SOUTHBANK INC.

AWS Cloud Workload for SBPay System:

IT Disaster Recovery Plan (DRP) for Core System, Infrastructure and Architecture

Table of Contents

A. Revisions & Change Management

A.1 Document Revision History

Version	Date	Author	Description of Changes
1.0	2025-02-23	Norman Armian	Initial IT-DRP document creation

A.2 Change Management Process

- **Review Cycle:** This DRP is reviewed and updated at least once a year or upon significant infrastructure changes.
- **Approval Workflow:** Changes are proposed by the DR team, reviewed by business continuity stakeholders, and approved by IT leadership.
- **Version Control:** A centralized repository maintains document versions for tracking updates and rollback capability.

1. Introduction

1.1 Purpose

This document defines the disaster recovery plan (DRP) for the Core Banking System hosted on AWS Cloud. The plan ensures business continuity by defining procedures to recover operations in the event of disruptions. It provides guidance on handling outages, minimizing downtime, and ensuring data integrity. The document is designed for IT teams, business continuity planners, and risk management teams to maintain operational resilience.

1.2 Scope

This DRP applies to all critical banking applications, databases, and supporting infrastructure deployed in AWS. It covers computing resources, storage, networking, and security components that support banking transactions and customer data. The plan includes guidelines for disaster prevention, mitigation, response, and recovery efforts across multi-region deployments.

1.3 Objectives

- Ensure minimal downtime and data loss through effective recovery procedures.
- Define clear roles and responsibilities during a disaster to ensure a coordinated response.
- Establish a structured recovery process that aligns with business continuity strategies.
- Comply with regulatory and security requirements.
- Implement a backup and failover mechanism to ensure service availability.

2. Disaster Recovery Strategy

2.1 Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)

Recovery Time Objective (RTO) defines the maximum acceptable downtime for each system component, while Recovery Point Objective (RPO) determines the maximum acceptable data loss measured in time.

Component	RTO	RPO
Core Banking System Portal	<30 min	<5 min
Database	<15 min	0 min
Network	<10 min	<12 hours

2.2 Disaster Recovery Tiers & AWS Services

The DR strategy involves leveraging AWS services based on different DR tiers:

- **Hot Standby (Multi-Region Active-Passive)** – Uses AWS Global Infrastructure, Route 53 for DNS failover, Auto Scaling for maintaining application availability, and AWS Transit Gateway for seamless connectivity. This setup means the organization has a fully ready backup environment in another AWS Region that can take over almost immediately during a failure, with DNS failover, auto-scaling, and seamless connectivity ensuring minimal disruption.

- **Warm Standby (Reduced-Capacity Standby)** – AWS EC2 instances with pre-configured AMIs, and RDS Multi-AZ deployments for database resilience. This means that the bank's backup environment is partially running (not full-scale) with pre-configured servers and resilient databases. In case of a failure, the standby setup can be quickly scaled up to take over operations with minimal downtime.

- **Backup & Restore (Cold DR)** – Data stored in Amazon S3 with cross-region replication, AWS Backup for scheduled snapshots, AWS Glacier for long-term archival, and Infrastructure as Code (IaC) using CloudFormation for automated recovery. This means the organization relies on backups and automated scripts to rebuild the environment after a disaster. It's cost-effective but has the longest recovery time compared to Warm or Hot Standby.

2.3 Conditions for the Activation of ITDR Plan

The IT Disaster Recovery (ITDR) Plan shall be activated immediately when one or more of the following conditions are met – this also means that the prolonged disruption will make the bank inoperable within 24 hours:

1. **Data Center / Cloud Infrastructure Outage**
    - Extended unavailability of the primary data center, cloud region, or critical infrastructure components (e.g., EC2, RDS, S3) exceeding acceptable downtime thresholds.
2. **Prolonged Network Failure**
    - Complete loss of connectivity to the Head Office, branch sites, or cloud services that cannot be restored within the defined Recovery Time Objective (RTO).
3. **Critical Application Failure**
    - Failure of core banking systems, payment platforms, or other mission-critical applications where restoration in the production environment is not possible within the RTO.
4. **Cybersecurity Incident**
    - Severe security breaches (e.g., ransomware, data corruption, unauthorized access) compromising data integrity, confidentiality, or availability that require isolation and system recovery.
5. **Physical Disasters**
    - Natural or man-made disasters (e.g., fire, flood, earthquake, power failure) that render the primary site inoperable.
6. **Regulatory or Management Directive**
    - Explicit instruction from executive management or regulatory bodies (e.g., BSP, Data Privacy Commission) requiring activation of disaster recovery procedures.
7. **Other Force Majeure Events**
    - Any unforeseen event significantly disrupting normal IT operations beyond defined risk tolerance levels.

