Open Banking

Open Banking Implementation Guidelines

For Banks

June 2026

Contents

01	Introduction: Open Banking in Nigeria	3
02	The Role of Banks in the Open Banking Ecosystem	5
03	Open Banking Use-cases for Banks	10
04	Bank readiness: gap assessment and landscape	17
05	Technology architecture and tool stack	22
06	Data Management, Storage, and Security	28
07	Organisational and cross-functional readiness	31
08	Customer education and engagement	33
09	Cost structure and revenue opportunities	35
10	Partnership strategy and ecosystem	39
11	Capability development for Open Banking success	40

Open Banking Implementation Guide for Banks

1. Introduction: Open Banking in Nigeria

The Central Bank of Nigeria (CBN) is set to declare Open Banking operational in Nigeria. The earlier released framework and operational guidelines are now transitioning from ‘concept documents’ into regulatory requirements.

Open Banking introduces a structured, consent-driven framework that allows financial data to be shared securely between banks, fintechs, and other regulated players within Nigeria’s financial ecosystem.

While compliance is a key motivator, success in Open Banking requires a perspective beyond just ’sticking with the rules’. This is necessary to remain relevant in the long run.

- **Rising Customer Expectations:** Customers now demand convenience, personalization, and transparency across all financial interactions.
- **Disintermediation and Competition:** Data sharing democratizes customer information, enabling FinTechs and platforms to compete directly.
- **New Growth Opportunities:** APIs are becoming products; players can monetize data, form strategic partnerships, and participate in ecosystem-driven value chains.
- **Shift in Industry Roles:** Banks evolve from product providers to platform participants and ecosystem enablers.

1.1. Why Open Banking Is Being Introduced Now and What Problem It Solves

- It reduces fragmentation by enabling a unified, permission-based view of customer financial data across institutions.
- It stimulates competition and innovation by lowering barriers for regulated fintechs to build customer-centric financial products.

- It establishes a safer, standardised framework for data sharing between banks and fintechs, anchored on explicit customer consent.
- It aligns Nigeria's financial system with global Open Banking practices, technical standards, and regulatory norms.

1.2. What Open Banking Means in Practical Terms for Banks

Effective participation in Open Banking extends beyond regulatory compliance or technical integration. It requires coordinated institutional readiness across strategy, operations, technology, and governance. Weakness in any one dimension can constrain adoption, elevate risk, or erode customer trust.

Participation therefore requires readiness across five (5) dimensions:

- **Strategic readiness:** Banks must first determine the role they intend to play within the ecosystem. Whether positioning as a utility provider, a platform orchestrator, or a hybrid participant, this choice influences investment priorities, partnership strategy, revenue architecture, and risk appetite.
- **Operational readiness:** Open Banking introduces new operational responsibilities that must function reliably at scale. Banks should establish clear internal processes for managing consent, onboarding partners, resolving disputes, responding to incidents, and supporting customers interacting with third-party providers.
- **Technical readiness:** Unlike traditional internal banking systems, Open Banking infrastructure must support continuous external access while maintaining security, performance, and reliability.
- **Governance readiness:** Open Banking expands the bank's risk perimeter beyond its internal systems to include third-party participants, shared infrastructure, and ecosystem dependencies. Governance structures must evolve accordingly.
- **Regulatory readiness**: A working knowledge of the CBN Open Banking Framework, the NDPR, and evolving compliance obligations is particularly crucial for Banks due to stricter regulatory expectations and oversight. This should be supported by internal capacity to monitor regulatory developments and respond to supervisory enquiries.

1.3. Purpose of This Guide

This guide was created to support banks in:

- Participating responsibly within regulatory expectations
- Making informed strategic and architectural decisions
- Building durable ecosystem capabilities
- Converting compliance into long-term competitive advantage

2.The Role of Banks in the Open Banking Ecosystem

Open Banking creates a distributed financial architecture in which banks serve as the **trusted foundation** upon which ecosystem innovation occurs.

