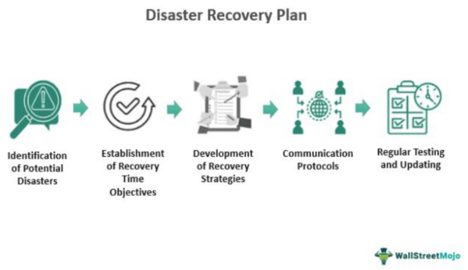
Disaster Recovery Plan Meaning

Disaster Recovery Plan is an essential strategy that defines the steps to be taken in the event of an unexpected disaster that disrupts normal business operations. It helps organizations minimize the impact of a disaster on their operations, assets, and employees and to resume normal business functions.


Disaster Recovery Plan
Identification of Potential Disasters
Establishment of Recovery Time Objectives
Development of Recovery Strategies
Communication Protocols
Regular Testing and Updating
WallStreetMojo

Disaster Recovery Plan

A comprehensive recovery plan will minimize the effect of a natural disaster on business continuity, compliance, and data loss. A good plan also helps speed up recovery from cyberattacks, such as those recently reported by Japanese game developer Capcom, Italian beverage maker Campari, and toy giant Mattel.

If your organization's disaster recovery plan is out of date, insufficient, or, worse, nonexistent, let these events motivate you to review, revise, or create a recovery strategy now, before you need it.

Here are eight steps to creating a disaster recovery plan that will help prevent data loss, facilitate business continuity, and ensure your regulated data and SLAs remain in compliance.

Step 1: Create a Disaster Response Team and Document Responsibilities

★.Your disaster response team will spearhead recovery efforts and disseminate information to employees, customers, and stakeholders during a crisis.

★.Assign each team member specific tasks during the response and document them so everyone knows who is in charge of what. You will also need backup staff for key team members in case a designated lead isn't available during a crisis.

Step 2: Set Clear RTOs and RPOs

Recovery time objective (RTO) is the length of time an application can be down before the business is negatively impacted. RTO varies widely among applications because some can be down for only a few seconds before the business, customers, or users are impacted, whereas others can be down for hours, days, or even weeks.

RTOs are calculated based on application importance:

★.RTO near zero: Mission-critical applications that must failover

★.RTO of four hours: Less critical, so there is time for on-site recovery from bare metal

★.RTO of eight or more hours: Nonessential applications that can be down indefinitely

Recovery point objective (RPO) is the most data that can be lost before the business is significantly harmed (i.e., how much buffer you need between an outage and the most recent working backup).

RPO is based on how much you are willing to spend to backup a particular application, because it can get expensive quickly:

★.RPO of near zero: Use continuous replication (mission-critical data)

★.RPO of four hours: Use scheduled snapshot replication

★.RPO of 8-24 hours: Use existing backup solution (data that can potentially be recreated from other repositories)

Step 3: Make a Blueprint of the Network Infrastructure

★.Creating detailed documentation of your entire network infrastructure will make it much easier to rebuild the system after a disaster, especially if the network was corrupted by a cyberattack.

★.Different components of the system have different levels of importance to business continuity, so be sure to indicate the priority of each service as mission-critical, essential, or nonessential so they can be restored in the appropriate order. Don't forget to include system dependencies in your blueprint, because they may impact how you prioritize recovery.

Step 4: Select a Disaster Recovery Solution

★.Storage capacity, recovery timeline, and configuration complexity will affect the cost of a disaster recovery solution. In many cases, you are choosing between a solution that offers quick recovery times but may lose days of data and a solution that maintains system availability but kills you with high complexity and costs.

★ Look for a disaster recovery solution like Arcserve UDP Cloud Direct that affordably protects your systems and applications from data loss. Arcserve also minimizes complexity by letting you manage backup and disaster recovery and restore service-level agreements from a single web-based UI.