3. AWS Infrastructure & Resiliency

3.1 Architecture Overview

The core banking system infrastructure is designed for high availability and resilience. Key AWS components include:

- **Primary Region:** Singapore (ap-southeast-1) hosting production workloads with Multi-AZ redundancy to distribute critical resources across multiple Availability Zones. This setup minimizes the impact of a single data center failure and enhances system resilience.

- **Secondary Region:** N. Virginia (us-east-1) configured for disaster recovery and failover mechanisms. AWS services like Route 53, AWS Global Accelerator, and cross-region replication ensure rapid failover in case of primary region failure, minimizing downtime and data loss.

- **Multi-AZ Database Deployment:** Uses Amazon RDS Multi-AZ to ensure high availability and fault tolerance. In case of a database instance failure, the standby instance in another Availability Zone is automatically promoted to the primary role, ensuring continued operations with minimal disruption.

- **Auto Scaling & Load Balancing:** AWS Auto Scaling dynamically adjusts capacity, and Application Load Balancer (ALB) ensures traffic is distributed across healthy instances. Auto Scaling monitors instance health and automatically replaces unhealthy instances, ensuring that new, healthy instances are launched to maintain service availability. ALB works in conjunction by detecting unhealthy targets and rerouting traffic to healthy ones, preventing service disruptions and improving system resilience.

- **Storage & Backup:** Amazon S3 with versioning and cross-region replication, AWS Elastic File System (EFS) for shared storage, and FSx for Windows File Server as needed.

4.Disaster Recovery Plan Execution

4.1 Incident Classification

The disaster recovery process follows a structured classification of incidents to determine the appropriate response:

- **Minor Disruption:** Service degradation without customer impact; handled through monitoring and auto-recovery mechanisms.
- **Major Disruption:** Partial system failure requiring failover to DR resources; may involve scaling up secondary region components.
- **Critical Disaster:** Complete system outage requiring full activation of DR sites; executed through failover mechanisms and infrastructure provisioning.

4.2 Disaster Declaration & Activation

1. **Detect & Assess:** Utilize AWS CloudWatch for monitoring, AWS GuardDuty for security threat detection, and AWS Security Hub for compliance checks.
2. **Notify Stakeholders:** Incident Response Team, AWS Enterprise Support, Business Units, and Compliance Teams.
3. **Raise DR Plan:** Execute pre-defined AWS CloudFormation templates or Terraform scripts to restore infrastructure, ensuring automated provisioning of compute, network, and database resources. Multi-AZ failover mechanisms ensure that in case of an Availability Zone failure, workloads automatically transition to healthy zones within the primary region. If a regional outage occurs, Route 53 and AWS Global Accelerator facilitate regional failover to the secondary region.
4. **Failover to DR Site:** Adjust Route 53 DNS failover policies, reconfigure AWS Transit Gateway for routing adjustments, and enable standby resources.
5. **Validate & Test:** Perform system checks, run test transactions, and verify application integrity before resuming full operations.
6. **Post-Recovery Assessment:** Conduct a root cause analysis, update DR procedures based on lessons learned, and document findings for continuous improvement.

5. Roles & Responsibilities

ROLE	RESPONSIBILITIES
L1 Support / Service Desk	Monitor alerts, escalate incidents, provide initial triage.
Incident Response Team	Investigate root causes, coordinate response, and document findings.
Cloud Engineers	Execute AWS-based recovery procedures, restore infrastructure.
Security Team	Ensure security compliance, monitor vulnerabilities, and mitigate threats.
DR Manager	Oversees DR execution, ensures communication with key stakeholders.
Business Continuity Team	Communicate with executives and customers, ensure regulatory compliance.
Testing Team	Validate system functionality post-recovery, run DR drills, and report gaps.

