IBM Cloud Application

# Disaster Recovery with IBM Cloud Virtual Servers

# Phase 4

# Development Part 2:

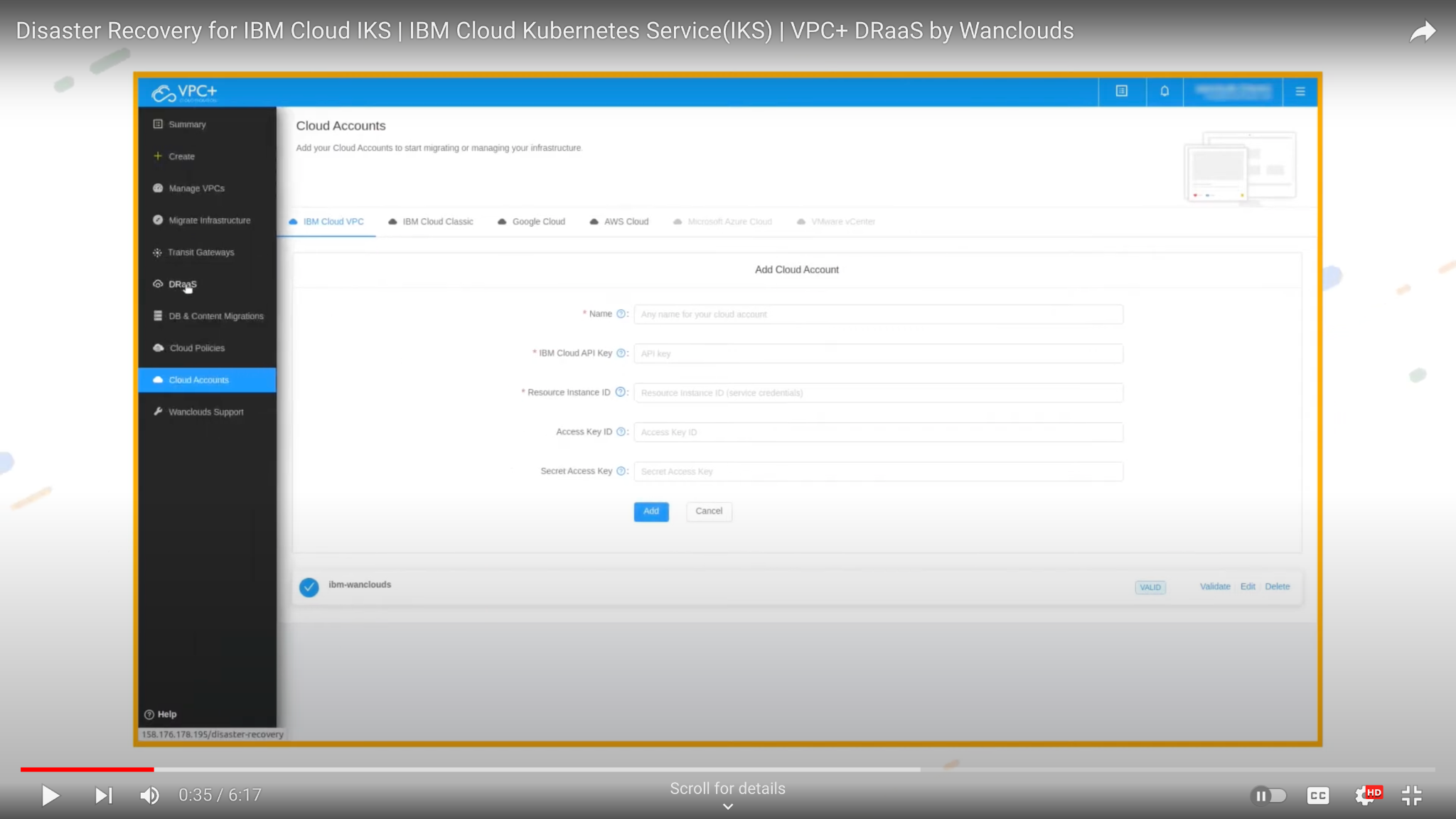
## **Continuing Disaster Recovery Enhancement**

In Phase 4 of our disaster recovery project, we aim to further enhance our disaster recovery plan by focusing on configuring replication and testing recovery procedures. This phase is instrumental in ensuring that our disaster recovery plan is not only robust but also fully functional. We will delve into the intricate details of implementing replication from onpremises to IBM Cloud Virtual Servers and rigorously test the effectiveness of our plan

## **Step 1: Creating a VPC Account**

To proceed with data replication, it is essential to set up an IBM Virtual Private Cloud (VPC) account, which will act as the bridge between your onpremises infrastructure and the IBM Cloud Virtual Servers.

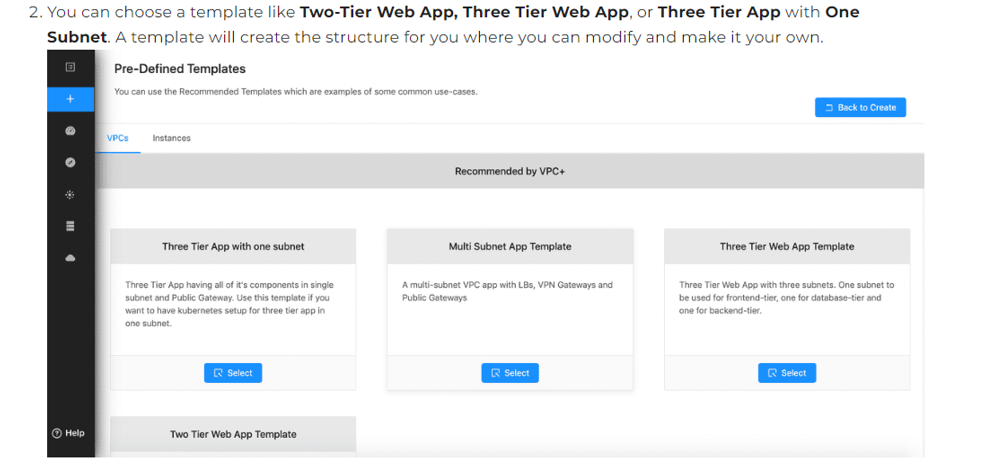
* Log in to your IBM Cloud account and navigate to the Virtual Private Cloud (VPC) dashboard.
* Select "Add Cloud Account."
* In the following window, provide the required information, including the API key and an appropriate account name.
* Click "Add" to finalize the setup of your VPC account. This account will play a crucial role in data replication between onpremises and IBM Cloud Virtual Servers.



