

# **SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES, CHENNAI – 602105**

**CAPSTONE PROJECT REPORT**

# **TITLE**

**Disaster Recovery and Business Continuity Planning**

**Submitted to**

# **SAVEETHA SCHOOL OF ENGINEERING**

**By**

**G.Sai Bhavani(192211319)**

**Guided by:**

## **Dr. J. Chenni Kumaran**

**Disaster Recovery Strategy:**

Identification of Critical Systems, Applications, and Data

* All critical systems, applications, and data are identified and prioritized effectively. Detailed impact analysis for each component is provided.
* Most critical systems, applications, and data are identified and prioritized. Some impact analysis is provided.
* Some critical systems, applications, and data are identified but lack prioritization. Minimal impact analysis is provided.
* Few critical systems, applications, and data are identified. Prioritization and impact analysis are inadequate or missing.
* Clear and appropriate RTOs and RPOs are defined for all critical components. Objectives align well with business requirements.
* Clear RTOs and RPOs are defined for most critical components. Minor misalignment with business requirements.
* RTOs and RPOs are defined but lack clarity or appropriateness for some components.
* RTOs and RPOs are poorly defined or missing for most components.

**Multi-Cloud Strategy:**

* Utilize multiple cloud service providers to distribute workloads and data. This approach mitigates the risk of a single point of failure.

**Implementation**:

* Distribute critical applications and data across at least two different cloud providers
* Implement data synchronization and replication between clouds.
* Use a cloud management platform to monitor and manage resources across providers.

**Benefits**:

* Increased redundancy and fault tolerance.
* Avoids vendor lock-in.
* Flexibility in choosing the best services from each provider.

**Backup and Restore Procedures:**

Development of Backup and Restore Procedures

* Comprehensive procedures are in place for backing up and restoring data, covering all critical scenarios.
* Effective backup and restore procedures are in place, covering most critical scenarios.
* Basic backup and restore procedures are in place but do not cover all critical scenarios.
* Backup and restore procedures are inadequate or poorly implemented.

**Failover and Redundancy:**

Implementation of Failover and Redundancy Mechanisms

* Robust failover and redundancy mechanisms implemented, ensuring high availability and fault tolerance.
* Effective failover and redundancy mechanisms implemented, with minor gaps.
* Basic failover and redundancy mechanisms in place but may not cover all scenarios.
* Failover and redundancy mechanisms are inadequate or missing.

**Automation of Failover Processes:**

* Failover processes are highly automated, minimizing downtime and manual intervention.
* Failover processes are partially automated, reducing downtime and manual intervention.
* Minimal automation in failover processes, requiring significant manual intervention.
* Failover processes are manual and prone to errors.

**Testing and Validation:**

Testing and Validation of Backup and Restore Procedures

* Regular and rigorous testing of backup and restore procedures, demonstrating high reliability and effectiveness.
* Regular testing of backup and restore procedures, with minor gaps in reliability.
* Infrequent or basic testing of backup and restore procedures, with significant gaps.
* Little to no testing of backup and restore procedures.

**Testing and Validation of Failover Mechanisms:**

* Failover mechanisms are thoroughly tested in real-world scenarios, proving their effectiveness.
* Failover mechanisms are tested regularly, with some real-world scenario testing.
* Failover mechanisms are tested infrequently or only in simulated scenarios.
* Failover mechanisms are rarely tested or untested.

**Cost-effectiveness:**

* Balance between Investment and Impact
* Excellent balance between investment in resilience measures and potential impact of disruptions. Cost-saving measures effectively implemented.
* Good balance, with some room for optimization in cost-saving measures.
* Basic balance, with significant areas for cost optimization.
* Poor balance, with either excessive spending or inadequate investment in resilience measures.

**Documentation:**

Quality and Completeness of Documentation

* Comprehensive documentation covering all aspects of DR and BCP, including procedures, strategies, roles, and contact information.
* Detailed documentation, with minor areas needing improvement.
* Basic documentation, missing some critical information.
* Poor or incomplete documentation.

Clarity and Accessibility

* Documentation is clear, well-organized, and easily accessible to all stakeholders.
* Documentation is clear and accessible, with minor areas needing better organization.
* Documentation is somewhat clear but may be disorganized or hard to access.
* Documentation is unclear, disorganized, or inaccessible.
* Inclusion of Incident Response Plans and Communication Protocols
* Incident response plans and communication protocols are detailed and thoroughly integrated into the documentation.
* Incident response plans and communication protocols are included, with minor gaps.
* Basic incident response plans and communication protocols included, but not detailed.
* Incident response plans and communication protocols are inadequate or missing.