Step 5: Create a Checklist of Criteria for Initiating the Disaster Response Plan

★.Not every incident warrants a full-fledged deployment of your disaster response plan. Creating a checklist of criteria to identify what constitutes a disaster helps your recovery team know when it's time to jump into action without wasting resources or money by overreacting to a minor threat.

★.For example, a temporary power outage and a direct hit from a category 4 hurricane require very different responses.

Step 6: Document the Disaster Recovery Process

★.To ensure data and operations are restored quickly after a disaster, create step-by-step instructions in plain language so your team can start the disaster recovery effort as soon as it's safe to do so.

★.Store a copy of the disaster recovery plan away from the network—preferably in the cloud—to protect it from corruption during a ransomware attack or physical loss from a natural disaster.

Step 7: Test Your Disaster Recovery Plan

★.Conduct regular tests of your disaster recovery plan to ensure it will work when you need it to. Run a partial recovery test twice a year and a full recovery simulation annually.

★.Additionally, it doesn't hurt to periodically spring surprise drills on the company so you can get an accurate assessment of how well the processes will work in the event of a real emergency.

Step 8: Review and Update Your Disaster Recovery Plan Regularly

★Post-COVID-19, there will be a lot of movement within companies. Changes may include employees leaving or joining the company, policies being modified to meet new regulations or standards, or business units being consolidated.

Benefits

There are several benefits to having a Disaster Recovery Plan (DRP) in place for a business. Here are some of the key benefits:

1.Minimizes Downtime: It helps businesses minimize downtime in a disaster, allowing them to resume operations quickly and reduce the impact on their customers.

2.Reduces Data Loss: It reduces the risk of data loss and associated costs.

3.Increases Resilience: It helps businesses build resilience by identifying potential risks and vulnerabilities and developing mitigation strategies.

4.Improves Business Continuity: It helps businesses ensure the continuity of their operations, even in the face of unexpected events, by providing a clear roadmap for recovery and resumption of services.

5.Protects Reputation: It helps businesses protect their reputation by minimizing the impact of a disaster on their customers, stakeholders, and the wider community.

6.Reduces Costs: It can help businesses reduce the costs associated with a disaster by minimizing downtime, reducing data loss, and avoiding the need for costly emergency measures.

7.Enhances Compliance: It helps businesses comply with industry regulations and standards, such as **HIPAA**, **SOX**, and **PCI**.

Example 1

Suppose a manufacturing company operates in a region vulnerable to natural disasters like hurricanes and earthquakes. To prepare for such events, the company has developed a Disaster Recovery Plan that includes the following:

★.Regular backups of critical data and systems.

★.A designated hot site location that can take over operations in case of a disaster.

★.Emergency contact information for employees, vendors, and customers.

★.Detailed recovery procedures for each critical function.

★.Regular testing and maintenance of it.

Disaster recovery testing

Disaster recovery (DR) testing is what you must do to keep your ability to be resilient, hoping not to need to do it for real. There are different types of disaster recovery testing that you can do to verify your resiliency capabilities:

★.DR dry test

★.DR simulation

★.Switch-over

Disaster recovery dry test

★.A DR dry test is performed by checking all of the resource availability and runbooks on paper, without running a real DR simulation or switch-over.

★.This type of testing is normally run with higher frequency compared to the other testing flavors as no real activities are performed, but it does require the same effort in terms of skills and people.

★.The adoption of a recovery orchestrator software improves the whole dry testing process and reduces the time and effort to be run because most of the operations are performed by the software itself. This also increases the preparedness checking of a real DR simulation or switch-over by periodic scanning that all of the components of the DR solutions are in place and works as expected.

Disaster recovery simulation

★.DR simulation is a way to verify or audit the emergency runbooks and check the recovery time objectives (RTO) and recovery point objectives (RPO) provided by the solution by simulating as much as possible in the same conditions as a real emergency.

★.This means introducing disruptions on replication network connections before interrupting the communications among the sites, hence simulating the sudden loss of the primary site.