## **Step 2: VPC Templates**

IBM provides templates to facilitate the creation of VPCs for your data replication needs. These templates are designed to streamline the process and ensure compatibility with IBM Cloud Virtual Servers.

* Browse the available VPC templates and select the one that aligns with your specific requirements. The templates are built to meet various use cases and offer flexibility in terms of network configuration and security settings.
* Follow the guided setup to create your VPC, ensuring that it integrates seamlessly with your disaster recovery plan. It is important to choose a template that complements your replication strategy.



## **Step 3: Implementing Replication**

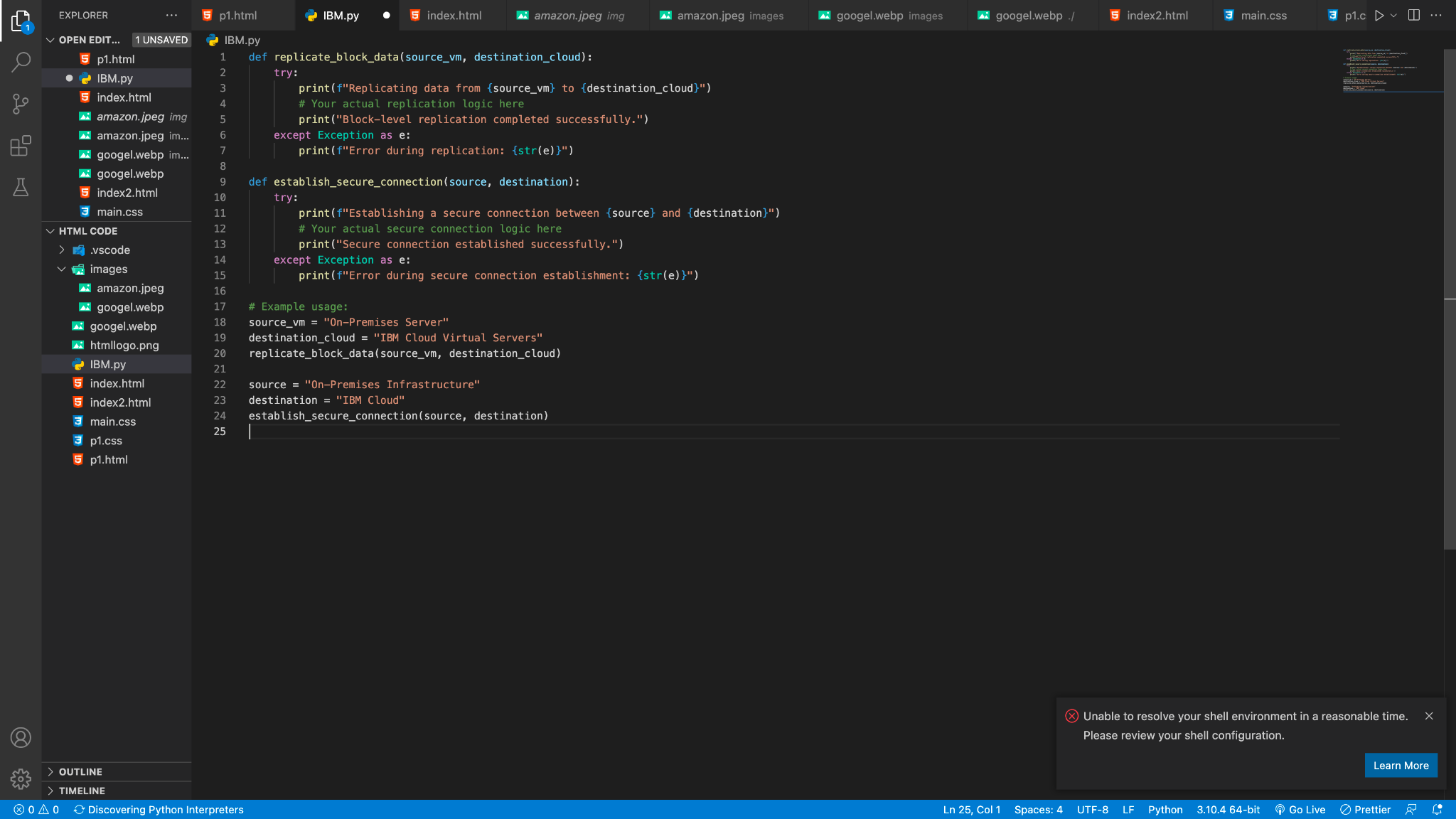
Data replication is a critical component of your disaster recovery plan. It involves ensuring that data and virtual machine images from your onpremises infrastructure are synchronized with IBM Cloud Virtual Servers. The replication method chosen should align with the specific needs and constraints of your organization.

### **Replication Method Selection**

BlockLevel Replication: This method involves copying data at the block level, ensuring that any changes made to data onpremises are quickly mirrored in the IBM Cloud.

### **Secure Connection**

Establish a secure and reliable connection between your onpremises infrastructure and IBM Cloud Virtual Servers. This connection is crucial for ensuring that data is transferred without compromise.



