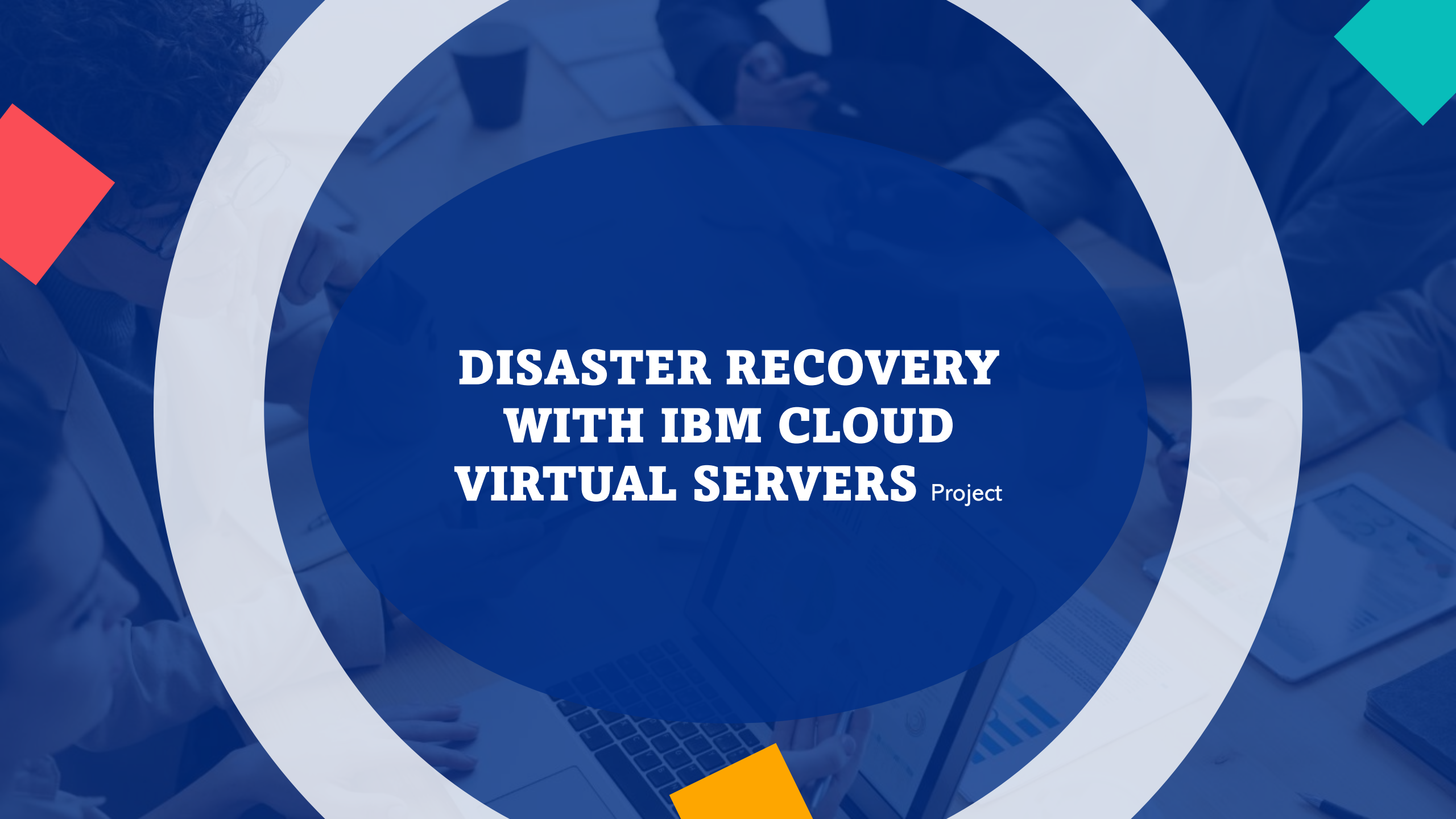


DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS Project

THE CREATIVE TEAM

We do things better

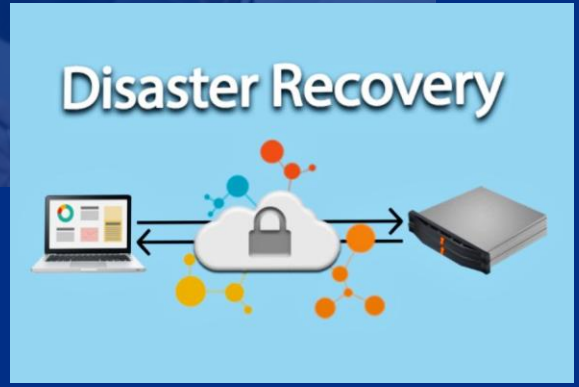
S. SONA	M. PRIYADHARSHINI	D. MYTHILI	M. NISHANTHI
Stylist			

OBJECTIVE

- Introduction
- Key Consideration
- Disaster Recovery Stages
- Cloud Disaster recovery Plan
- Methodology
- Conclusion

INTRODUCTION

- Disaster recovery Consists of IT technologies and best practices designed to prevent or minimize data loss and business disruption resulting from catastrophic Events
- Everything from Equipment failure and localized power outage to cyber attacks, civil emergencies, criminal or military attacks and natural disasters.
- Disaster recovery planning involves Strategizing, planning, deploying appreciate technology and continuous testing.



KEY CONSIDERATIONS

- Security
- Monitoring & alerting
- Scalability
- Resource Allocation

Security:

- Ensure data security During failover &recovery process

Monitoring & Alerting:

- Implement Continuous Monitoring &alter to detect And respond to issues promptly.

Scalability:

- Ensure that your DR plan Can scale as your infrastructure And workloads grow.

Resource Allocation:

- Allocate the necessary Resource For DR, including Computer power, storage And network bandwidth.

