Step 1: Implement Replication to IBM Cloud Virtual Servers

1. **Select Replication Method**: Choose an appropriate replication method based on your requirements. Common methods include block-level replication, file-level replication, or image-based replication. For this scenario, consider using image-based replication, which can capture the entire virtual machine state.
2. **Set Up IBM Cloud Virtual Servers**: If you haven't already, create the virtual servers in IBM Cloud that will serve as your disaster recovery targets. Ensure they have the required resources to accommodate the replicated data and VMs.
3. **Choose Replication Software**: Select a replication software or tool that's compatible with your on-premises environment and IBM Cloud. IBM Cloud offers various solutions for this, such as IBM Cloud Continuous Data Replicator or third-party tools like Veeam, Zerto, or AWS DataSync.
4. **Configure Replication**: Set up replication between your on-premises infrastructure and IBM Cloud Virtual Servers. This involves configuring source and target endpoints, selecting the data to replicate, and specifying the replication frequency.
5. **Monitor and Test Replication**: Regularly monitor the replication process to ensure it's functioning as expected. Test the replication by triggering manual failovers to the IBM Cloud Virtual Servers to verify data consistency and integrity.

Step 2: Conduct Recovery Tests

It's essential to regularly test your disaster recovery plan to ensure it works as intended and that your team is familiar with the procedures.

1. **Schedule Test Scenarios**: Create a testing schedule that includes various disaster scenarios, such as hardware failures, data corruption, or site-wide outages. Ensure the testing scenarios cover both data and virtual machine recovery.
2. **Simulate Disaster Events**: Simulate the chosen disaster scenarios. For example, for a hardware failure scenario, you can temporarily

disconnect a critical server or storage device in your on-premises environment.
3. **Initiate Recovery Procedures**: In response to the simulated disaster, initiate the recovery procedures you've documented in your disaster recovery plan. This might include initiating failover to the IBM Cloud Virtual Servers, restoring data from backups, and reconfiguring network settings.
4. **Document Results**: Keep detailed records of each test, including the time it took to recover, any issues encountered, and the overall success of the recovery process.
5. **Iterate and Improve**: Based on the results of your tests, make necessary improvements to your disaster recovery plan. If you encounter issues during the tests, identify the root causes and adjust your procedures accordingly.
6. **Training and Awareness**: Ensure that your IT staff is well-trained in disaster recovery procedures and that all relevant personnel are aware of their roles during recovery efforts.
7. **Regularly Review and Update**: Disaster recovery plans are not static. Regularly review and update your plan as your infrastructure, applications, and business needs evolve.

By following these steps, you'll be well-prepared to respond effectively to disasters and maintain business continuity. Remember that testing and documentation are critical to ensuring the success of your disaster recovery plan.