### **Recovery Testing**

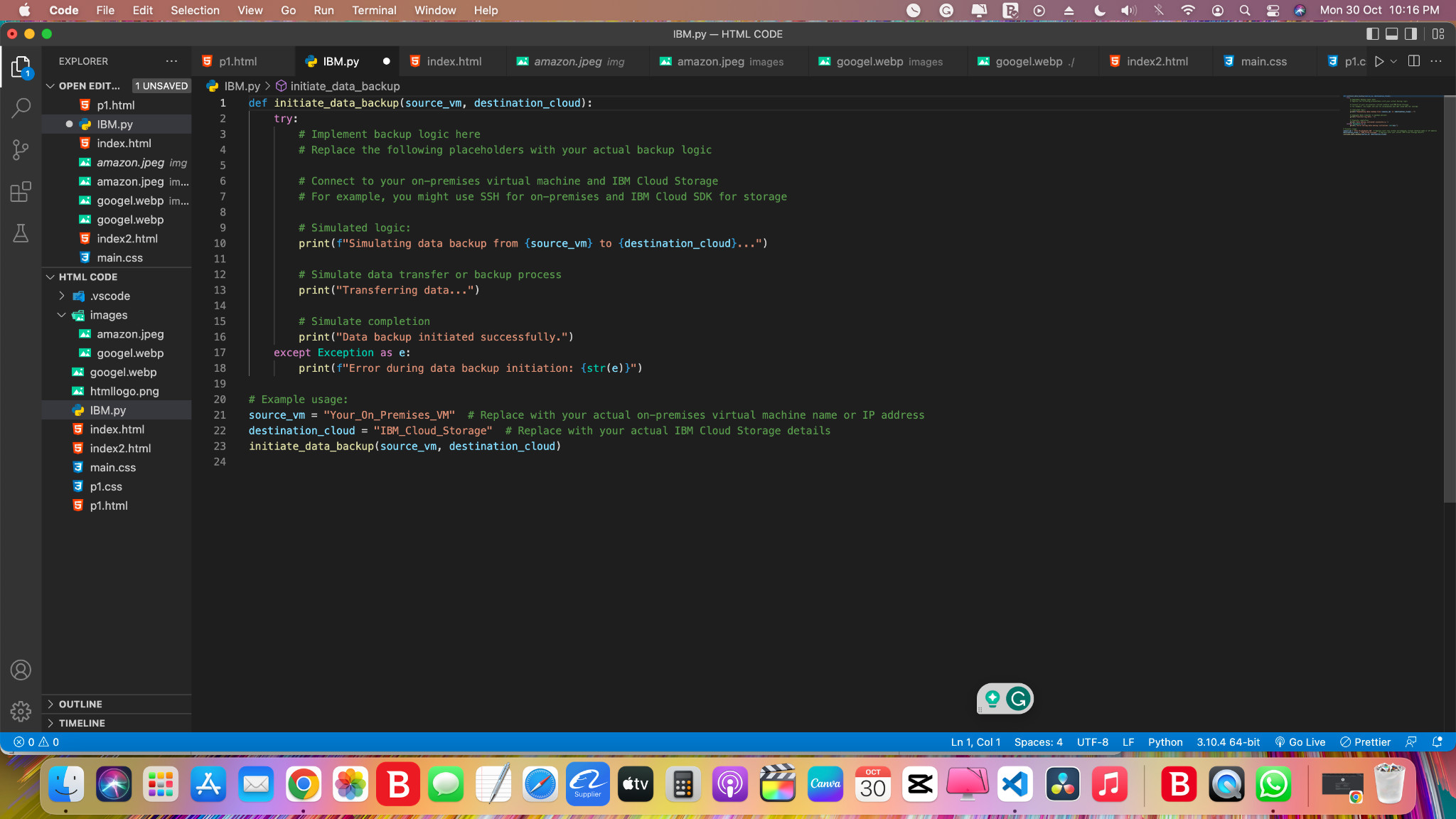
Testing and validation of your disaster recovery plan are imperative to ensure that the plan works as intended and can minimize downtime. It is essential to simulate disaster scenarios and practice recovery procedures rigorously. Here are the detailed steps for recovery testing.

## **Step 4: Backup Strategies Using Virtual Servers**

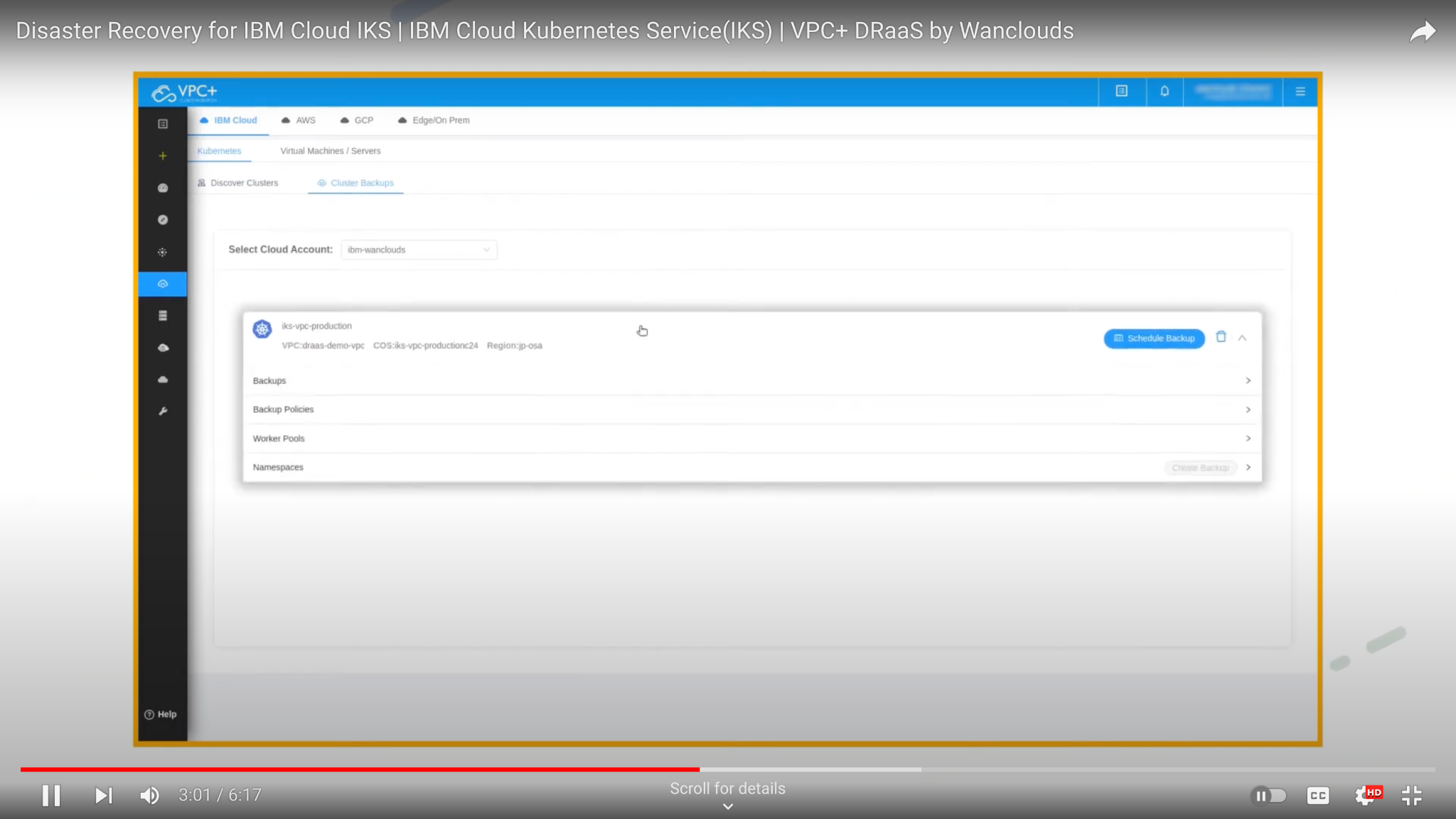
In this phase, backup strategies are pivotal to the recovery process. Here's an overview of backup strategies that leverage Virtual Servers.

