BUSINESS REQUIREMENTS DOCUMENT

Core Digital Transformation for Retail Banking

Enterprise Architecture & Regulatory Compliance Initiative

Project Title	Core Digital Transformation for Retail Banking
Document Type	Business Requirements Document (BRD)
Date	February 17, 2026
Prepared By	Business Analyst / Project Manager
Version	1.0 – Initial Release
Status	Draft – Pending Stakeholder Review
Classification	Confidential

1. Executive Summary

A major retail bank currently operates legacy systems across critical banking operations including customer onboarding, loan servicing, fraud detection, and compliance monitoring. These fragmented systems result in compliance gaps, poor data integrity, and slow service rollouts. This BRD defines the business requirements for modernizing the bank's core systems using a secure, compliant, and cloud-native architecture — unifying all operations into a single, scalable digital platform.

2. Business Need & Problem Statement

Current State (As-Is)

- Legacy systems with siloed databases and batch processing workflows causing processing delays.
- Manual processes with limited real-time data visibility, increasing operational risk.
- High risk of non-compliance with regulatory mandates (KYC, AML, PCI-DSS, GDPR).
- Poor customer experience due to slow onboarding and loan processing times.
- Fragmented fraud detection with delayed alerting and manual review bottlenecks.

Future State (To-Be)

- Unified cloud-native architecture using microservices and containerization.
- Real-time data pipelines, centralized data warehouse, and secure APIs.
- Real-time fraud detection alerts and compliance monitoring dashboards.
- Full auditability, encryption, and role-based access controls (RBAC).
- Streamlined customer onboarding and loan processing via automated workflows.

3. Project Scope

In Scope

- Migration of all core banking applications to cloud-native microservices architecture.
- Design and deployment of real-time data pipelines and centralized data warehouse.
- Secure API gateway for inter-service communication and third-party integrations.
- Fraud detection and alerting system with customer analytics dashboards.
- Full encryption, role-based access control (RBAC), and audit logging.
- Regulatory compliance alignment: KYC, AML, PCI-DSS, and GDPR.
- Staff training on new systems and security protocols.

Out of Scope

- Retail branch network upgrades or physical infrastructure changes.
- Third-party vendor product development or modifications.
- Mobile app development (addressed in a separate parallel workstream).
- International market expansion activities.

4. Business Objectives

ID	Objective	Domain	Priority
OBJ-01	Migrate to a secure, cloud-native infrastructure by Q4 2026.	Technology	Critical
OBJ-02	Improve customer onboarding and loan processing time by 40%.	Operations	High
OBJ-03	Achieve 100% compliance with KYC, AML, PCI-DSS, and GDPR.	Compliance	Critical
OBJ-04	Maintain 99.99% uptime with scalable, redundant infrastructure.	Technology	High
OBJ-05	Reduce fraud losses through real-time detection and alerting.	Risk	High
OBJ-06	Enable data-driven decision-making via centralized analytics.	Strategy	Medium

5. Assumptions

- Executive sponsorship and budget approval remain stable throughout the project lifecycle.
- Vendor contracts are in place and cloud environment is provisioned and secure.
- Stakeholders are available for workshops, reviews, and validations.
- Cloud infrastructure and licensing will be procured within the first 60 days.
- Existing regulatory mandates (KYC, AML, PCI-DSS, GDPR) will not materially change during the project.
- Third-party API providers will maintain service availability during integration sprints.

6. Constraints

- All regulatory compliance milestones must be met without exception.
- Production system downtime must be minimized to approved maintenance windows only.
- Data residency requirements must comply with applicable jurisdiction laws.
- Project must operate within the approved annual IT budget of USD $7,920,000.
- Resource availability may be constrained during peak business periods (e.g., quarter-end).

7. Success Metrics

ID	Metric	Domain	Priority
SM-01	Zero regulatory violations post-launch in KYC, AML, PCI-DSS, and GDPR audits.	Compliance	Critical
SM-02	Less than 2 seconds of average API response time for all public-facing APIs.	Performance	High
SM-03	System uptime of 99.9% or greater following go-live across all production services.	Reliability	High
SM-04	Fraud detection alerts operational within 30 seconds of suspicious activity.	Security	High
SM-05	Successful CI/CD implementation with rollback functionality tested and validated.	DevOps	Medium
SM-06	Customer satisfaction improvement of 20%+ based on post-deployment NPS survey.	CX	Medium
SM-07	100% of core banking systems migrated to cloud-native architecture within timeline.	Technology	Critical

8. Key Stakeholders

Stakeholder	Role	Interest
CEO	Executive Sponsor	Strategic compliance and growth outcomes
CIO	Project Manager	On-time, on-budget delivery
CCO	Compliance Advisor	Zero regulatory violations
Enterprise Architect	Technical Governance	Scalable, secure architecture
CISO	Security Lead	Zero breaches, RBAC operational
Data Engineering Lead	Pipeline Owner	Real-time data integrity
Business Analyst	Requirements / UAT	Validated requirements and UAT sign-off
UX Lead	Customer Advocate	Improved onboarding NPS
External Auditor	Compliance Validator	Clean audit opinion

9. High-Level Risks

- Data migration errors: Phased migration with parallel run validation and rollback procedures.
- Regulatory non-compliance: Continuous compliance monitoring with dedicated Compliance Officer oversight.
- Legacy integration failures: Thorough API testing, sandbox environments, and incremental cutover.
- Cybersecurity breach: Zero-trust security posture, penetration testing, and 24/7 SOC monitoring.
- Budget overrun: Strict change control process; executive approval required for all scope changes.

10. Approval & Sign-Off

By signing below, the designated approvers confirm they have reviewed the contents of this Business Requirements Document and authorize progression to the requirements elicitation and design phases.

Name	Title	Signature	Date
	Chief Executive Officer		
	Chief Information Officer		
	Chief Compliance Officer		