# PHASE 2:PROJECT

## INNOVATION OF CLOUD DISASTER RECOVERY

Disaster recovery is a portfolio of policies, tools, and processes used to recover or continue operations of critical IT infrastructure, software, and systems after a natural or human-made disaster.

### Cloud-Based Disaster Recovery (DRaaS):

Disaster Recovery as a Service (DRaaS) has become more prevalent.It leverage the clouds scalability and flexibility, allowing organization to replicate and recovery the data and system.

### Serverless Computing for Resilience:

Serverless computing platforms, such as AWS Lambda and Azure Functions, offer built-in fault tolerance and auto-scaling. This can enhance disaster recovery by reducing the need for manual scaling.

### Multi-Cloud Strategies:

Using multiple cloud providers for disaster recovery reduces dependency on a single provider. This approach can be more robust, as it mitigates the risk of a cloud provider.

### Automation and Orchestration:

Automation tools like Terraform and Kubernetes have been adapted for disaster recovery. They enable automatic failover, scaling, and recovery .

### AI and Machine Learning:

These technologies are used for predictive analytics and anomaly detection. By analyzing data patterns.By analyzing data patterns, they can identify potential threats.

### Immutable Infrastructure:

Immutable infrastructure ensures that no changes can be made to a running system. This approach is increasingly used in disaster recovery .

### Zero Trust Security:

Zero Trust architecture has gained prominence in disaster recovery planning. It assumes that threats exist both inside and outside the network.

### Ransomware Mitigation:

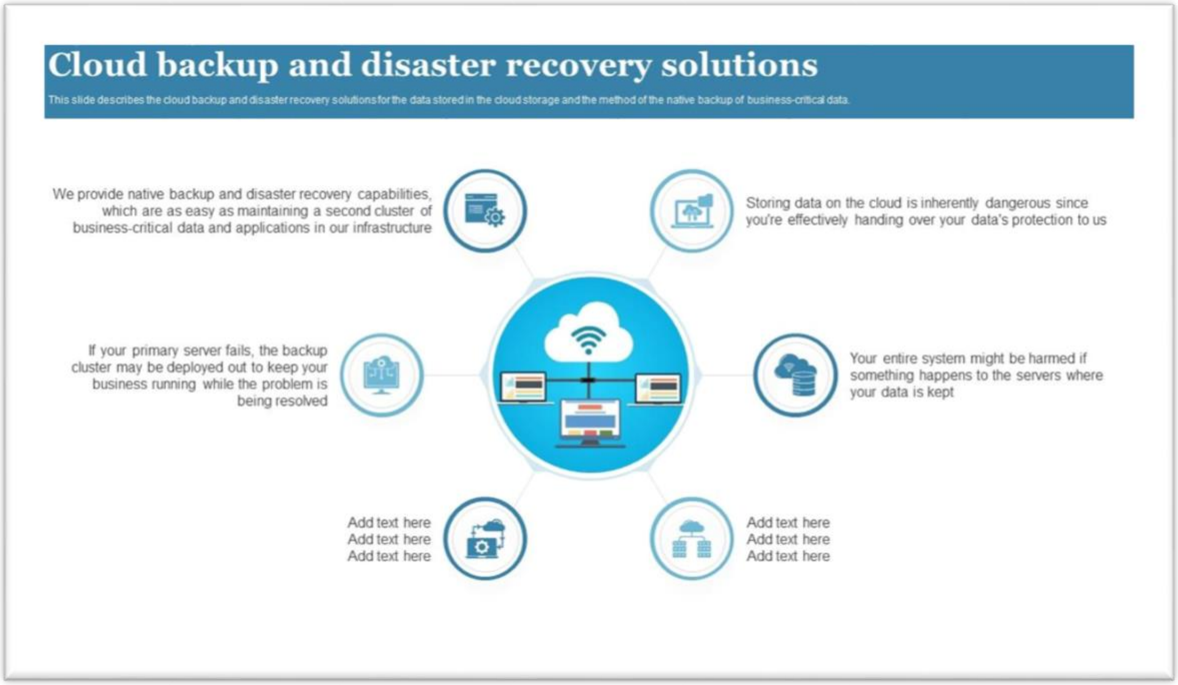
With the rise of ransomware attacks, innovative approaches to data protection and recovery have emerged.

### Edge Computing for Redundancy:

Edge computing brings resources closer to the end-users. By deploying disaster recovery capabilities at the edge, organizations can maintain services.

### Blockchain for Data Integrity:

Blockchain technology is being explored to ensure the integrity of backup and recovery data. It provides a transparent and tamper-proof record of data changes.



Cloud backup and disaster recovery solutions

This slide describes the cloud backup and disaster recovery solutions for the data stored in the cloud storage and the method of the native backup of business-critical data.

We provide native backup and disaster recovery capabilities, which are as easy as maintaining a second cluster of business-critical data and applications in our infrastructure

Storing data on the cloud is inherently dangerous since you're effectively handing over your data's protection to us

If your primary server fails, the backup cluster may be deployed out to keep your business running while the problem is being resolved

Your entire system might be harmed if something happens to the servers where your data is kept

Add text here
Add text here
Add text here

Add text here
Add text here
Add text here

- ### Assessment and Risk Analysis:

Identify potential risks and assess their impact on your operations. Consider natural disasters, hardware failures, data breaches, and more.

- ### RTO and RPO Definition:

Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum tolerable downtime, while RPO is the maximum data loss you can accept.

- **Backup and Replication** :

  Use cloud-based backup solutions and data replication to ensure data redundancy and availability. Consider services like Amazon S3, Azure Blob Storage, or Google Cloud Storage.

- **Virtual Machines (VMs) and Containers:**

  Use cloud-based VMs or containers to replicate and run critical applications in case of a disaster. Services like AWS EC2, Azure Virtual Machines, and Google Compute Engine can be valuable.

- **Load Balancing:**

  Implement load balancing across multiple regions or availability zones to ensure high availability and failover capabilities.

- **Data Encryption:**

  Encrypt data at rest and in transit to protect it from breaching during recovery.

- **Automation and Orchestration:**

  Use cloud management tools and automation scripts to quickly provision resources, reducing recovery time.

- **Testing:**

Regularly test your disaster recovery plan to ensure it works as expected. Cloud providers offer tools for this, like AWS Disaster Recovery Testing or Azure Site Recovery.