### **Data Backup and Restoration**

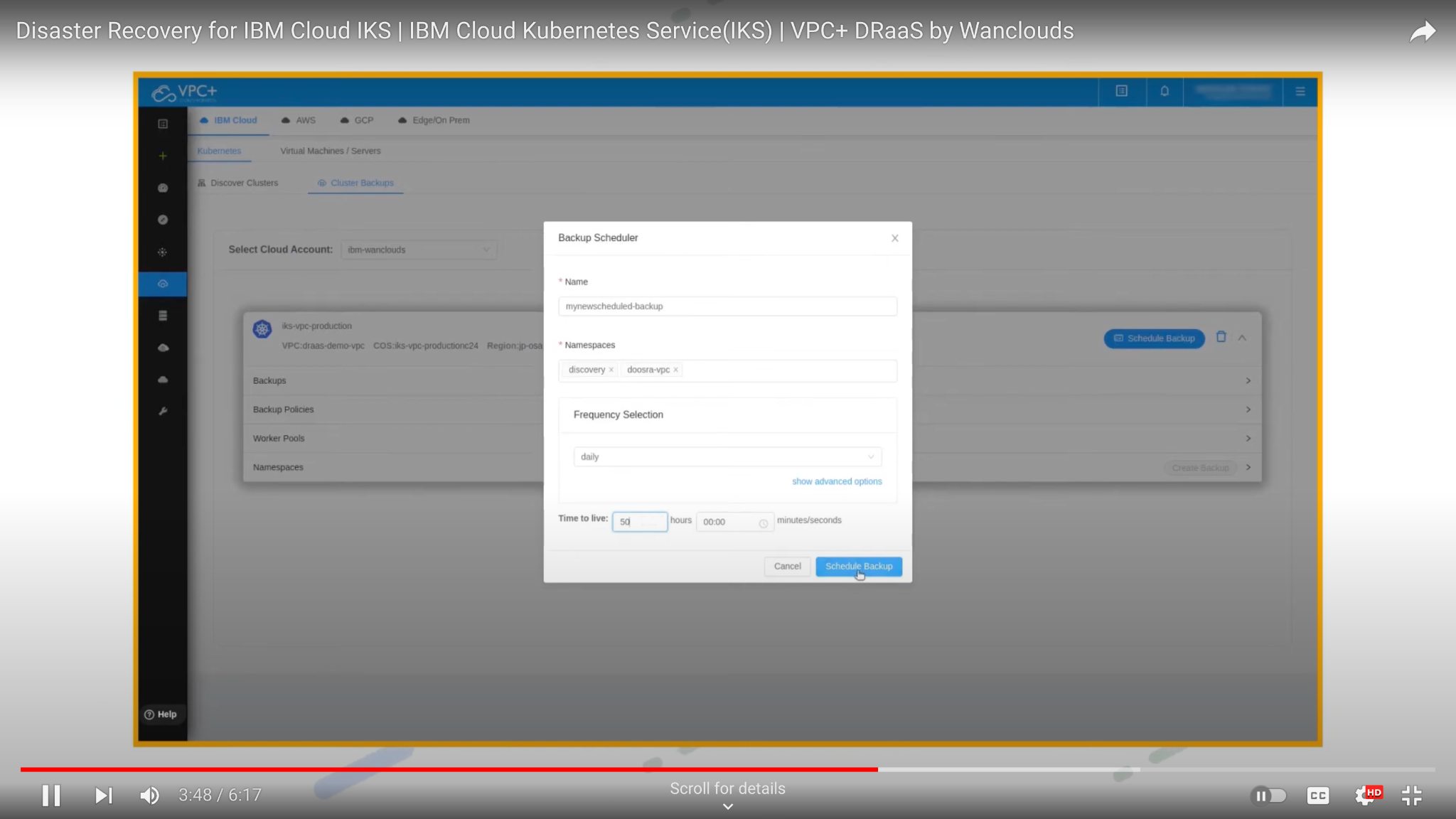
Configure your disaster recovery plan to initiate regular data backups of onpremises virtual machines. Ensure that these backups include critical data and configurations.



