PROJECT CHARTER

Core Digital Transformation for Retail Banking

Enterprise Architecture & Regulatory Compliance Initiative

Project Title	Core Digital Transformation for Retail Banking
Date	February 17, 2026
Project Sponsor	Chief Executive Officer (CEO)
Project Manager	Chief Information Officer (CIO)
Version	1.0 – Initial Release
Status	Active

1. Project Description

The Core Digital Transformation for Retail Banking project is a strategic initiative to modernize the bank's entire technology infrastructure and operational systems. The project will replace legacy batch-processing platforms with a unified, cloud-native architecture leveraging microservices, containerization, and real-time data pipelines. The transformation addresses critical gaps in customer experience, regulatory compliance, and data integrity across all banking operations including customer onboarding, transaction processing, and loan servicing.

2. Objectives

The project will achieve the following strategic objectives:

- Migrate all legacy systems from siloed databases and batch workflows to a unified cloud-native microservices architecture.
- Establish real-time data pipelines and a centralized data warehouse with secure APIs to enable data-driven decision-making.
- Implement full auditability, encryption, and role-based access controls (RBAC) to meet regulatory mandates.
- Achieve full compliance with KYC, AML, PCI-DSS, and GDPR regulatory frameworks.
- Reduce manual processing errors and improve system scalability to support business growth.
- Deploy fraud detection and customer analytics dashboards with real-time alerting capabilities.

3. Success Criteria

Project success will be measured against the following criteria:

- 100% of core banking systems migrated to cloud-native architecture within project timeline.
- Zero critical compliance findings in post-implementation KYC, AML, PCI-DSS, and GDPR audits.
- System uptime of 99.9% or greater following go-live for all production services.
- Real-time transaction processing latency reduced to under 500ms for 95th percentile requests.
- Fraud detection alerts operational within 30 seconds of suspicious activity.
- All data encrypted in transit and at rest; RBAC fully implemented and auditable.
- Successful User Acceptance Testing (UAT) with sign-off from business unit leads.

4. Key Stakeholders and Roles

Role / Title	Name / Department	Responsibility
Project Sponsor	CEO	Executive decision authority; final approval
Project Manager	CIO / IT Department	Day-to-day oversight and delivery
Enterprise Architect	IT Architecture Team	System design and integration governance
Compliance Officer	Regulatory Affairs	KYC, AML, PCI-DSS, GDPR alignment
Business Analyst	Operations	Requirements gathering and UAT coordination
Data Engineer	Data & Analytics	Pipeline design and data warehouse build
Security Officer	Information Security	Encryption, RBAC, and audit controls
Customer Rep / UX Lead	Customer Experience	Onboarding flow and dashboard design
External Auditor	Third-Party Firm	Independent compliance validation

5. Scope

5.1 In Scope

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

5.2 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.

6. Deliverables

- Cloud-native microservices architecture (deployed and tested in production).
- Real-time data pipeline and centralized data warehouse.
- Secure API gateway with full documentation.
- Fraud detection and customer analytics dashboards.
- Role-based access control system with encryption at rest and in transit.

- Regulatory compliance documentation package (KYC, AML, PCI-DSS, GDPR).
- System integration and UAT test results reports.
- Staff training materials and completion records.
- Post-implementation support runbooks and operational documentation.

7. Assumptions

- Executive sponsorship and budget approval remain stable throughout the project lifecycle.
- All required cloud infrastructure and licensing will be procured within the first 60 days.
- Business unit leads will dedicate sufficient time and resources to UAT activities.
- Existing regulatory mandates (KYC, AML, PCI-DSS, GDPR) will not materially change during the project.
- The bank's existing network infrastructure is capable of supporting the new cloud-native workloads.
- Third-party API providers will maintain service availability during integration sprints.

8. Constraints

- All regulatory compliance milestones must be met without exception; no scope reductions are permitted.
- Production system downtime must be minimized and scheduled only during approved maintenance windows.
- Data residency requirements must comply with applicable jurisdiction laws; no data may be stored outside approved regions.
- Project must work within the approved annual IT budget allocation.
- Resource availability may be constrained during peak business periods (e.g., quarter-end).

9. High-Level Risks

Risk	Prob.	Impact	Mitigation Strategy
Data migration errors causing data integrity issues	Medium	High	Phased migration with parallel run validation and rollback procedures.
Regulatory non-compliance during transition	Low	Critical	Continuous compliance monitoring; dedicated Compliance Officer involvement at all phases.
Legacy system integration failures	Medium	High	Thorough API testing, sandbox environments, and incremental cutover strategy.
Key personnel attrition during project	Low	Medium	Knowledge documentation, cross-training, and contractor contingency plan.
Cloud vendor outages or SLA breaches	Low	High	Multi-region redundancy and vendor SLA with financial penalties.
Budget overrun due to scope creep	Medium	Medium	Strict change control process; executive approval required for all scope changes.
Cybersecurity breach during migration	Low	Critical	Zero-trust security posture, pen testing, and 24/7 SOC monitoring throughout migration.

10. Milestones

Milestone	Target Date	Owner
Project Kick-off & Charter Approval	March 2026	CIO / Sponsor
Architecture Design & Infrastructure Provisioning	May 2026	Enterprise Architect
Data Pipeline & Warehouse Development Complete	August 2026	Data Engineer
Compliance Controls Implemented & Validated	October 2026	Compliance Officer
User Acceptance Testing (UAT) Completed	November 2026	Business Analyst
Production Go-Live	January 2027	CIO
Post-Implementation Review & Project Closure	March 2027	Project Manager

11. Budget

The following represents a high-level budget estimate for the project. Detailed cost breakdowns will be established in the Project Management Plan.

Budget Category	Estimated Cost (USD)
Cloud Infrastructure & Licensing	$2,400,000
Software Development & Integration	$3,200,000
Data Migration & Engineering	$800,000
Regulatory Compliance & External Audit	$500,000
Training & Change Management	$300,000
Contingency Reserve (10%)	$720,000
TOTAL BUDGET	**$7,920,000**

12. Approval

By signing below, the designated approvers authorize the initiation of this project and commit the resources and support defined herein.

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