5.1 Incident Response Team (IRT)

Composition:

ROLE/FUNCTION	POINT PERSON	CONTACTS
Incident Manager	Norman Armian / Lorenzo Valdez	norman@southbankinc.com Lorenzo.valdez@ictph.com
Cloud Engineers / Tech Specialists	Rob Castillon /CJ Bayno	rob@southbankinc.com / cj.bayno@ictph.com
Application Support	Edbelle Valencia / Elaine San Pedro	ed@southbankinc.com / elaine.sanpedro@ictph.com
Database Administrator	Jon Dagle / CJ bayno	cj.bayno@ictph.com
L1 Support / Service Desk	Paula Suralta / Kenneth Menor	paula@southbankinc.com support@ictph.com
AWS Enterprise Support (if any)		

Roles & Responsibilities:

- Monitor & Detect: Identify incidents using AWS CloudWatch, GuardDuty, and AWS Security Hub.
- Assess & Classify: Determine severity levels (Minor, Major, Critical).
- Investigate & Contain: Perform root cause analysis, isolate affected services, and initiate recovery procedures.
- Communicate & Escalate: Notify stakeholders, escalate major incidents to AWS Support, and keep leadership informed.
- Execute DR Actions: Trigger DR failover, restore services using CloudFormation/Terraform scripts, and verify application health.
- Post-Incident Analysis: Conduct retrospective analysis, document findings, and recommend preventive actions.

5.2 Security Team

Composition:

ROLE/FUNCTION	POINT PERSON	CONTACTS
Security Analysts / Security Engineers	Norman Armian / CJ Bayno	norman@southbankinc.com / cj.bayno@ictph.com
Compliance / Risk Officers	Jaylie Patlunag / Des Maglatang	jaylie@southbankinc.com / des.maglatang@ictph.com

Roles & Responsibilities:

- Monitor & Detect Threats: Utilize AWS Security Hub, GuardDuty, and AWS Config for threat detection.
- Assess Security Impact: Determine if incidents involve unauthorized access, data breaches, or compliance violations.
- Implement Countermeasures: Enforce security controls, disable compromised accounts, and mitigate risks.
- Support Recovery Efforts: Validate restored environments against security policies.
- Ensure Compliance: Align recovery actions with banking regulations.
- Perform Security Audits: Post-incident assessments to identify and address security gaps.

5.3 IT Business Continuity Team (IT BCT)

Composition:

ROLE/FUNCTION	POINT PERSON	CONTACTS
IT Business Continuity Manager	Norman Armian / Lorenzo Valdez	norman@southbankinc.com Lorenzo.valdez@ictph.com
Risk Management Officer / Compliance	Jaylie Patlunag / Des Maglatang	jaylie@southbankinc.com / des.maglatang@ictph.com
IT Service Continuity Team / Support Leads	Ed Valencia & Paula Suralta / Kenneth Menor	paula@southbankinc.com support@ictph.com
Banking Operations	Harmon Galigao / Elaine San Pedro	harmon@southbankinc.com / elaine.sanpedro@ictph.com
Executive Stakeholders	IT STEERING COMMITTEE	

Roles & Responsibilities:

- Coordinate Business Impact Analysis (BIA): Identify critical applications and define acceptable downtime limits.
- Ensure Regulatory Compliance: Maintain adherence to financial and banking regulations.
- Communicate with External Stakeholders: Inform customers, partners, and regulators about outages and recovery progress.
- Approve Disaster Declaration: Authorize full DR site activation when necessary.
- Oversee Business Recovery: Ensure operational teams can resume normal business functions post-disaster.