★.You can do this only if your data replication solution is resilient and not providing impact on the production, which continues on the primary site. If this is not the case, then look at the documentation for plan and design for the worst conditions.

★.DR simulation deploys a duplicate of your production environment on the DR site that you can use to perform validation and checking. This environment is cleaned at the end of the simulation and updates that happened to the DR test environment are discarded, as the real production has continued on the primary site.

★.It is important thus that network streams flowing to the DR test environment are copies of the real production environment. Usually these network flows are intercepted and duplicated at the primary site (that receives the real flow) and sent to the DR site, which operates on separated and different network subnets than production.

Switch-over

★.Opposite to the DR simulation, in the switch-over test, production is moved from primary site to DR site to verify and audit the ability to run and sustain production operations for a long period.

★.In this option, we don't test DR runbooks, as this would imply the emergency restart, which has an impact on the production environment.

★.To avoid any impact to the production environment, you should pose all the possible attention in performing this switch, such to minimize all those impacts.

★.Production operations are closed orderly on the primary site and reopened from the DR site.

★.Data replication is reverted once everything in the DR site has been verified and before network streams are rerouted to the DR site.

★.Production runs in the DR site for whatever period you have chosen before returning to the primary site at your most convenient time. During this period, your production site is performing as the DR until the next switch-over.

★.Updates happened to the production running in the DR site is kept and replicated back to the primary site.

Disaster Recovery Test Frequency

DR test frequency depends on many factors, but in general you should have a DR test at least once per year. This is the bare minimum frequency that is accepted by auditors to prove your ability to recover.

In setting the frequency though, you should increase this base minimum to a level depending on multiple elements specific of the cloud, such as:

How dynamic is your production environment

The more your production environment is dynamic, the more you need to exercise a DR test to verify that changes introduced didn't affect your ability to recover.

How dynamic is your infrastructure

As an example, if you have chosen to provision some of the DR resources on demand, you should consider that you have no control on the type of resources or technologies that you will find at the time of a disaster. In fact, changes in the underlying technologies (for example, the servers), configurations (for example, network topologies), or service levels (for example, time to provision new resources) from your last test. So, it is recommended to increase the testing frequency in such a case, especially if you believe that your applications might be sensitive to the underlying infrastructure technology.

disaster recovery testing steps:

Disaster recovery testing, as we've already mentioned, is different for every business. However, there are some basic steps that need to be taken before the actual process of testing begins.

Step 1: Perform an audit of IT resources

Before business continuity and normality can resume after a disaster, businesses need to know what 'normal' actually is. This involves identifying all the disparate assets that exist on the business network infrastructure. By creating an inventory of all of the IT resources on the network, and identifying what they contain, a business can start the process of consolidation, making it easier and more streamlined for the backup and recovery process in the future.

Step 2: Decide what is mission critical

During the audit of assets, businesses may find that a great deal of data is actually redundant, or not necessary to keep the system running. Transferring every piece of unnecessary data in the network to a backup server could use a huge amount of processing power. Sorting redundant data can help reduce the size of a backup file, saving storage space and expense.

Step 3: Create specific roles and responsibilities for all involved in the DR plan

Every employee in an organization should have a role to play in an effective disaster recovery plan. While automated disaster recovery testing serves an important purpose in a DR plan, it only tests the technical components. If a real disaster occurs, it's the people within an organization who will need to know what to do to rapidly restore uptime.

When everyone knows what to do in response to an emergency, your DR plan will be more effective than it would be if nobody knew what to do when a disaster occurs.

