REQUIREMENTS DOCUMENT

Core Digital Transformation for Retail Banking

Functional & Non-Functional Requirements

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

1. Purpose

This Requirements Document captures all functional and non-functional requirements gathered from key banking stakeholders through structured interviews and workshops. It serves as the authoritative reference for system design, development, testing, and compliance validation across the Core Digital Transformation for Retail Banking project. All requirements are traceable to business objectives and regulatory mandates.

2. Requirements Elicitation Approach

Requirements were elicited from the following stakeholder groups using the methods outlined below:

Stakeholder Group	Method	Focus Areas
Product Owners	Interviews + Workshops	Business logic for onboarding, transaction flow, loan approval, and fraud management
Compliance Teams	Document Review + Interviews	Audit trail requirements, KYC/AML data governance, PCI-DSS and GDPR reporting standards
DevOps Engineers	Technical Workshops	CI/CD pipeline needs, monitoring requirements, security enforcement, and deployment frequency
Customers (Sample)	Surveys + Focus Groups	Service reliability expectations, digital experience quality, and access control preferences
Security Officers	Threat Modelling Sessions	Zero-trust posture, encryption standards, RBAC design, and incident response workflows

3. Functional Requirements (FR)

Functional requirements define specific behaviors the system must perform. Each requirement is mapped to its originating stakeholder group and assigned a priority level.

3.1 Customer Onboarding & Account Management

ID	Requirement	Source	Priority	Status
FR-01	Customers can securely register and onboard via web and mobile apps with identity verification and KYC checks completed in real time.	Product Owners / Customers	**Critical**	Approved
FR-02	Customers can manage account settings, view statements, and update personal information through a self-service portal.	Product Owners / Customers	**High**	Approved
FR-03	The system must send automated notifications (email/SMS) for account actions, transaction alerts, and compliance events.	Product Owners	**Medium**	Approved
FR-04	Customer onboarding must be completed within 5 minutes end-to-end under normal operating conditions.	Product Owners / Customers	**High**	Approved

3.2 Compliance & Audit

ID	Requirement	Source	Priority	Status
FR-05	Compliance staff can access real-time audit logs and KYC/AML reports via a dedicated compliance dashboard.	Compliance Teams	**Critical**	Approved
FR-06	The system must automatically flag transactions that trigger AML rules and route them to compliance review queues.	Compliance Teams	**Critical**	Approved
FR-07	All data processing activities must be logged with a full audit trail including user, timestamp, action, and data modified.	Compliance Teams	**Critical**	Approved
FR-08	The system must support automated GDPR data subject access and deletion requests within mandated response timeframes.	Compliance Teams	**High**	Approved
FR-09	PCI-DSS compliant cardholder data environment must be isolated from non-payment systems with strict access controls.	Compliance / Security	**Critical**	Approved

3.3 Loan Servicing & Transaction Processing

ID	Requirement	Source	Priority	Status
FR-10	Product owners can configure loan approval workflows, eligibility rules, and interest rate parameters without code changes.	Product Owners	**High**	Approved
FR-11	The system must process payment transactions in real time with confirmation delivered within 500ms at the 95th percentile.	Product Owners / Customers	**Critical**	Approved
FR-12	Loan applications must be processed end-to-end — from submission through decision and disbursement — within 24 hours.	Product Owners	**High**	Approved

ID	Requirement	Source	Priority	Status
FR-13	The system must support automated credit scoring integration with third-party bureau APIs.	Product Owners	Medium	Approved

3.4 Fraud Detection & Alerting

ID	Requirement	Source	Priority	Status
FR-14	The fraud detection engine must generate alerts within 30 seconds of identifying suspicious transaction patterns.	Product Owners / Security	Critical	Approved
FR-15	Fraud detection rules must be configurable by authorized staff without system downtime or code deployments.	Product Owners	High	Approved
FR-16	The system must provide a fraud case management dashboard with investigation workflow, evidence capture, and resolution tracking.	Compliance / Security	High	Approved

3.5 DevOps & Deployment

ID	Requirement	Source	Priority	Status
FR-17	DevOps engineers can automate builds, tests, and deployment pipelines using a CI/CD platform integrated with the version control system.	DevOps Engineers	High	Approved
FR-18	Every deployment must include automated rollback capability triggered by failed health checks within 2 minutes of detection.	DevOps Engineers	Critical	Approved
FR-19	The system must support blue-green and canary deployment strategies to enable zero-downtime releases.	DevOps Engineers	High	Approved
FR-20	Infrastructure as Code (IaC) must be used for all environment provisioning to ensure consistency and auditability.	DevOps Engineers	Medium	Approved

4. Non-Functional Requirements (NFR)

Non-functional requirements define the quality attributes, performance standards, and operational constraints the system must satisfy. These apply system-wide unless otherwise specified.