### **IBM Server**



### **IBM backup**

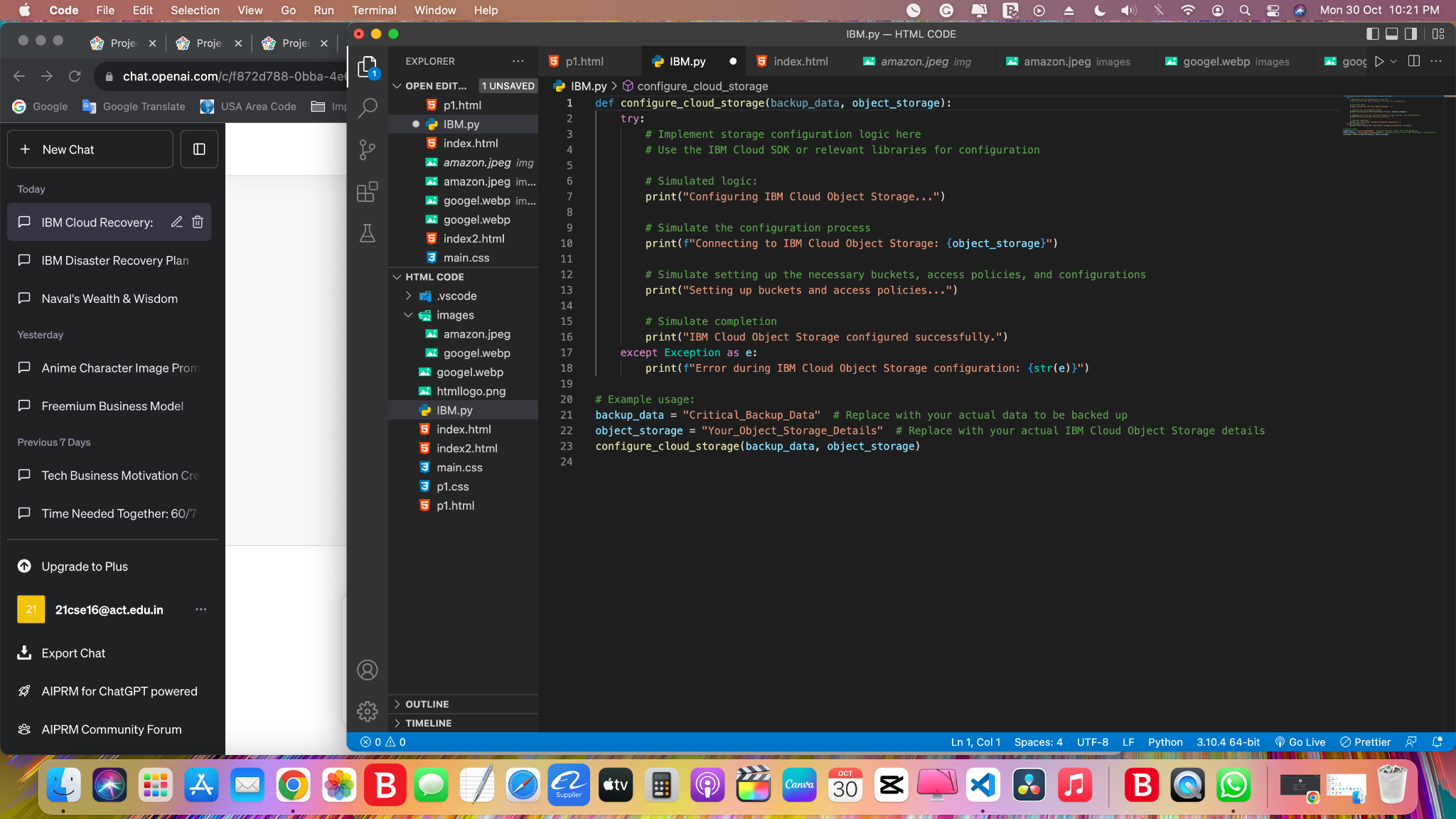


## **Step 5: Cloud Object Storage**

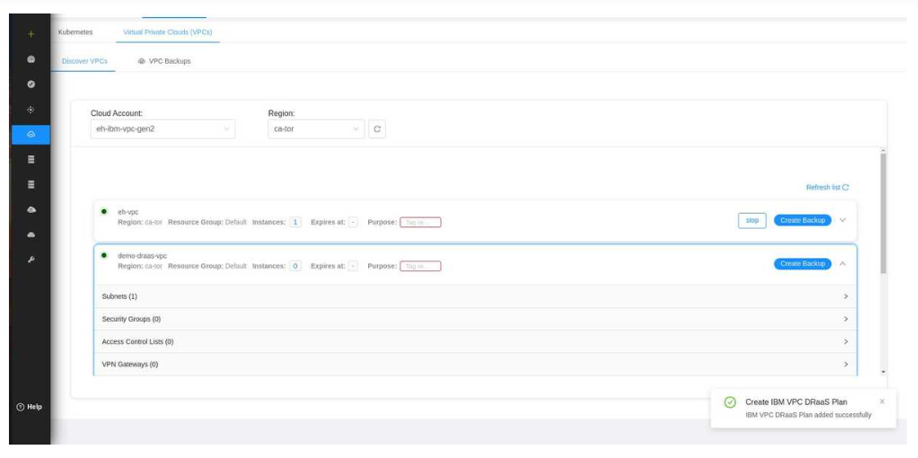
IBM Cloud Object Storage is a reliable and scalable solution for storing critical backup data. It is essential to integrate this storage service into your disaster recovery plan.

### **Storage Configuration**

Ensure that the IBM Cloud Object Storage is properly configured to support your backup and recovery procedures.