2.1. Banks as Custodians, Infrastructure Providers, and Platform Enablers

Within this model, banks are authorised data holders responsible for safeguarding customer information while enabling controlled access through secure interfaces. With customer consent and within regulatory parameters, banks must be able to:

- Provide access to defined financial datasets
- Support permitted actions such as payment initiation
- Maintain infrastructure resilience
- Authenticate ecosystem participants
- Preserve data integrity

This positioning shifts banks from closed operators toward controlled platform participants. In practical terms, banks function as the **trust anchor of Open Banking** ensuring that innovation does not compromise systemic stability.

2.2. How Banks Complement Fintechs

Open Banking is not designed to displace banks, but to redistribute innovation across specialised participants.

Banks contribute:

- Regulatory credibility
- Balance sheet strength
- Mature risk frameworks

- Operational resilience

Fintechs extend this by delivering:

- Experience-led interfaces
- Specialised solutions
- Faster iteration cycles

2.0. Strategic Readiness: Open Banking Readiness in Banks

Before committing capital or restructuring operating models, as a bank, you must first establish a clear view of **why** you are participating in Open Banking and what role you intend to play within the emerging ecosystem.

When there is absence of strategic clarity, Open Banking initiatives often devolve into fragmented compliance programmes – technologically functional but commercially deficient.

Strategic readiness therefore begins with an explicit articulation of your intended posture: the level of ecosystem influence you seek, the capabilities you are prepared to build, and the risk you are willing to absorb in pursuit of long-term value.

While institutional strategies vary, Open Banking participation typically clusters around three positioning models.

2.1. Banks as Utility Providers

Banks adopting a utility posture focus on delivering secure, reliable, and compliant access to customer-permissioned data while monetising infrastructure through structured API exposure.

The strategic objective is simply operational excellence rather than ecosystem orchestration.

This model is characterised by:

- Emphasis on resilience, security, and regulatory alignment
- Predictable usage-based revenue from API consumption
- Controlled partner exposure
- Lower organisational disruption

For many institutions, particularly those early in their digital maturity journey, the utility model provides a pragmatic entry point into Open Banking.

However, while strategically conservative, it offers limited differentiation. Over time, infrastructure provision alone risks becoming commoditised as ecosystem standards mature.

2.2. Banks as Platform Orchestrators

A platform posture positions the bank as an ecosystem orchestrator rather than a passive financial infrastructure provider. The bank actively curates partner networks, embeds financial capabilities into third-party journeys, and enables distribution beyond its proprietary channels.

Instead of asking customers to come to the bank, the bank becomes present wherever customers transact.

This approach typically involves:

- Hosting partner marketplaces or embedded finance capabilities
- Enabling third-party distribution of banking services
- Co-creating products with fintech partners
- Leveraging data to personalise ecosystem experiences

The upside can be significant however, platform strategies demand far more than technology investment. They require organisational transformation, including:

- Product-led operating models
- Mature partnership governance
- Faster decision cycles
- Elevated risk management capabilities
- Management comfort with controlled openness

2.3. Banks as Hybrid Participants

In practice, many banks must evolve toward a hybrid posture i.e. combining the stability of a **utility provider** with **selective platform plays** in areas aligned to institutional strengths.

A hybrid strategy allows banks to:

- Maintain predictable infrastructure revenue
- Experiment with ecosystem-led growth
- Sequence transformation rather than forcing it
- Allocate capital more deliberately

For example, a bank may operate as a utility for basic data services while building platform capabilities around SME financing, payments, or embedded credit — domains where it already possesses competitive advantage.

Hybrid positioning reduces strategic overreach while preserving future optionality.
Strategic implication: Leadership discipline lies in choosing where to orchestrate and where to enable.

2.4. Strategic Clarity Before Execution

Open Banking is not a neutral compliance shift, it is a structural change in how banks create and distribute value.

A clearly defined posture helps leadership answer critical questions early:

- Where will the bank compete versus enable?
- Which capabilities must remain proprietary?
- How much ecosystem dependency is acceptable?
- What revenue pools should Open Banking unlock?

Without this clarity, technology investments risk becoming disconnected from the strategy.

Strategy should therefore precede architecture not the reverse.