4.1 Performance

ID	Requirement	Source	Priority	Status
NFR-01	Less than 2 seconds average API response time for all public-facing APIs under normal load conditions.	DevOps / Customers	Critical	Approved

ID	Requirement	Source	Priority	Status
NFR-02	Transaction processing latency must not exceed 500ms at the 95th percentile for all payment operations.	Product Owners	Critical	Approved
NFR-03	The system must support a minimum of 10,000 concurrent users without performance degradation.	DevOps Engineers	High	Approved
NFR-04	Database query response times must not exceed 200ms for 99% of queries under peak load.	DevOps Engineers	High	Approved

4.2 Availability & Reliability

ID	Requirement	Source	Priority	Status
NFR-05	System must achieve 99.99% uptime across all core services, measured on a rolling 30-day basis.	DevOps / Product Owners	Critical	Approved
NFR-06	Mean Time To Recovery (MTTR) from any production incident must be under 15 minutes.	DevOps Engineers	High	Approved
NFR-07	All critical services must be deployed across multiple geographic availability zones to prevent single points of failure.	DevOps / Security	Critical	Approved
NFR-08	Automated failover must activate within 60 seconds of any primary service failure without manual intervention.	DevOps Engineers	High	Approved

4.3 Security & Compliance

ID	Requirement	Source	Priority	Status
NFR-09	All data at rest and in transit must comply with bank-grade AES-256 encryption policies.	Security / Compliance	Critical	Approved
NFR-10	Role-based access control (RBAC) must be implemented across all systems with least-privilege principles enforced.	Security	Critical	Approved
NFR-11	Multi-factor authentication (MFA) must be enforced for all administrative and privileged user accounts.	Security	Critical	Approved
NFR-12	Annual penetration testing and quarterly vulnerability assessments must be conducted by a qualified third party.	Security / Compliance	High	Approved
NFR-13	All access to sensitive data must be logged and monitored with anomaly detection alerts sent within 5 minutes.	Security	Critical	Approved

4.4 Scalability & Maintainability

ID	Requirement	Source	Priority	Status
NFR-14	The architecture must support horizontal auto-scaling to handle 3x peak traffic without manual intervention.	DevOps / Product Owners	High	Approved
NFR-15	All microservices must be independently deployable and versioned to enable rolling updates without system-wide downtime.	DevOps Engineers	High	Approved
NFR-16	The system must support configuration management without code changes for non-technical business rule updates.	Product Owners	Medium	Approved

4.5 Usability & Accessibility

ID	Requirement	Source	Priority	Status
NFR-17	All customer-facing interfaces must comply with WCAG 2.1 AA accessibility standards.	Customers / UX Lead	High	Approved
NFR-18	Customer satisfaction improvement of 20% or more must be achieved based on post-deployment NPS survey.	Product Owners / Customers	Medium	Approved
NFR-19	Staff must be able to complete training on new systems and pass competency assessment within 4 hours.	HR / Operations	Medium	Approved

5. Requirements Summary

Category	Count	Critical	High	Medium
Functional – Onboarding	4	1	2	1
Functional – Compliance & Audit	5	4	1	0
Functional – Loan & Transactions	4	2	1	1
Functional – Fraud Detection	3	1	2	0
Functional – DevOps	4	1	2	1
NFR – Performance	4	2	2	0
NFR – Availability	4	2	2	0
NFR – Security	5	4	1	0
NFR – Scalability	3	0	2	1
NFR – Usability	3	0	1	2
TOTAL	39	17	16	6

6. Priority Legend

Priority	Definition
Critical	Must be implemented for go-live. Failure to deliver constitutes project failure or regulatory breach.

Priority	Definition
High	Required for full business value. Should be delivered in initial release; deferral requires executive approval.
Medium	Desirable for user experience or operational efficiency. May be deferred to a subsequent release if necessary.