5.4 Testing Team

Composition:

ROLE/FUNCTION	POINT PERSON	CONTACTS
DR Testing Coordinator	Norman Armian / Lorenzo Valdez	norman@southbankinc.com Lorenzo.valdez@ictph.com
Technical Team (AWS Engineer, Application, Database)	Robemar Castillon / CJ Bayno	rob@southbankinc.com / cj.bayno@ictph.com
IT Service Continuity Team / Support Leads	Ed Valencia & Paula Suralta / Kenneth Menor	paula@southbankinc.com support@ictph.com
Banking Operations	Harmon Galigao / Elaine San Pedro	harmon@southbankinc.com / elaine.sanpedro@ictph.com
Audit and Compliance	Jaylie Patlunag / Des Maglatang	jaylie@southbankinc.com / des.maglatang@ictph.com
EXECOM	At least 2 representatives from EXECOM Members	

Roles & Responsibilities:

- Develop Test Scenarios: Define test cases for failover, backup restoration, and system recovery.
- Conduct DR Drills: Perform DR testing at least once a year.
- Measure RTO & RPO Compliance: Validate that recovery times meet business requirements.
- Identify Gaps & Improve DR Plan: Analyze test results, report deficiencies, and update the DR plan.
- Ensure Post-Recovery Validation: Confirm application performance, database consistency, and end-user accessibility.

6. Testing & Maintenance

6.1 DR Drills & Testing

- **Frequency:** DR testing is conducted annually (minimum) to validate the plan's effectiveness.
- **Testing Methods:**

1. Tabletop Exercises: Simulated discussions where teams review and analyze hypothetical disaster scenarios.

2. Live Failover Simulations: Execution of failover procedures in a controlled environment to validate AWS infrastructure resilience.

3. Chaos Engineering Experiments: Intentional disruption of AWS resources (using external tools or teams) to test fault tolerance and self-healing mechanisms.

- **Evaluation Criteria:**

1. Adherence to RTO/RPO objectives.
2. System performance and functionality after recovery.
3. Validation of audit logs, security compliance, and backup integrity.

6.2 Roles & Responsibilities for DR Testing

ROLE	RESPONSIBILITIES
DR Manager	Oversees testing, ensures execution aligns with DR policy.
Cloud Engineers	Implement failover, restore infrastructure, and analyze test results.
Application Owners	Validate application availability and integrity post-recovery.
Security Team	Ensure compliance and monitor for security vulnerabilities.
Business Continuity Team	Review business impact, update stakeholders on test outcomes.
Testing Team	Execute test cases, document issues, and recommend improvements.

6.3 Continuous Improvement

- Regular updates to DRP based on new AWS features, infrastructure changes, and security threats.
- Conduct security audits and compliance reviews to ensure adherence to industry and regulatory standards.
- Incorporate lessons learned from past incidents to refine and enhance the DR strategy.

7. Compliance & Regulatory Considerations

The DRP aligns with industry regulations and security standards:

- Alignment to BSP Circulars for banking compliance in the Philippines.
- Conformance to ISO 27001 standards for information security management.
- Implementation of AWS Well-Architected Framework best practices for disaster recovery.

8. Contacts & Escalation Procedures

8.1 Escalation Levels & Response Workflow

Escalation Level	Responsible Team	Actions Taken
Level 1 - Initial Detection & Triage	Service Desk (L1)	• Monitor AWS CloudWatch alerts, Security Hub findings, and GuardDuty threats. • Log incidents in the ITSM platform (e.g., ServiceNow, Jira). • Perform basic troubleshooting (restart instances, check IAM permissions). • Escalate unresolved incidents to L2.
Level 2 - Investigation & Containment	Cloud & Infrastructure Team (L2)	• Analyze root cause using AWS logs, AWS Config, and X-Ray. • Execute initial remediation (restore backups, reroute traffic via Route 53, auto-scale instances). • Activate Multi-AZ failover for affected RDS instances. • If necessary, escalate to Security or DR team.
Level 3 - DR Execution & Failover	Disaster Recovery Team	• Declare disaster and execute DR failover to secondary region. • Run CloudFormation/Terraform scripts to restore infrastructure. • Ensure database replication consistency. • Verify service restoration and initiate rollback if needed.
Level 4 - Business & Compliance Review	Business Continuity & Compliance Teams	• Assess business impact and regulatory requirements. • Notify executive leadership and regulatory bodies if required. • Conduct post-recovery audit and documentation.