3.0. Open Banking Use-cases for Banks

3.1. Identifying High-Value Open Banking Use Cases

Open Banking introduces a broad set of technical capabilities, but not every capability translates into strategic value for a bank. Banks must therefore approach use-case selection as a disciplined strategic exercise rather than a reactive response to movement in the ecosystem.

High-value use cases are those that strengthen customer relevance, unlock new revenue pools, improve risk intelligence, or increase operational efficiency without introducing unnecessary complexity or regulatory exposure.

Strong Open Banking use cases typically:

- Address a clearly defined customer or partner need.
- Enhance decision-making through responsible use of permissioned financial data.
- Reduce friction across onboarding, payments, lending, or servicing journeys.
- Improve the bank's competitive positioning or distribution reach.
- Can be delivered reliably within the bank's existing or planned technology architecture.

Conversely, initiatives driven primarily by technological novelty or by the availability of external data rarely produce durable advantage. Banks should avoid pursuing capabilities that expand infrastructure obligations without a clear path to enterprise value.

Use-case prioritisation should therefore balance:

- **Strategic relevance**: Does this strengthen our long-term position?
- **Data dependency**: Do we have reliable access to the required data?
- **Execution feasibility**: Can we deliver this safely at scale?
- **Risk implications**: Are governance and controls sufficient?
- **Economic viability**: Does the opportunity justify the investment?

Institutions that apply this discipline are better positioned to convert Open Banking from a compliance requirement into a strategic growth lever.

3.2. Some priority use-case domains for banks

Open Banking expands what banks can deliver not only through their own channels but across partner ecosystems. However, value creation requires focus. Rather than attempting to pursue all opportunities simultaneously, banks should concentrate on domains aligned with their balance sheet strengths, customer base, and strategic ambition.

Open Banking use cases for banks typically cluster across four interconnected domains, each carrying distinct implications for risk, infrastructure, and organisational readiness.

3.2.1. Payments

A merchant building an online checkout today may depend on card payments. Customers must manually input card details, transactions can fail due to authentication or network issues, and merchants incur card processing fees. Similarly, recurring payments often require customers to repeatedly authorise transactions or depend on ineffective debit mandate systems that can be tough to set up and manage.

Open Banking allows customers to authorise payments directly from their bank accounts through secure APIs. The result is faster payments, lower costs for merchants, and fewer steps for customers during checkout. This enables:

- **Pay-by-bank and account-to-account payments –** This allows customers to make payments directly from their bank accounts without relying on cards or manual transfers. Instead of entering card details, the customer simply authorises the payment through their bank using a secure consent flow.
- **Direct-debit/recurring payment flows –** This, on the other hand, allows customers to authorise a fintech/merchant to debit their account automatically at agreed intervals (e.g. Netflix subscriptions). After the initial consent, payments can be triggered without requiring the customer to manually approve each transaction (This may still be subject to regulatory safeguards and mandate controls however the existing protocol around the GSI gives it a launchpad to take off).
- **Card Management –** Offers APIs for secure access to card-related information, enabling customers to manage their cards within third-party apps.

3.2.2. Credit

An SME applying for a loan today may need to submit months of bank statements and wait several days or weeks for manual review. Even then, lenders may struggle to accurately assess cash-flow stability, leading either to rejected applications or very tough lending limits.

With customer consent, lenders can securely access transaction-level financial data directly from bank accounts. This enables:

- **Cash-flow–based lending –** Fintechs can now assess affordability and risk using real-time transaction data, supporting inclusion for underserved individuals and SMEs. The conversation easily moves from “do you have collateral?” to “does your financial behaviour support repayment?”
- **Real-time Credit Decisioning:** With access to verified financial data from banks, time-to-yes or time-to-no will significantly be shortened reducing the time between application and decision. Beyond this, lenders will be able to monitor borrower health after disbursement and catch risk early on.
- **Embedded Credit:** This will allow fintechs embed credit products at the point of need e.g. BNPL checkout on e-commerce platforms, inventory financing inside merchant tools etc.
- **Dynamic Credit Limits:** Rather than issuing static loan limits, fintechs can adjust exposure as a borrower’s financial position evolves. e.g. increasing limits when income improves or tightening exposure when risk indicators rise.

