RISK REGISTER

Core Digital Transformation for Retail Banking — Enterprise Architecture & Regulatory Compliance Initiative

Date: February 18, 2026 | Version: 1.0 | Prepared By: Business Analyst / Project Manager | Status: Active

Risk ID	Risk Title	Category	Cause	Event	Impact Description	Probability (1–5)	Impact (1–5)	Risk Score (P × I)	Trigger / Early Warning Sign	Response Strategy
R1	KYC API SLA Violation	Threat	Third-party provider latency or service downtime	Delay in customer onboarding and account activation	Compliance risk, reputational damage, customer churn	4	5	20	Missed onboarding logs or delayed provider API response beyond SLA threshold	Implement provider SLA monitoring with automated escalation matrix; establish fallback identity verification provider
R2	Legacy System Integration Failure	Threat	Outdated APIs and schema mismatches between legacy and modern systems	Transactional errors, data inconsistency, or data loss during migration	Project delay, rollback required, additional cost, potential compliance exposure	4	4	16	Failed data validation checks between legacy and modern system environments	Conduct sandbox integration tests and version control audits; enforce phased cutover with parallel-run validation
R3	CI/CD Pipeline Breakdown	Threat	Inadequate rollback automation or pipeline misconfiguration	Deployment failure causing production outage or failed sprint releases	System downtime, failed sprint releases, SLA breach on 99.9% uptime commitment	3	3	9	Build errors, test failures, or unresponsive staging environments detected during CI/CD run	Enhance automated rollback scripts; add pre-deployment quality gates and canary deployment validation
R4	Positive Stakeholder Adoption	Opportunity	Intuitive UX workflows, dashboards, and effective change management	Increased staff and customer engagement with the new digital platform	Accelerated feedback loops, smoother rollout, higher NPS, reduced training cycles	2	4	8	Early user feedback praising UX design and positive adoption metrics from sandbox testing	Highlight success stories internally; promote adoption features through champions programme and recognition of early adopters
R5	Regulatory Non-Compliance During Transition	Threat	Incomplete compliance controls or gaps during system cutover	KYC, AML, PCI-DSS, or GDPR audit findings during or after migration	Regulatory penalties, project halt, reputational damage, potential enforcement action	2	5	10	Compliance dashboard alerts showing unresolved audit findings or missed control checkpoints	Continuous compliance monitoring with dedicated CCO oversight; zero-exception policy on all compliance milestones
R6	Cybersecurity Breach During Migration	Threat	Elevated attack surface during cloud migration window	Unauthorised access or data exfiltration during transition period	Data breach, regulatory penalties, severe reputational damage, financial loss	2	5	10	SOC anomaly detection alerts; unexpected access patterns in audit logs	Zero-trust security posture; penetration testing prior to go-live; 24/7 SOC monitoring throughout migration
R7	Budget Overrun Due to Scope Creep	Threat	Uncontrolled scope changes or underestimated complexity	Project costs exceed approved budget of USD $7,920,000	Project delays, reduced deliverables, executive escalation, resource reallocation	3	3	9	Change requests exceeding 10% of sprint capacity or budget variance warnings in project dashboards	Strict change control process requiring executive approval for all scope changes; weekly budget variance reviews

RISK SCORING LEGEND

High Risk (Score ≥ 15)
Medium Risk (Score 9–14)
Low Risk (Score < 9)
Opportunity