### **Cloud storage backup:**

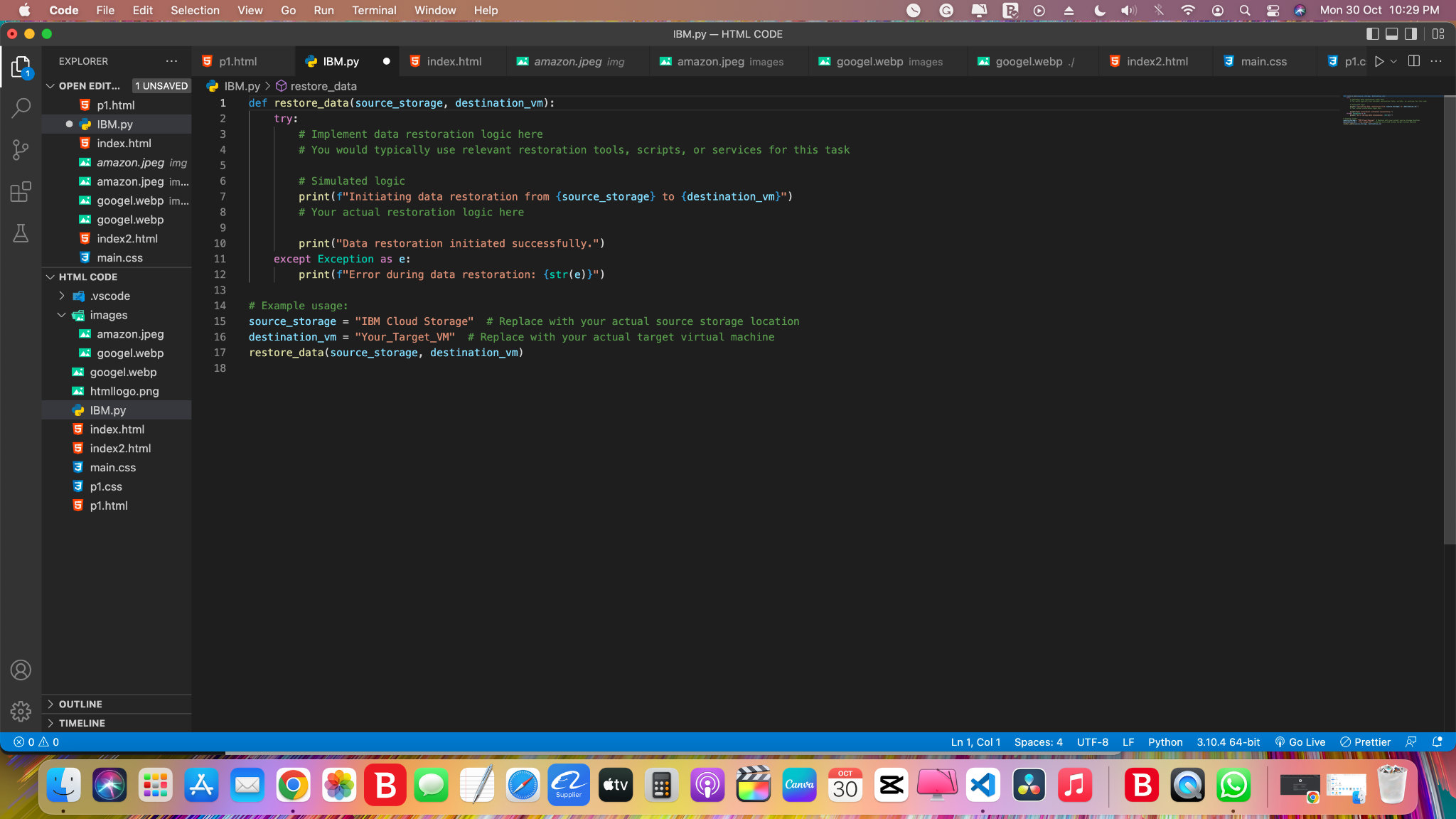


## **Step 6: Restoration Process**

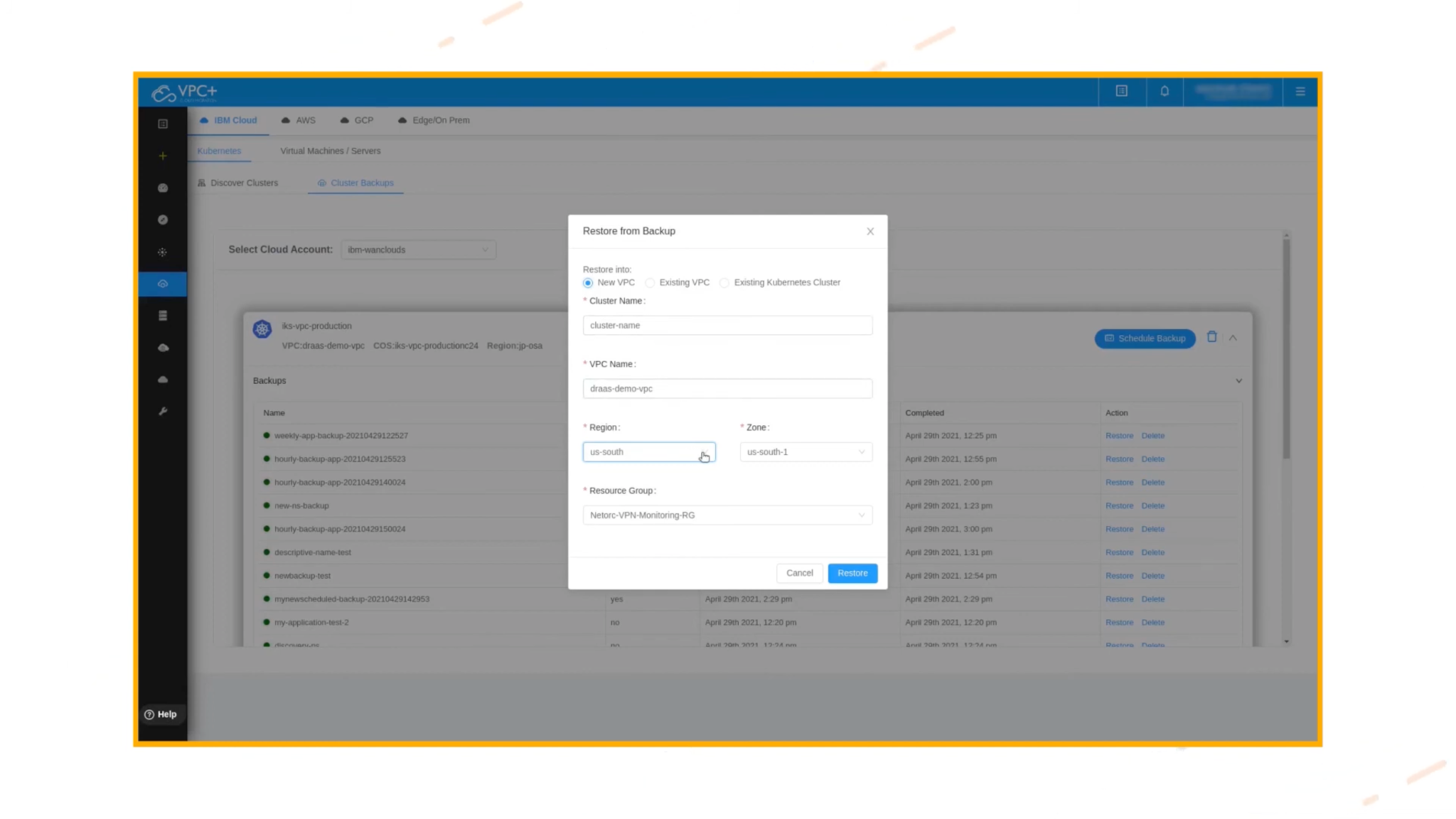
It is vital to have a welldefined process for restoring data and virtual machine images using Virtual Servers.

### **Recovery Steps**

Outline the steps involved in the restoration process. Be prepared to recover data and virtual machine images efficiently.