3.2.3. Personal finance management

In the current financial ecosystem, a salaried professional might receive income in one bank account, keep savings in another, and make payments using a third account or digital wallet. To understand their monthly financial position, they would need to check multiple apps and manually combine the information. Similarly, a budgeting application that does not integrate with banks may require users to manually input expenses, which quickly becomes impractical and leads to incomplete financial records.

With customer consent, Open Banking allows fintechs to securely retrieve account balances and transaction data across multiple banks through standardised APIs. This enables:

- **Account aggregation and holistic financial views**
  With customer consent, banks can integrate data from external institutions to construct a comprehensive picture of a customer's financial life. This supports more relevant advisory, improved segmentation, and stronger relationship depth.
- **Personal financial management capabilities**
  Embedding spend analysis, budgeting support, and behavioural insights within digital channels can help customers make better financial decisions while increasing engagement with the bank's primary interface.
- **Savings and financial wellness tools**
  Data-driven nudges, automated savings mechanisms, and goal-based planning tools can improve customer outcomes while strengthening long-term deposit relationships.

3.2.4. Identity management and verification

A bank receiving a new customer application today typically relies on manual document submission, BVN/NIN validation, and internal checks to confirm identity and account ownership. In addition to this, Open Banking will enable banks to participate in a consent-driven identity infrastructure; both as providers of verified identity data to authorised third parties, and as consumers of identity signals from other institutions where permitted.

This creates two distinct opportunities for banks:

- As an identity data provider, banks can expose secure, consent-gated APIs that allow authorised fintechs and third-party applications to verify customer identity attributes in real time. This includes account-to-name matching, account status validation, and other verification services. Rather than customers repeating the same onboarding process across multiple platforms, the bank becomes the trusted source of record.
- As a consumer of risk signals, where supported and permitted, banks can receive structured financial signals from other participating institutions to supplement their own customer data. This supports more accurate risk profiling, safer customer- acquisition decisions, and stronger transaction monitoring particularly for customers with thin internal credit histories.

3.2.5. Ecosystem distribution and embedded finance

Open Banking shifts banks from being destination institutions to becoming embedded financial providers within broader commercial ecosystems.

- **Banking-as-a-Service (BaaS)**
  Exposing regulated capabilities such as accounts, payments, or lending infrastructure allows partners to integrate financial services directly into their offerings.
- **Partner marketplace models**
  Banks can curate fintech solutions within their channels, creating a controlled ecosystem while retaining customer nearness.
- **Contextual financial services**
  Embedding credit, insurance, or payment options at the point of customer need increases conversion while reducing acquisition costs.

3.2.6. Operational efficiency and risk enhancement

Not all Open Banking value is customer-facing. Some of the most immediate benefits arise internally through smarter processes and improved risk visibility.

- **Digitised onboarding and identity verification**
  Permissioned data access can streamline KYC processes and reduce manual documentation requirements.
- **Fraud detection and anomaly monitoring**
  Broader transaction visibility supports earlier detection of suspicious patterns.
- **Automated financial reconciliation**
  Access to structured data can simplify treasury and back-office workflows, particularly for corporate clients.
- **Regulatory reporting and audit support**
  Standardised data flows improve traceability and reduce reporting friction.

3.3. Evaluating use-cases: a decision framework for investment prioritisation

Open Banking investments compete with other enterprise priorities for capital, technology capacity, and leadership attention. Banks should therefore evaluate use cases through a structured decision framework that supports disciplined investment choices. Rather than asking *"Can we build this?"*, the more important question is *"Should we build this now?"*

A practical evaluation model considers four core dimensions:

3.3.1. Strategic value

Assess the degree to which the use case strengthens the bank's long-term positioning.

Key considerations include:

- Does this deepen primary customer relationships?
- Will it expand distribution or ecosystem reach?
- Does it reinforce our intended posture (utility, platform, or hybrid)?
- Can it create durable competitive differentiation?

