DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVICES

PRESENTED BY,

R.DIVYA

E.JANANI

R.R.KANISHKA

P.KAVISRI

P.VINOTHINI

OBJECTIVES:

* The primary objective of disaster recovery is to ensure that an organization can quickly and effectively restore its critical IT systems and data to normal operation after a disruptive event, such as a natural disaster, cyberattack, hardware failure, or any other incident that could result in data loss or system downtime.
* The key goals of disaster recovery include minimizing downtime, preserving data integrity, and maintaining business continuity to reduce the impact of such events on the organization's operations and reputation.

DESIGN THINKING PROCESS:

**Empathize:**

* Understand the needs and concerns of the affected people, communities, and the organization itself.
* Gather insights through interviews, surveys, and observation to empathize with those impacted by the disaster.

**Define:**

* Clearly define the problem or challenges related to disaster recovery. This could involve identifying specific system vulnerabilities, data recovery needs, or communication gaps.
* Create a user-centered problem statement to guide the design process.

**Ideate:**

* Brainstorm and generate creative solutions to the defined problems. Encourage diverse perspectives and ideas from the team.
* Consider innovative approaches to disaster recovery, such as new technology, communication methods, or resource allocation.

**Prototype:**

* Create tangible prototypes or mock-ups of the proposed solutions. This might involve developing new disaster recovery plans, communication strategies, or technology implementations.
* Test these prototypes on a small scale to gather feedback.

**Test:**

* Implement the prototypes in a controlled environment to assess their effectiveness.
* Collect feedback from stakeholders, including disaster recovery experts and those affected by disasters, to refine the solutions.

**Iterate:**

* Based on feedback and test results, make necessary adjustments and refinements to the disaster recovery solutions.
* Continue testing and refining the solutions until they are effective and meet the needs of the organization and the community.

**Implement:**

* Once the disaster recovery solutions are refined and proven effective, implement them on a larger scale.
* Ensure that all relevant stakeholders are trained and prepared to use these solutions in a real disaster scenario.

**Evaluate:**

* Continuously monitor and evaluate the effectiveness of the implemented disaster recovery solutions.
* Make further improvements as needed to adapt to changing circumstances and emerging threats.
* Design thinking promotes a human-centered, iterative, and creative approach to disaster recovery, with a focus on addressing real-world needs and challenges in a dynamic and evolving environment.

DEVELOPMENT PHASE:

**Risk Assessment and BIA:** Identify risks, assess critical processes, and set recovery objectives.

**Strategy Formulation:** Create a disaster recovery strategy, considering various approaches.

**Plan Development:** Detail actions for data backup, system recovery, and business continuity.

**Resource Allocation:** Determine needed resources and allocate budget accordingly.

**Technology Selection:** Choose and implement data backup and recovery technologies.

**Training and Testing:** Train staff, conduct regular disaster recovery drills.

**Documentation and Communication**: Document plans, establish clear communication protocols.

**Regulatory Compliance:** Ensure compliance with relevant regulations and standards.

**Continuous Improvement**: Regularly review and improve disaster recovery plans.

**Incident Response Integration**: Integrate disaster recovery with incident response procedures.

**Monitoring and Reporting:** Implement systems to track critical systems and report on preparedness status.

**DISASTER RECOVERY STRATEGIES:**

* A disaster recovery strategy is a comprehensive plan and set of procedures aimed at minimizing the impact of unexpected events or disasters on an organization's operations and data.
* Its primary goal is to ensure business continuity and the ability to recover from various types of disasters, such as natural disasters, cyberattacks, hardware failures, and more. Key elements include risk assessment, business impact analysis, backup and data recovery, redundancy, data replication, disaster recovery sites, a detailed recovery plan, a communication plan, testing and training, documentation, legal and compliance considerations, budget allocation, and continuous improvement. The strategy's purpose is to protect an organization's data, operations, and reputation by minimizing downtime and facilitating a swift recovery after a disaster.

**CONFIGURATION BACKUP:**

Backup and disaster recovery involves periodically creating or updating one more copies of files, storing them in one or more remote locations, and using the copies to continue or resume business operations in the event of data loss due to file damage, data corruption, cyberattack or natural disaster.

**REPLICATION SETUP:**

* Disaster recovery replication refers to creating exact copies of data, either within a single location or between a main location and alternative one(s). Disaster recovery replication should be constant and ongoing since if a disaster happens, you need to fail over your latest business-critical IT-processes to the DR software and hardware within an acceptable period.
* Although at present, cloud replication is becoming increasingly popular, the use of alternative physical sites remains highly prevalent. The two main types of physical sites are the hot site and cold site. A hot site is a copy of your primary datacenter, containing the same equipment, software and hardware, so if your primary location is not operable, the hot site can instantly become a failover point. As you can probably imagine, its cost is correspondingly high. A cold site, on the other hand, is just a space with no hardware and software installed, which yet contains the necessary power and communication lines.

**RECOVERY TESTING PROCEDURES:**

1**. Assessment and Planning**: Assess recovery requirements and identify critical workloads, data, and services to protect.

2. **Replication Setup**: Establish data replication for data consistency on IBM Cloud

3. **RPO and RTO**: Set Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to guide testing.

4. **Test Environment**: Create a testing environment mirroring production.

5**. Test Scenarios**: Define disaster scenarios and recovery procedures.

6. **Test Execution**: Simulate disaster scenarios in a controlled manner.

7. **Validation**: Ensure recovery meets RPO and RTO goals.

8. **Documentation**: Record test steps, configurations, and results.

9. **Iterate and Improve**: Adjust recovery plans based on test results.

10**. Regular Testing**: Conduct routine recovery tests to maintain effectiveness.

**DISASTER RECOVERY WITH PLAN GUARANTEE BUSINESS CONTINUITY IN UNFORSEEN EVENTS:**

A disaster recovery plan (DRP) guarantees business continuity in unforeseen events by mitigating risks, facilitating rapid responses, preserving data, and enabling the recovery of infrastructure. It includes strategies for alternative work environments, clear communication, resource allocation, testing, and compliance with regulations. Continuous improvement ensures the DRP remains effective over time.