8.2 Key Contact List

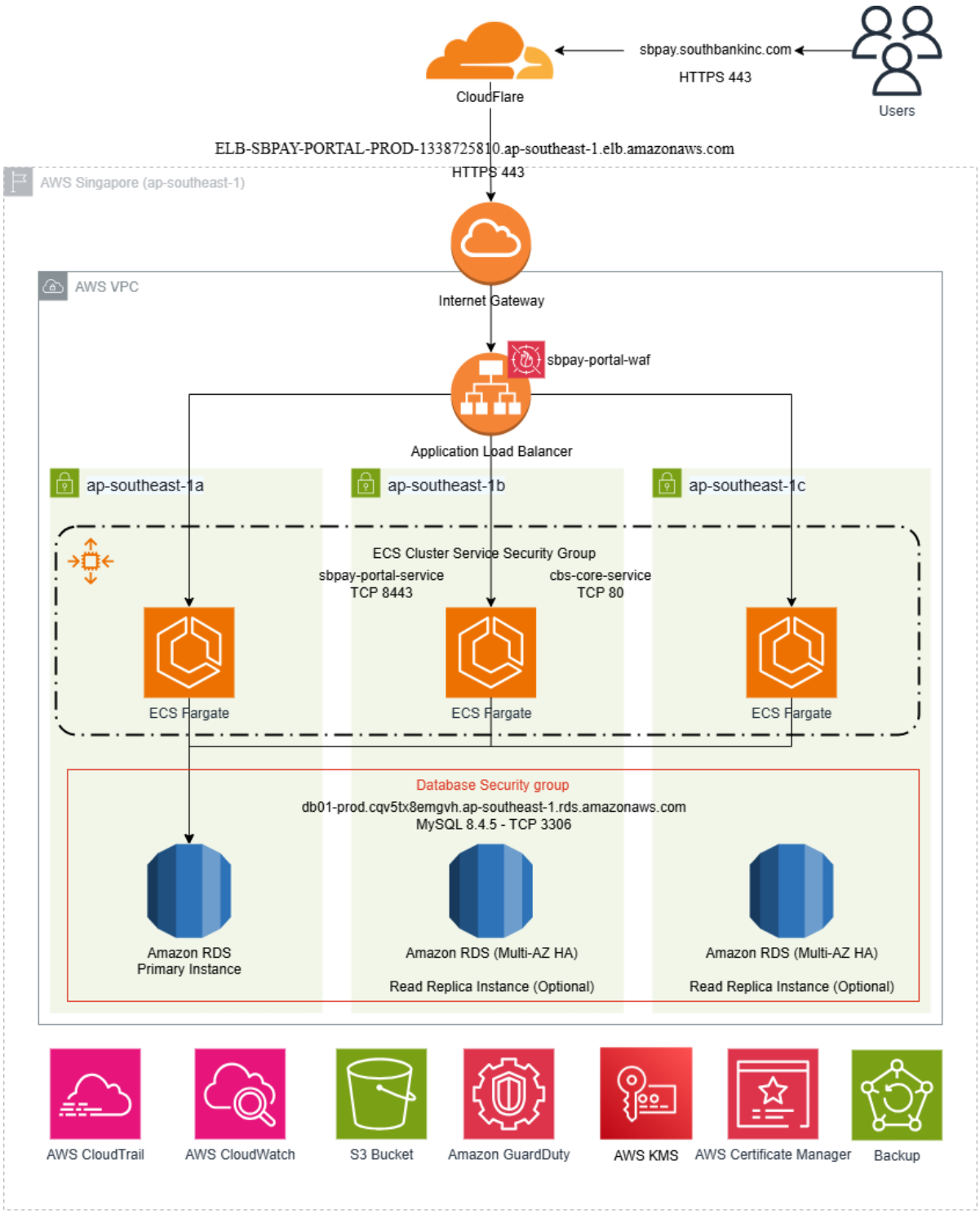
Role	Name	Contact	Responsibility
DR Manager	Norman Armian	norman@southbankinc.com	Leads DR activation, ensures alignment with business continuity.
Cloud Infrastructure Lead	Christian Jay Bayno	cj.bayno@ictph.com	Oversees AWS infrastructure failover and recovery.
Security Incident Response Lead	Norman Armian / Christian Jay Bayno	norman@southbankinc.com /cj.bayno@ictph.com	Handles security-related threats, ensures compliance.
Database Administrator	Jon Dagle	support@ictph.com	Manages database failover and integrity validation.
Business Continuity Officer	Jaylie Patlunag	jaylie@southbankinc.com	Communicates recovery status to business stakeholders.
AWS Enterprise Support Contact	Janna Leow	jannalyt@amazon.com	Engages AWS support for critical incidents.