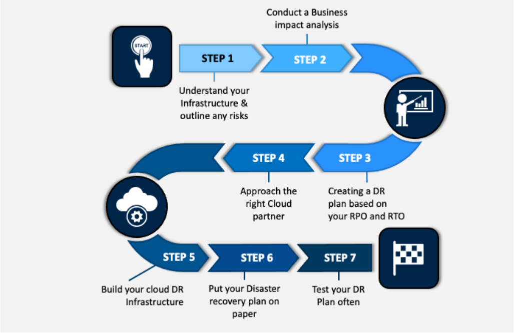
Step 4: Determine your recovery goals

Decide how quickly your organization needs to recover, and set your RTOs and RPOs. This could involve prioritizing which data needs to be accessed immediately, and which is less important. Data that doesn't require immediate access could be assigned a longer recover time and less frequent backups. While important data, like financials and compliance could be assigned more urgent RPOs and RTOs or even a backup server to take over for the main server in disaster recovery process.

Step 5: Implement a cloud data storage solution

Disasters like cyber attacks and ransomware attacks could destroy an organization's primary data storage solution, resulting in the permanent loss of that data. Cloud-based solutions can automatically download and copy data every few days (or even every few hours). Unlike older, manual backup methods requiring users to copy data to a disk or USB drive, backups via a cloud-based solution can be carried out at any time, and without having to access physical media.

Another example is if physical assets storing your data are damaged, by fire, flood, or human tampering, remote data backup can help minimize business disruptions.


Conduct a Business impact analysis
STEP 1
STEP 2
Understand your Infrastructure & outline any risks
STEP 4
STEP 3
Approach the right Cloud partner
Creating a DR plan based on your RPO and RTO
STEP 5
STEP 6
STEP 7
Build your cloud DR Infrastructure
Put your Disaster recovery plan on paper
Test your DR Plan often

On-premises VMware VM to IBM Cloud VPC migration with RMM

To implement a data center transformation, the RackWare Management Module (RMM) migration solution provides a seamless virtual-to-virtual replatforming for VMware virtual machine (VM) to IBM Cloud® virtual server instance migration. It allows the adoption of existing capabilities of IBM Cloud. Its intuitive GUI allows you to move the OS, application, and data from VMware ESXi to IBM Cloud VPC virtual server instance.

This guide shows you how to complete a migration from your on-premises VMware VM to IBM Cloud VPC.

Supported operating systems

★.CentOS 7.8, 7.9

★.RHEL 7.2, 7.3, 7.4, 8.1

★.Ubuntu 18.04, 20.04

★.Debian 9.x, 10.x

★.Windows 2012, 2012R2, 2016, 2019

Replicating data and virtual machine images from on-premises to IBM Cloud virtual services typically involves setting up a data replication and migration strategy. Here are the steps to implement this process:

Assess Your Requirements:

First, identify your specific requirements, such as the data volume to be replicated, the types of virtual machines to be migrated, and any compliance or security considerations.

Select the Replication Method:

IBM Cloud offers various tools and methods for data replication and virtual machine migration.

Common options include:

★. IBM Cloud Direct Link: Establish a dedicated network connection between your on-premises environment and IBM Cloud.

★. IBM Cloud Object Storage: Replicate data to IBM Cloud Object Storage using tools like rclone or AWS S3 Transfer Acceleration.

★. VMware Solutions: If you're using VMware on-premises, VMware HCX or vSphere Replication can be used to migrate VMs to IBM Cloud's VMware solutions.

★.Third-Party Tools: There are third-party tools and services for data replication and migration that may be suitable for your needs.

Set Up IBM Cloud Environment:

Create the necessary virtual machines, storage resources, and network configurations in IBM Cloud to receive the replicated data and virtual machine images.

Data Replication:

Configure data replication from your on-premises environment to IBM Cloud. This may involve setting up periodic data synchronization, backup jobs, or continuous replication based on your chosen method.

Image Conversion and Migration:

If you're migrating virtual machine images, convert them into formats compatible with IBM Cloud's virtualization platform. For example, convert VMware VMs to a format suitable for IBM Cloud's VMware environment.

Network Connectivity:

Ensure that there is a secure and reliable network connection between your on-premises environment and IBM Cloud, such as IBM Cloud Direct Link or VPN.