3.3.2. Economic potential

Evaluate whether the initiative can generate measurable financial return, directly or indirectly.

Banks should consider:

- Revenue generation (API fees, interchange alternatives, lending growth)
- Balance sheet impact (deposit growth, improved asset quality)
- Cost reduction (manual processing, onboarding friction)
- Customer lifetime value expansion

Not all high-value use cases monetise immediately; however, they should demonstrate a credible path to economic contribution.

3.3.3. Execution readiness

Determine whether the bank can deliver the capability safely and reliably within current constraints.

Assessment areas include:

- Technology maturity and integration complexity
- Availability of internal skills and delivery capacity
- Partner readiness where ecosystem participation is required
- Operational support capabilities

Use cases that significantly exceed current execution capacity may be better sequenced into later phases.

3.3.4. Risk and regulatory exposure

Open Banking expands the bank’s operational surface area. Each initiative should therefore be evaluated for incremental risk.

Key questions include:

- Does this increase data exposure or third-party dependency?
- Are governance and control frameworks sufficiently mature?
- Could service failure materially affect customers or market confidence?
- Are regulatory expectations clear?

Where risk is elevated, institutions should ensure that control capabilities scale in parallel with product ambition.

4.0. Bank readiness: gap assessment and landscape audit

Before participating meaningfully in Open Banking, banks must develop a clear view of their current-state capabilities relative to ecosystem expectations. Readiness is rarely limited by a single deficiency; more often, it is a combination of legacy architecture, fragmented processes, unclear ownership structures, and inadequate risk models.

A structured gap assessment enables banks to transition deliberately, reducing execution risk while ensuring that investments align with long-term strategic positioning.

4.1. Assessing the current state against Open Banking requirements

The readiness exercise should begin with a comprehensive review of the bank's products, API architecture, integration landscape, and operating model to determine their suitability for external, permission-based data sharing.

Key questions include:

- Which existing products can be exposed safely through APIs without compromising core system stability?
- Is the current API architecture capable of supporting secure, real-time external access?
- Do operating processes assume closed-system control, or are they adaptable to a multi-party ecosystem?
- Are risk frameworks calibrated for third-party participation?

This assessment should extend beyond compliance checklists to evaluate whether the bank can support sustained ecosystem interaction without introducing operational fragility.

Banks often discover that systems designed for internal efficiency require redesign before they can support reliable external consumption.

4.2. Identifying capability gaps across technology, people, process, and governance

Once the current state is understood, institutions should map capability gaps across four operational layers.

4.2.1. Technology

Technology gaps often emerge when systems originally designed for internal banking operations are required to support real-time external integrations.

- Legacy core systems not designed for real-time interoperability
- Limited API management capabilities
- Insufficient monitoring of external traffic
- Authentication frameworks that require modernisation
- Architectural dependencies that create single points of failure

For example: *A bank's core banking system processes transactions in batch cycles overnight, rather than in real time. When fintech partners attempt to retrieve account balances or transaction histories through APIs, the data may be delayed or inconsistent. The impact of this could be that Fintech applications relying on real-time data cannot function reliably, leading to poor customer experiences.*

Addressing these gaps early reduces the likelihood of service instability once integrations scale.

4.2.2. People

Open Banking introduces capabilities that may not currently exist within traditional banking teams. While general technical competence may exist, the teams are not trained in bridging technical competence and Open Banking strategy.

For example: *A bank assigns Open Banking responsibility to a traditional IT delivery team focused on internal system upgrades. The team approaches Open Banking as a technical integration project rather than a platform strategy, resulting in slow growth and unclear value creation.*

Banks should evaluate whether they have:

- Product leaders experienced in platform thinking
- Engineers skilled in API-first design
- Risk and compliance professionals familiar with data-sharing ecosystems
- Partnership managers capable of governing fintech relationships
- Customer support teams prepared to handle consent-related queries

Where gaps exist, banks must decide whether to build internally, upskill, or selectively partner.

4.2.3. Process

Processes designed for closed banking environments often prove too rigid for ecosystem participation.