8.3 Communication & Notification Procedures

1. **Incident Reporting:** All incidents must be logged in the ITSM platform and assigned an urgency level.
2. **Internal Notification:** Alerts sent via Email, Viber, Messenger GCs and other relevant communication channels to the team.
3. **Executive & Regulatory Communication:** Business Continuity Team will escalate major incidents to executives and external regulators if required.
4. **Post-Recovery Documentation:** A formal post-mortem report is prepared within 48 hours to document findings and improvements.

9.0 DR Infrastructure & Architecture

9.1 Architecture



9.2 AWS DR Environment

- **Primary Region**: Singapore (ap-southeast-1)
- **Secondary DR Region**: N. Virginia (us-east-1)
- **Backup Storage**: Amazon S3, Amazon RDS Snapshots, AWS Backup Vault
- **Replication Mechanisms**: AWS DRS, AWS Backup, Amazon S3 cross-region replication

9.3 Primary Architecture

- Compute Layer: Amazon EC2 instances hosting core banking applications.
- Database Layer: Multi-AZ Amazon RDS (MySQL) with multi-region replication.
- Storage Layer: Amazon S3 for backup object storage and Amazon EBS for persistent volumes.
- Networking: AWS VPN, AWS Transit Gateway, VPC Peering, and Route 53 for DNS failover.
- Security: AWS IAM for access control, AWS Security Hub, AWS WAF, and AWS Shield for threat protection.
- Monitoring & Logging: Amazon CloudWatch, AWS Config, and AWS CloudTrail for visibility and compliance.

9.4 Core Banking System Web Application & Microservices

Web Application

- Hosted on Amazon EC2 or AWS Elastic Beanstalk for scalability.
- Frontend built with React, Angular, or Vue.js, served via Amazon S3 and CloudFront.
- Backend APIs hosted on Amazon ECS (Fargate) or AWS Lambda for serverless execution.
- API Gateway to manage requests and security policies.

Microservices Architecture

- Containerized Services: Utilizes Amazon ECS or EKS (Kubernetes) for orchestration.
- Service Communication: AWS App Mesh for service discovery and communication.
- Data Layer: Each microservice connects to Amazon DynamoDB, RDS, or ElastiCache for optimized performance.
- Event-Driven Processing: Uses Amazon SQS and Amazon SNS for asynchronous communication.
- CI/CD Pipeline: AWS CodePipeline and CodeBuild for automated deployments and updates.
- Security: Implemented with AWS WAF, Shield, and IAM policies to restrict access.

9.5 AWS Services Used

SERVICE	PURPOSE
Amazon EC2	Compute for core banking applications
Amazon RDS	Database replication
AWS Backup	Scheduled backup and recovery
Amazon S3	Object storage for backups
AWS IAM	Access control
AWS Security Hub	Security monitoring
AWS Transit Gateway	Network connectivity management
Amazon Route 53	DNS failover and traffic routing
AWS CloudWatch	Monitoring and alerting
AWS CloudTrail	Logging and compliance tracking
Amazon ECS/EKS	Container orchestration

10. Disaster Recovery Process

2.1 Disaster Declaration

- Incident is reported to the DR Team / IT Group channeled via ticketing system or ITSM.
- Severity assessment is conducted.
- DR Manager declares a disaster and triggers the DR plan.

2.2 Recovery Execution Steps

1. Activate backup region (failover to secondary AWS region).
2. Restore databases from most recent backups or replica.
3. Restore microservices and web application using infrastructure-as-code (CloudFormation/Terraform).
4. Verify network connectivity and application availability.
5. Conduct security validation and compliance checks.
6. Test core banking transactions.
7. Notify stakeholders on recovery status.

2.3 Post-Recovery Actions and Reporting

- System performance monitoring.
- Security and compliance review.
- Root cause analysis and corrective measures.
- Reporting