

# STAKEHOLDER ENGAGEMENT PLAN

## Core Digital Transformation for Retail Banking

Enterprise Architecture & Regulatory Compliance Initiative

<b>Project Title</b>	Core Digital Transformation for Retail Banking
<b>Date</b>	February 17, 2026
<b>Prepared By</b>	Project Manager / CIO
<b>Version</b>	1.0 – Initial Release
<b>PMI Scale</b>	Unaware (U) → Resistant (R) → Neutral (N) → Supportive (S) → Leading (L)

### Purpose

This Stakeholder Engagement Plan identifies the current and desired commitment levels of all 13 project stakeholders using the PMI engagement scale. For each stakeholder, a gap analysis is performed between the current state and the desired state, and targeted engagement strategies are defined to close that gap — or maintain the existing level where it is already sufficient. The plan is a living document and should be reviewed and updated at each major project milestone.

### PMI Engagement Scale

Code	Level	Description
U	Unaware	Unaware of the project and its potential impact.
R	Resistant	Aware of the project but resistant to any change it may bring.
N	Neutral	Aware of the project but neither supportive nor resistant.
S	Supportive	Aware of the project and actively supportive of its success.
L	Leading	Actively engaged in ensuring the project succeeds; a visible champion.

### Engagement Gap Summary

The table below provides a snapshot of each stakeholder's current vs. desired engagement level and whether the goal is to move them up the scale or maintain their current level.

ID	Stakeholder	Current	Desired	Action
S-01	Chief Executive Officer (CEO)	S	L	Move →
S-02	Chief Information Officer (CIO)	L	L	Maintain
S-03	Chief Compliance Officer (CCO)	S	L	Move →

ID	Stakeholder	Current	Desired	Action
S-04	<b>Enterprise Architect</b>	L	L	Maintain
S-05	<b>Chief Information Security Officer (CISO)</b>	N	L	Move →
S-06	<b>Data Engineering Lead</b>	S	L	Move →
S-07	<b>Business Analyst</b>	S	L	Move →
S-08	<b>Customer Experience / UX Lead</b>	S	S	Maintain
S-09	<b>Retail Banking Operations Manager</b>	N	S	Move →
S-10	<b>External Auditor (Third-Party Firm)</b>	N	S	Move →
S-11	<b>Cloud Infrastructure Vendor</b>	S	S	Maintain
S-12	<b>Bank Staff / End Users</b>	N	S	Move →
S-13	<b>Regulatory Bodies (FCA, CFPB, PCI Council)</b>	N	N	Maintain