DISASTER RECOVERY STAGES

Recovery Team Assessment

Activate Team Recovery Plan

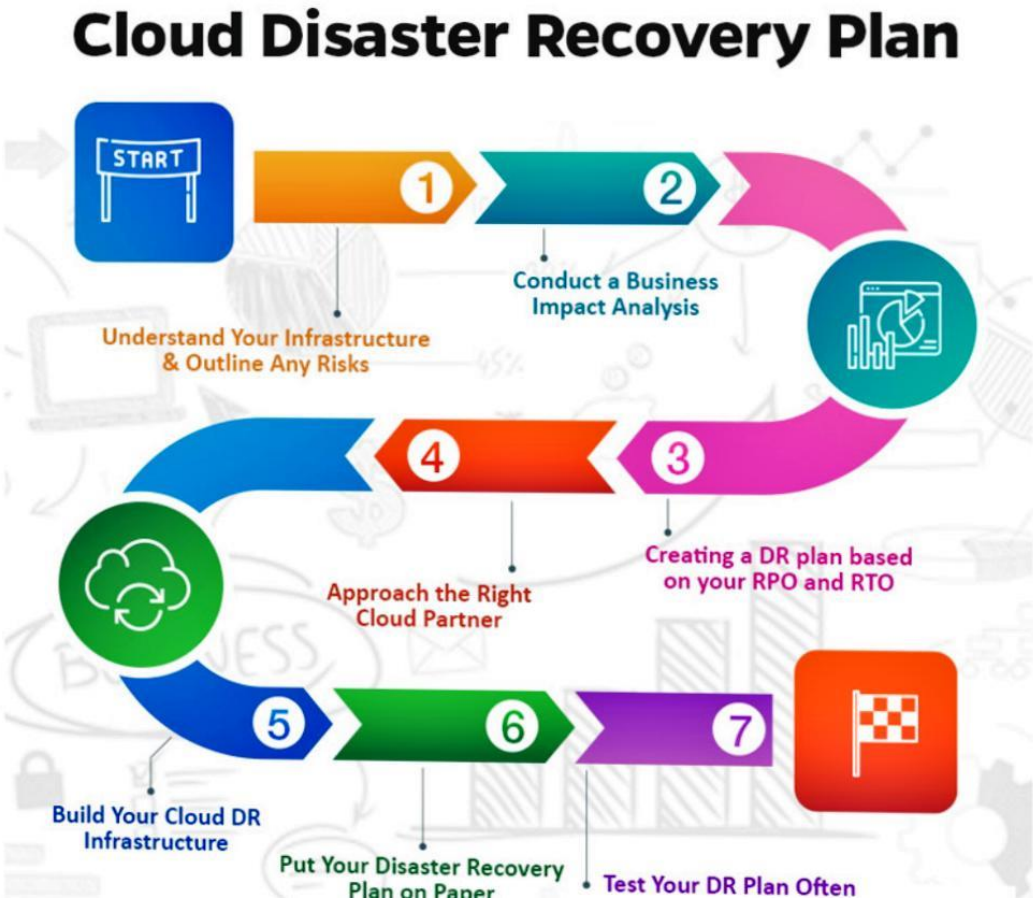
Identify Disaster Recovery Script

Open Incident Report and change control request and Execute

- # CLOUD DISASTER RECOVERY PLAN

Step-1:Understand Your Infrastructure and outline any risks.

Step-2:Conduct a business Impact analysis.
Step-3:Creating a DR plan based on your RPO and RTO.
Step-4:Approach a Right cloud Partner.
Step-5:Build your Cloud DR infrastructure.
Step-6:Put your Disaster recovery plan on paper.
Step-7: Rest your DR plan often.



STEPS FOR DISASTER RECOVERY PLANNING:

Step-1:

It is essential to consider your IT infrastructure, including the assets, equipment, and data you possess to Create an effective disaster recovery process.

Step-2:

A business impact analysis is next on the list. They will give you an understanding of the limitations of your business operations once disaster strikes.

Step-3:

Now that you have determined your RTO and RPO, you can focus on designing a system to meet your IT disaster recovery planning goals.

Step-4:

After you have considered creating a cloud disaster recovery plan., the next step should be to look for a trust cloud service provider that will help in deployment.

Step-5:

After consulting a cloud disaster recovery service partner, you can work with the provider to implement your design and set up your DR plan

Step-6:

It's is essential to have standard guidelines to process flowchart with specific instructions for each and everyone involved in your IT disaster recovery plan.

METHODOLOGY

Assessment and planning:

- Identify Your critical workload and data that need to be protected.
- Determine your recovery time objective and recovery point Objective

Backup and Snapshotting:

- Implement regular backups and snapshot of your virtual servers.
- You can use IBM Cloud object storage for storing backups.

```
Ibmcloud is snapshot-create <virtual-server-id>”Snapshot Name”
```

Replication:

- Set up replication of your virtual servers to a geograhically separate IBM cloud data center or region

```
Ibmcloud is instance-failover<source-virtual-server-id> -- to <target-location>
```

Failover Testing:

- **Regularly test your disaster recovery plan by performing failover drills.**

```
Ibmcloud is instance –failover<source-virtual-server-ie>-- to <target-location>
```

Monitoring and automation:

- **Implement monitoring to detect failure and automate the failover process**

```
Ibmcloud is instance –monitoring-create<virtual-server-id>-- alert-threshold-value>
```

Documentation:

- **Document your disaster recovery plan and procedures for your team**

Conclusion:

A well- executed disaster recovery plan using cloud virtual servers can help organizations minimize downtime, protect data, and maintain business continuity in the face of unexpected disasters or disruptions. Regular updates, testing, and monitoring are essential to ensure the plan remains effective over time.


THANK YOU