Automated Backup and Disaster Recovery Test Report

1. Automated Backup Strategy

1.1. Purpose of Automated Backups

The backup strategy follows three primary goals:

- **Data Durability** – Ensuring no critical data loss.
- **Minimal Downtime** – Rapid recovery to meet business SLAs.
- **Regulatory Compliance** – Compliance with **GDPR, SOC 2, ISO 27001** regulations.

1.2. Backup Categories and Retention Policies

Backup Type	Description	Frequency	Retention Period	Cloud Service Used
Full System Backup	Captures entire VM snapshots for recovery	Daily (12 AM)	30 Days	AWS Backup, Google Snapshots, Azure Backup
Incremental Backup	Stores only changed data since the last backup	Every 3 Hours	15 Days	AWS S3 Intelligent-Tiering, GCP Nearline, Azure Cool Storage
Database Backup	Logical database backup (RDS, CloudSQL, AzureSQL)	Every 6 Hours	60 Days	AWS RDS Snapshots, GCP Cloud SQL Backups, Azure SQL Backups
Log Backup	Stores system, security, and application logs	Every 1 Hour	30 Days	AWS CloudWatch, GCP Stackdriver, Azure Monitor
Object Storage Backup	Backup for S3, GCS, Blob Storage	Real-time	Versioning Enabled	AWS S3 Versioning, GCP Object Versioning, Azure Blob Snapshots

---

2. Disaster Recovery (DR) Strategy

2.1. DR Objectives and Key Components

- **Multi-region Replication** – Data stored across multiple geographical locations.
- **Automated Failover** – Traffic shifts automatically to the healthiest available region.
- **Cross-Cloud Resilience** – Ensures availability even if one cloud provider fails.

2.2. Disaster Recovery Architecture

Cloud Provider	DR Strategy	Failover Mechanism	Recovery Service
AWS	Multi-AZ replication, Cross-Region Backup	AWS Route 53 Failover, Elastic Disaster Recovery	AWS Disaster Recovery
Google Cloud	Regional replication, Multi-region storage	Google Cloud Traffic Director, Global Load Balancer	GCP Disaster Recovery
Azure	Geo-redundant storage, Cross-region replication	Azure Site Recovery, Azure Traffic Manager	Azure Backup & DR

---

3. Disaster Recovery Testing Methodology

3.1. Test Scenarios and Expected Outcomes

Test Scenario	Test Type	Expected Outcome
Primary Region Failure	Simulated AWS/GCP/Azure region outage	Auto-failover to secondary region
Database Failover	Kill Primary DB Node	Secondary DB takes over instantly
Object Storage Restore	Delete S3/GCS/Azure Blob data	Object restored from backup
Compute Instance Failure	Terminate Primary VM	Backup instance spins up
Kubernetes Cluster Crash	Force delete worker nodes	Cluster auto-recovers using Velero

---

4. Disaster Recovery Performance Metrics

4.1. Key Performance Metrics

Metric	Description	Target Value	Current Value
Backup Success Rate	Percentage of successful backups vs. attempts	≥ 99%	**98.8%**
Recovery Time Objective (RTO)	Time required to restore services	≤ 15 min	**12 min**

Metric	Description	Target Value	Current Value
Recovery Point Objective (RPO)	Maximum acceptable data loss period	≤ 5 min	**4 min**
Failover Success Rate	Percentage of successful failovers	≥ 99.9%	**99.7%**

4.2. Detailed Failure Scenarios & Responses

Failure Scenario	Impact	Mitigation Strategy	Response Time
Primary Region Failure	Application downtime in main region	Auto-failover to secondary region using DNS routing	10 seconds
Database Corruption	Loss of critical data	Restore from latest RDS/CloudSQL/AzureSQL backup	3 minutes
Object Storage Data Loss	Permanent data loss	Restore from versioned backups (S3/GCS/Azure Blob)	2 minutes
Compute Instance Crash	Service disruption	Auto-restart via auto-scaling group	5 seconds
Security Breach (Data Encryption)	Unauthorized data encryption (ransomware)	Restore clean backups, revoke compromised credentials	5 minutes

---

5. Recommendations for DR Improvement

5.1. Findings and Suggested Actions

Category	Findings	Recommended Action
Backup Success Rate	98.8% (Below 99%)	Improve error handling in automation scripts
Recovery Time (RTO)	12 min (Target ≤ 15 min)	Optimize network routing for faster response
Recovery Point (RPO)	4 min (Target ≤ 5 min)	Maintain current backup frequency
Failover Success Rate	99.7% (Target ≥ 99.9%)	Implement active-active DR across all regions

6. Summary and Next Steps

6.1. Key Takeaways

- Backup automation is stable (98.8% success rate).
- Failover mechanisms are functional but need active-active enhancements.
- Recovery times meet required objectives (RTO: 12 min, RPO: 4 min).
- Security resilience needs improvement with automated threat response.