**PHASE 4-DEVELOPMENT PART 2**

**Configure Replication:**

Configuring data replication is a fundamental aspect of your disaster recovery plan. This step ensures that your data is continuously synchronized and available for failover to the IBM Cloud Virtual Servers.

Here's a more detailed breakdown of the replication setup:

**A. Data Replication Configuration:**

1. Select a Replication Solution: Choose a replication solution suitable for your environment. IBM Cloud offers services like IBM Cloud Continuous Data Replication, which enables near-real-time replication.

2. Install Replication Agents: Install replication agents or tools on your on-premises virtual machine(s) to capture and transmit data changes.

3. Configuration Parameters: Configure replication parameters, including source and target locations, replication schedules, bandwidth limitations, and encryption settings for secure data transmission.

4. Data Consistency: Ensure data consistency and integrity during replication. Consider using consistency checkpoints and synchronization policies.

**B. Virtual Machine Replication:**

1. Replication Targets: Create the corresponding virtual servers on IBM Cloud, where the replicated VMs will run.

2. Virtual Machine Image Replication: Use tools like IBM Cloud Continuous Data Replication to replicate the virtual machine image and data from your on-premises VM to the IBM Cloud Virtual Server.

3. Network Configuration: Ensure that the networks in IBM Cloud are properly configured to support the replicated VMs. This includes subnets, firewall rules, and security group settings.

**Testing Recovery Procedures**:

After you've configured replication, it's crucial to thoroughly test your recovery procedures to ensure that they work as intended. This involves simulating a disaster scenario and practicing the recovery process. Here's how to approach this:

**A. Failover Testing:**

1. Simulate Disaster: Trigger a simulated disaster scenario on your on-premises VM. This could involve shutting down the VM, simulating data corruption, or other predefined failure conditions.

2. Initiate Failover: Activate the recovery process, switching to the replicated VM on IBM Cloud. This should involve automated failover processes, such as using IBM Cloud Load Balancer to route traffic to the cloud-based VM.

3. Monitor and Verify: Monitor the recovery process closely to ensure it completes successfully. Verify that the application and data are available on the IBM Cloud Virtual Server.

**B. Data and Application Testing:**

1. Data Integrity: Validate that the data replicated to the cloud matches the source data. This can involve checksum verification or data comparison.

2. Functional Testing: Conduct functional testing to confirm that your applications operate correctly on the recovered virtual machine.

**C. RTO and RPO Verification:**

1. Recovery Time Objective (RTO): Measure the time it took to recover your system. Ensure it aligns with your defined RTO.

2. Recovery Point Objective (RPO): Confirm that the amount of data loss during the failover adheres to your defined RPO.

**D. Documentation and Evaluation:**

1. Document the results of your recovery test, including any issues encountered and the time taken for recovery.

2. Evaluate the effectiveness of the recovery plan and identify any areas for improvement. Make necessary adjustments to the plan based on your findings.

**E. Regular Testing:**

Perform recovery tests and drills on a regular schedule, as this helps ensure that your disaster recovery plan remains up-to-date and your team is prepared to respond effectively in case of a real disaster.

Keep in mind that this is a complex process, and real-world implementation may involve additional considerations, such as automated monitoring, alerting, and coordination with relevant stakeholders. It's crucial to involve your disaster recovery team and experts who understand your infrastructure to ensure the plan is robust and reliable.