**Example Process for AWS RDS resilience with specific RTO & RPO targets**

This document provides a step-by-step process for achieving AWS RDS resilience with a Recovery Point Objective (RPO) of 15 minutes and a Recovery Time Objective (RTO) of 4 hours for a 500 GB database. It outlines the recommended industry best practices to ensure high availability, data durability, and timely recovery in case of failures. The process includes setting up Multi-AZ deployment, automated backups, and utilizing additional AWS services for disaster recovery.

**Reference to the Industry Best Practices:**

* [AWS RDS Best Practices](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html)
* [Architecting for High Availability with Amazon RDS](https://aws.amazon.com/blogs/database/architecting-for-high-availability-with-amazon-rds/)

Step-by-Step Process:

| **Step** | **Procedure** | **AWS Documentation Reference** |
| --- | --- | --- |
| 1 | Determine the appropriate AWS region for the RDS database deployment. | - [AWS Global Infrastructure](https://aws.amazon.com/about-aws/global-infrastructure/) |
| 2 | Choose the suitable RDS database engine (e.g., MySQL, PostgreSQL, etc.) and instance size based on workload needs. | - [Amazon RDS Documentation](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBInstanceClass.html) |
| 3 | Configure Multi-AZ deployment to provide automatic failover to a standby replica in a different Availability Zone. | - [Multi-AZ Deployments for Amazon RDS](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html) |
| 4 | Enable automated backups with a retention period of at least 15 days. | - [Amazon RDS Automated Backups](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html) |
| 5 | Define a backup window that accommodates the backup duration and database activity patterns. | - [Amazon RDS Backup Window](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Using.BackupWindow.html) |
| 6 | Regularly monitor RDS database metrics, including storage, CPU utilization, and replication status. | - [Amazon RDS Monitoring](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.html) |
| 7 | Implement CloudWatch alarms to trigger notifications for critical events or performance thresholds. | - [Amazon RDS Monitoring with CloudWatch](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatch) |
| 8 | Enable Enhanced Monitoring for detailed insight into database performance using OS-level metrics. | - [Amazon RDS Enhanced Monitoring](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.Enhanced) |
| 9 | Implement additional RDS features, such as Read Replicas, to offload read traffic and improve performance. | - [Amazon RDS Read Replicas](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html) |
| 10 | Test the recovery process by performing regular database snapshots restoration and verifying data integrity. | - [Amazon RDS Restoring a DB Instance](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html) |
| 11 | Establish a disaster recovery plan by creating a standby database in a separate AWS region. | - [Amazon RDS Disaster Recovery](https://aws.amazon.com/rds/disaster-recovery/) |
| 12 | Regularly review and update the RDS resilience strategy based on changing business requirements or workload. | - [Amazon RDS Best Practices](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html) |