the disaster recovery team members and key stakeholders during a disaster situation.

**8. Training and Awareness**

8.1 Training for Disaster Recovery Team

Provide comprehensive training to the disaster recovery team members to ensure they are proficient in executing the disaster recovery procedures and handling emergency situations effectively.

8.2 Raising Awareness Among Employees

Raise awareness among all employees about the importance of the disaster recovery plan and their roles in supporting the successful execution of the plan during a disaster event.

**9. Plan Review and Revision**

9.1 Regular Plan Review

Conduct regular reviews of the disaster recovery plan to assess its relevance, effectiveness, and alignment with the evolving business requirements and technological advancements.

9.2 Revision Process and Documentation

Establish a systematic process for revising the disaster recovery plan based on the findings from the plan reviews and document all revisions to maintain an updated and comprehensive plan.

**10. Conclusion**

10.1 Summary of the Disaster Recovery Implementation Plan

Summarize the key components of the disaster recovery implementation plan, highlighting its critical elements and emphasizing the importance of maintaining a robust and reliable disaster recovery strategy.

10.2 Next Steps

Outline the next steps for the ongoing management and maintenance of the disaster recovery plan, including specific action items, timelines, and responsible stakeholders for each task.