### **IBM restore:**

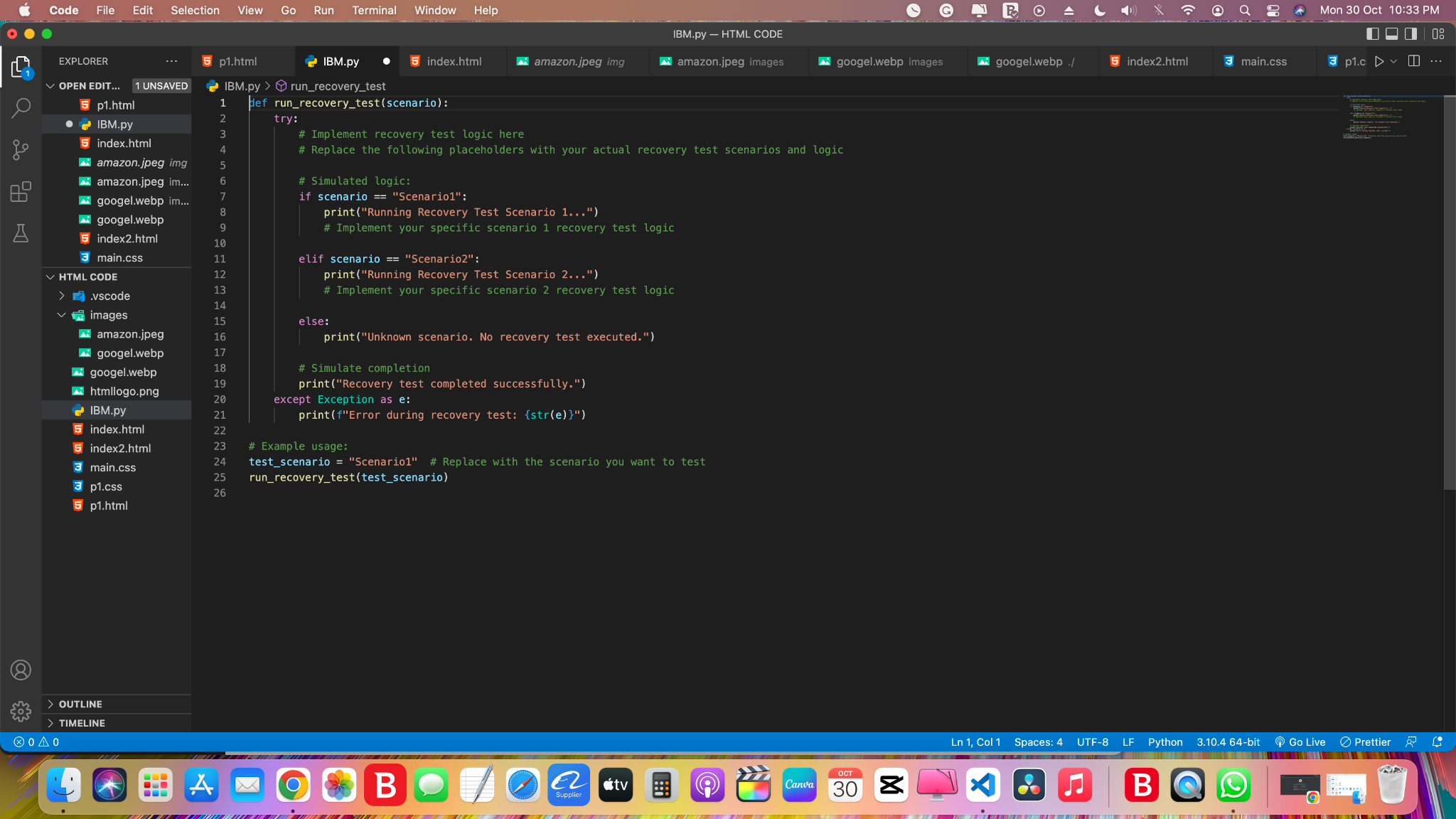


## **Step 7: Testing and Validation**

Carry out comprehensive testing to validate the effectiveness of your disaster recovery plan.

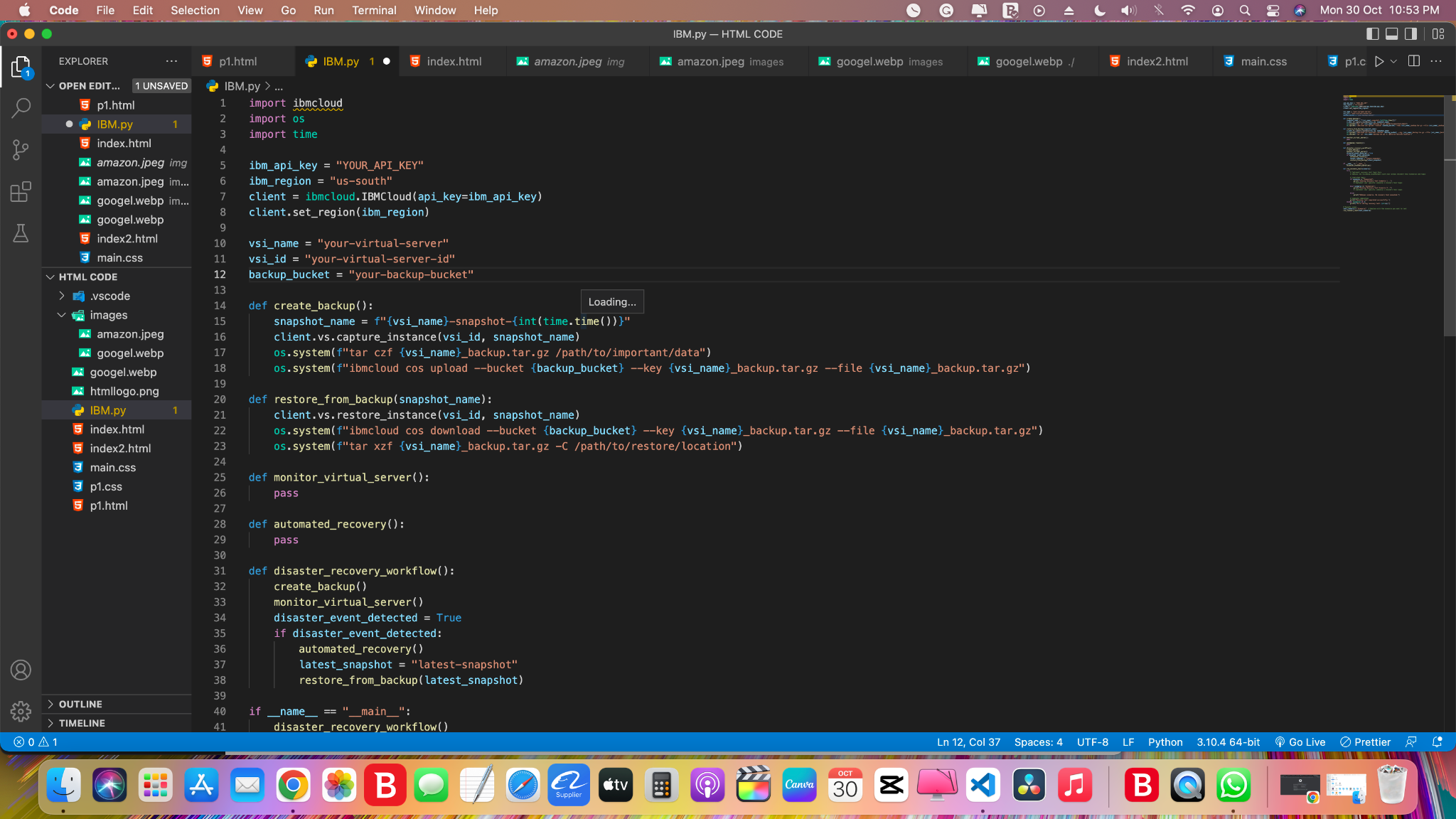
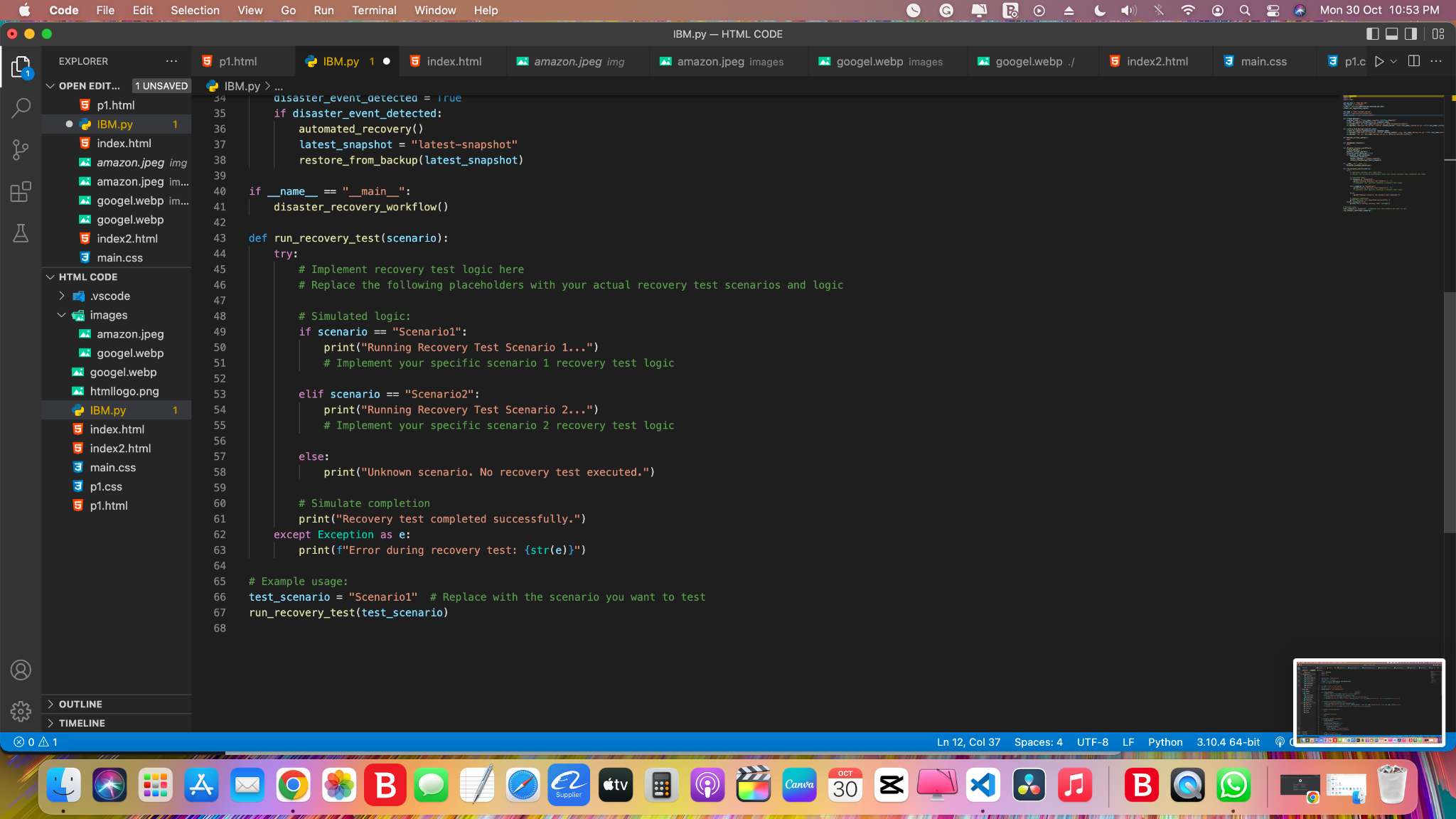
### **Recovery Test Scenarios:**