## Stakeholder Engagement Plan — Detail

ID	Stakeholder	Current Level	→	Desired Level	Rationale for Gap	Engagement Strategies
S-01	Chief Executive Officer (CEO)	S – Supportive	→	L – Leading	Sponsor needs to actively champion the initiative, not just approve deliverables.	<ul style="list-style-type: none"> <li>1. Monthly executive briefings with milestone dashboards and risk summaries.</li> <li>2. Involve CEO in milestone celebrations and regulatory validation announcements.</li> <li>3. Provide concise escalation memos to keep decisions fast and visible.</li> </ul>
S-02	Chief Information Officer (CIO)	L – Leading	→	L – Leading	Project Manager is already at the highest engagement level; maintain momentum.	<ul style="list-style-type: none"> <li>1. Weekly status reviews and daily stand-ups during critical delivery phases.</li> <li>2. Empower CIO with real-time project dashboards and risk registers.</li> <li>3. Recognize contributions publicly in steering committee updates.</li> </ul>
S-03	Chief Compliance Officer (CCO)	S – Supportive	→	L – Leading	Regulatory stakes are critical; CCO must co-lead compliance decisions, not merely review.	<ul style="list-style-type: none"> <li>1. Bi-weekly compliance checkpoint meetings with live audit trail reviews.</li> <li>2. Include CCO as approver for all KYC, AML, PCI-DSS, and GDPR deliverables.</li> <li>3. Provide early warning alerts for any regulatory risk so CCO can act proactively.</li> </ul>
S-04	Enterprise Architect	L – Leading	→	L – Leading	Technical governance requires sustained leadership engagement through all design phases.	<ul style="list-style-type: none"> <li>1. Weekly architecture review cadence with documented design decisions.</li> <li>2. Assign EA as technical approver for all integration and API designs.</li> <li>3. Involve EA in vendor evaluation and cloud infrastructure sign-offs.</li> </ul>
S-05	Chief Information Security Officer (CISO)	N – Neutral	→	L – Leading	Security is a critical risk vector; CISO must shift from passive reviewer to active security champion.	<ul style="list-style-type: none"> <li>1. Schedule bi-weekly security design reviews with early threat-model walkthroughs.</li> <li>2. Involve CISO in zero-trust architecture decisions and pen-test planning.</li> <li>3. Share a dedicated security risk register and escalate findings immediately.</li> <li>4. Align CISO success metrics (zero breaches, RBAC validation) with project KPIs.</li> </ul>
S-06	Data Engineering Lead	S – Supportive	→	L – Leading	Pipeline integrity and warehouse design decisions require leading-level accountability.	<ul style="list-style-type: none"> <li>1. Weekly sprint reviews with data quality dashboards.</li> <li>2. Empower as technical owner for all pipeline and warehouse deliverables.</li> <li>3. Pair with Compliance Officer to ensure data governance requirements are embedded.</li> </ul>
S-07	Business Analyst	S – Supportive	→	L – Leading	UAT coordination and requirements traceability are pivotal; BA must drive, not just facilitate.	<ul style="list-style-type: none"> <li>1. Assign sole ownership of requirements traceability matrix and UAT plan.</li> <li>2. Host bi-weekly requirements reviews with business unit stakeholders.</li> <li>3. Provide structured feedback loops after each sprint to keep BA engaged.</li> </ul>
S-08	Customer Experience / UX Lead	S – Supportive	→	S – Supportive	Current supportive engagement is appropriate; sustain through design and testing phases.	<ul style="list-style-type: none"> <li>1. Bi-weekly UX review sessions with prototype walkthroughs and user feedback.</li> <li>2. Involve in customer onboarding flow sign-off and dashboard UAT.</li> <li>3. Share post-launch NPS metrics to validate UX impact and sustain motivation.</li> </ul>
S-09	Retail Banking Operations Manager	N – Neutral	→	S – Supportive	Operational alignment is essential to minimize	<ul style="list-style-type: none"> <li>1. Monthly progress briefings with impact-on-operations summaries.</li> <li>2. Involve in change management planning and rollout communications.</li> <li>3. Host 'future-state' demos to build confidence in new systems and workflows.</li> </ul>

ID	Stakeholder	Current Level	→	Desired Level	Rationale for Gap	Engagement Strategies
					disruption and ensure staff adoption.	
S-10	External Auditor (Third-Party Firm)	N – Neutral	→	S – Supportive	A well-informed auditor produces cleaner reviews; proactive engagement reduces audit risk.	<ol style="list-style-type: none"> <li>Formal milestone gate reports with full compliance evidence packages.</li> <li>Schedule pre-audit briefings to align on evidence requirements and formats.</li> <li>Maintain open document repository accessible to auditors throughout the project.</li> </ol>
S-11	Cloud Infrastructure Vendor	S – Supportive	→	S – Supportive	Vendor is a key delivery partner; sustain engagement through SLA monitoring and reviews.	<ol style="list-style-type: none"> <li>Monthly service reviews with SLA performance scorecards.</li> <li>Escalation path defined in contract for outages or delivery failures.</li> <li>Quarterly roadmap discussions to align vendor capabilities with future needs.</li> </ol>
S-12	Bank Staff / End Users	N – Neutral	→	S – Supportive	Adoption by end users directly impacts operational success; resistance must be pre-empted.	<ol style="list-style-type: none"> <li>Change management newsletter cadence explaining 'what's changing and why'.</li> <li>Role-based training sessions with hands-on practice in sandbox environments.</li> <li>Feedback forums after training to surface concerns and iterate on materials.</li> <li>Recognise early adopters to build internal champions across branches.</li> </ol>
S-13	Regulatory Bodies (FCA, CFPB, PCI Council)	N – Neutral	→	N – Neutral	Regulators are external authorities; maintain compliance and formal reporting — no more engagement needed.	<ol style="list-style-type: none"> <li>Timely formal submissions of all required compliance reports.</li> <li>Ensure zero findings at each compliance milestone gate.</li> <li>Maintain regulatory change log in case mandates evolve during the project.</li> </ol>