Testing and Validation:

Test the replication and migration process in a controlled environment to ensure that everything works as expected.

Data Consistency and Cutover:

Ensure data consistency between the on-premises and cloud environments. Plan a cutover window for the final data sync and migration.

Final Data Sync and Migration:

During the cutover window, perform the final data synchronization and virtual machine migration.

Monitoring and Optimization:

Continuously monitor the replication and migration process for any issues. Optimize the performance and reliability of the setup.

Failover and Rollback Plan:

Develop a failover and rollback plan in case there are issues during the migration. This plan should include a way to return to the on-premises environment without data loss.

Documentation and Training:

Document the entire process and provide training to your IT staff to ensure they can manage and maintain the new environment effectively.

Security and Compliance:

Ensure that the replicated data and virtual machines meet security and compliance standards, especially if you are handling sensitive or regulated data.

Post-Migration Testing:

After the migration, perform extensive testing to confirm that everything is functioning as expected in the IBM Cloud environment.

Optimization and Cost Management:

Regularly review and optimize your cloud resources to manage costs and ensure efficient resource utilization.

Replicating data and virtual machines from on-premises to IBM Cloud is a complex process that requires careful planning and execution. Depending on your specific use case and requirements, the tools and methods you use may vary. It's advisable to work closely with IBM Cloud support or consulting services to ensure a successful migration.

```
import ibm_boto3

from ibm_botocore.client import Config



# Define your IBM Cloud Object Storage credentials

cos_credentials = {

    ‘apikey’: ‘YOUR_API_KEY’,

    ‘resource_instance_id’: ‘YOUR_RESOURCE_INSTANCE_ID’,

    ‘iam_service_endpoint’: ‘https://iam.cloud.ibm.com/identity/token’,

    ‘endpoint’: ‘YOUR_ENDPOINT’,

    ‘ibm_auth_endpoint’: ‘https://iam.cloud.ibm.com/identity/token’,

}
```

```
# Create a client for IBM Cloud Object Storage

cos = ibm_boto3.client(‘s3’,

                    ibm_api_key_id=cos_credentials[‘apikey’],

                    ibm_service_instance_id=cos_credentials[‘resource_instance_id’],

                    ibm_auth_endpoint=cos_credentials[‘ibm_auth_endpoint’],

                    config=Config(signature_version=‘oauth’),

                    endpoint_url=cos_credentials[‘endpoint’])


# Define local file paths for data and VM images

local_data_path = ‘/path/to/local/data’

local_vm_image_path = ‘/path/to/local/vm-image.qcow2’


# Define IBM Cloud Object Storage bucket name

bucket_name = ‘your-ibm-cos-bucket-name’


# Upload data to IBM Cloud Object Storage

cos.upload_file(Filename=local_data_path, Bucket=bucket_name, Key=‘data/file.dat’)


# Upload VM image to IBM Cloud Object Storage

cos.upload_file(Filename=local_vm_image_path, Bucket=bucket_name, Key=‘vm-images/vm-image.qcow2’)


print(“Data and VM image uploaded to IBM Cloud Object Storage.”)
```

A disaster recovery test (DR test) is the examination of each step in a disaster recovery plan

Disaster recovery testing is the process to ensure that an organization can restore data and applications and continue operations after an interruption of its services, critical IT failure or complete disruption. It is necessary to document this process and review it from time to time with their clients. It will ensure that you know how to save your client in the event of any fail. Keep reading to learn more about disaster recovery testing scenarios and disaster recovery testing best practices.