Develop a test plan that outlines different recovery scenarios and objectives. Define specific tests that you want to conduct to validate the recovery process.



### **Recovery Test Scenarios Process:**

## **Overall Code:**

## **Disaster scenario and practice recovery procedures:**

Conducting recovery tests to ensure that your disaster recovery plan works as intended is a critical step in disaster preparedness. This involves simulating a disaster scenario and practicing the recovery procedures. Here's how you can do it:

### Planning and Preparation:

Schedule a testing window during a time when it has the least impact on your production environment.

Notify all relevant team members about the upcoming test and its objectives.

### Scenario Definition:

Define a disaster scenario that you want to simulate. This could be a data center outage, server failure, or any other relevant disaster event.

Document the specific conditions and constraints of the scenario, such as the extent of data loss, the duration of the outage, and the trigger for the recovery.

### Test Environment Setup:

Set up a separate testing environment that mirrors your production environment. This should include virtual machines, data, and configurations.

Ensure that you have the necessary backup data and recovery tools readily available.

### Recovery Procedures:

Document and follow the stepbystep recovery procedures that are part of your disaster recovery plan.

Assign specific tasks to team members responsible for recovery, and ensure everyone knows their roles.

### Simulation:

Simulate the disaster scenario. For example, if you're testing data center recovery, you might physically disconnect the power or network to mimic an outage.

Alternatively, you can simulate a virtual server failure by intentionally shutting down a server.

### Recovery Execution:

Execute the recovery procedures, starting from data restoration to service reactivation.

Ensure that all steps are followed accurately as per the disaster recovery plan.

### Monitoring and Verification:

Continuously monitor the progress of the recovery and ensure that it's proceeding as expected.

Verify the restored data and services to ensure they are functioning correctly.

### Testing Variations:

Consider testing variations and edge cases. For example, test with different types and levels of data loss or with variations in the disaster scenario's severity.

### Validation and Documentation:

Document the results of the recovery test, noting any issues or areas for improvement.

Validate whether the recovery objectives and RTO (Recovery Time Objective) were met.

### PostTest Evaluation:

After the test, hold a posttest evaluation meeting with the team to discuss the results, what worked well, and what needs improvement.

Revise and update the disaster recovery plan based on lessons learned from the test.

### Regular Testing:

Schedule regular recovery tests at planned intervals to ensure the continued effectiveness of your disaster recovery plan.

As your infrastructure evolves, update and adapt the recovery tests accordingly.

### Documentation and Reporting:

Maintain clear records of all tests, including dates, outcomes, and any recommended improvements.

Share the results and recommendations with relevant stakeholders and management.

## **Conclusion:**

These comprehensive efforts ensure that our disaster recovery plan is robust, fully functional, and prepared to handle recovery scenarios efficiently. By creating VPC accounts, utilizing templates, and integrating various components, we have laid a strong foundation for disaster recovery in our IBM Cloud Virtual Servers environment.

The diligent and methodical efforts put into our disaster recovery planning have yielded a robust and fully functional strategy for handling recovery scenarios in our IBM Cloud Virtual Servers environment. The combination of creating VPC (Virtual Private Cloud) accounts, utilizing well-defined templates, and seamlessly integrating various critical components has established a strong foundation for our disaster recovery preparedness.

These key elements represent the cornerstones of our disaster recovery plan, setting the stage for effective response and resilience in the face of unexpected challenges. By fostering a proactive approach to disaster recovery, we're better equipped to safeguard our critical data, maintain operational continuity, and minimize the impact of disruptive events on our organization.