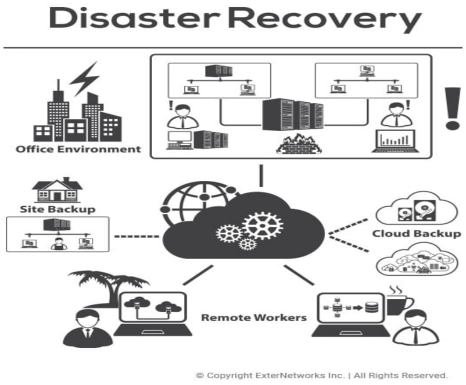
This should include a plan for regular testing of disaster recovery scenarios, again so you can demonstrate that you've done your due diligence, as well as finding and eliminating potential problems before they become real problems.

There are several variables that will affect how much disaster recovery testing you'll need to do, as well as what you'll be charging, and what expectations your clients will have. The size of the company you're supporting, their budget for a DR solution, the complexity of their data structures and networks, (whether all contained on your network, or some internally on their network, or more at additional service providers), amount of data to be backed up, and so forth.

Methods for Disaster Recovery Testing

This isn't as simple as picking one of the methods below. You might need to use all of them. Some cover ensuring that business practices align with the disaster recovery plan, some cover ongoing changes to your systems (or your customer's systems), and some cover testing the hardware and software by simulating a disaster and restoring a file or system or data center to full functionality.

All of these plans should be reviewed and tests should be ongoing. This doesn't necessarily mean running through a full plan once a month – you might run through some part of each plan on a weekly basis, a bigger part once a month, and a full test once a year. The important part is to perform disaster recovery testing regularly, and ensure that any additions to the business are reflected in the DR plan.



© Copyright ExterNetworks Inc. | All Rights Reserved.

Practicing disaster recovery with IBM Cloud Virtual Services involves creating a procedure to ensure that you can recover your virtual machines (VMs) and data in case of a disaster. Here's a high-level recovery procedure for IBM Cloud Virtual Services:

1. Preparing for Recovery:

★.Ensure that your disaster recovery plan is up to date and documented.

★.Verify that your backup strategies, such as snapshotting and regular backups, are functioning correctly.

2. Initial Assessment:

★.In the event of a disaster, assess the scope and impact of the incident to determine if recovery is needed.

3. Communication:

★.**Notify** key stakeholders, including your disaster recovery team, management, and potentially customers, if applicable.

4. VM Recovery:

★.Access your IBM Cloud Virtual Services account and identify the VMs that need to be recovered.

★.Verify that you have recent backups or snapshots available for the affected VMs.

5. VM Restoration:

★. Create new VMs or restore VM snapshots from your backups to replace the lost or damaged VMs.

★. Ensure that the configuration of these VMs matches the original setup.

6. Data Recovery:

★.Access your backup systems or data storage to retrieve the necessary data and files.

★. Restore data to its original location or to alternative storage, depending on the nature of the disaster.

7. Network Configuration:

★.Set up or reconfigure network connectivity for the recovered VMs, ensuring they can communicate with the required resources.

8. Application and Service Restoration:

★.Install and configure any required applications or services on the recovered VMs.

★. Test to ensure the applications and services are functioning as expected.

9. Testing:

★.Perform tests to verify the recovered VMs and services are fully functional.

★.Conduct a thorough system test to ensure business continuity.

10. Validation:

★. Confirm that the recovery was successful and that all critical systems and data are operational.

11. Documentation:

★.Update your disaster recovery plan to reflect the changes made during the recovery process.

★.Document any lessons learned and improvements that can be made for future recovery procedures.

12. Continuous Improvement:

★.Regularly review and update your disaster recovery plan.

★.Schedule routine disaster recovery drills to ensure that your team is well-prepared and that your procedures are effective.

13. Reporting:

★.Report the incident, response, and recovery process to management or relevant authorities, if required.

14. Post-Recovery Evaluation:

★.Review the recovery process and make any necessary improvements to enhance your disaster recovery capabilities.

Remember that disaster recovery should be an ongoing process, and regular testing and refinement of your procedures are critical. Additionally, your recovery procedure should align with your specific **IBM Cloud Virtual** Services configuration and the services you're using. Tailor your disaster recovery plan to your organization's needs and priorities.