For example: *a fintech partner seeking API access must pass through multiple internal approval layers involving technology, legal, compliance, and procurement. The impact of this could be that onboarding takes 6 to 9 months, discouraging fintechs from integrating with the bank.*

Common areas requiring redesign include:

- Third-party onboarding and due diligence workflows
- Incident detection and coordinated response
- Consent lifecycle management
- Partner change management
- Cross-functional decision-making

Processes should prioritise clarity, repeatability, and speed without weakening risk controls.

4.2.4. Governance

Governance models must evolve as the bank's risk perimeter expands beyond institutional boundaries.

For example: *responsibility for Open Banking is shared informally between digital banking, IT, branding/marketing, and customer-facing teams while appointing an Open Banking Centre of Excellence (CoE) Lead as a single point of co-ordination. This means that no single leader has authority to coordinate investments, partnerships, and operational priorities; however, a single role exists to oversee this collaboration.*

Banks should assess whether they have:

- Clearly defined accountability for Open Banking initiatives
- An Open Banking Centre of Excellence (CoE) to drive cross-competency collaboration.
- Executive oversight aligned with strategic importance
- Decision frameworks balancing innovation with prudential standards
- Mechanisms for continuous risk evaluation

Weak governance frequently manifests not as overt failure, but as delayed decisions and fragmented execution.

4.3. Prioritising gaps based on risk, effort, and strategic relevance

Not all gaps require immediate remediation. To be effective, banks must sequence their readiness investments using three lenses:

- **Risk Exposure**
  Capabilities that protect customer data, ensure system stability, or support regulatory compliance should be addressed first.
- **Implementation Effort**
  Banks should distinguish between foundational upgrades that require multi-year transformation and targeted improvements that unlock near-term participation.
- **Strategic Relevance**
  Priority should be given to capabilities that support the bank's intended ecosystem role. A platform-oriented bank, for example, may invest earlier in developer experience and partner tooling, while a utility-focused participant may emphasise resilience and cost efficiency.

This structured prioritisation prevents institutions from overinvesting in capabilities that do not materially advance their Open Banking objectives.

4.4. From assessment to execution

A gap assessment delivers value only when translated into an actionable roadmap. Banks should consolidate findings into a phased readiness plan that:

- Sequences foundational and advanced capabilities
- Aligns investment with strategic intent
- Establishes measurable readiness milestones
- Integrates regulatory timelines without becoming compliance-driven

Importantly, readiness should be treated as a progression rather than a binary state. Institutions rarely become "fully ready" before participating; instead, they mature through iterative capability building. Banks that approach readiness as a strategic transformation rather than a regulatory hurdle are significantly better positioned to capture long-term value.

An example of what prioritizing execution looks like

Assessment Finding

The bank’s third-party onboarding process was designed for large vendors and can take several months to complete.

Execution Response

The bank introduces a tiered partner onboarding model, where:

- Low-risk fintech integrations follow a streamlined approval process
- Higher-risk integrations undergo deeper due diligence

In parallel, the bank creates clear incident response protocols for managing service disruptions involving external partners.

Outcome:

Fintech onboarding becomes faster while maintaining appropriate risk oversight.

5.0. Technology architecture and tool stack

Open Banking transforms the bank's technology environment from an inward-facing infrastructure into an externally consumable platform. Systems that were historically optimised for internal control must now support secure, continuous interaction with third-party participants without compromising resilience, performance, or customer trust.

Technology architecture should therefore be approached not as a compliance requirement, but as a long-term strategic capability that supports the bank's role in the ecosystem. Poor architectural decisions at this stage will become deeply embedded and difficult to solve once partner dependencies form.

5.1. Designing for external consumption

Traditional banking infrastructure assumes predictable traffic patterns and limited external exposure. Open Banking introduces variable demand, partner-driven integrations, and real-time data access expectations.

Banks should ensure their architecture is deliberately designed to:

- Support secure external connectivity without exposing core systems
- Handle fluctuating integration volumes without service degradation
- Maintain consistent performance across partner channels
- Enable controlled evolution as standards and use cases mature
- Maintain disaster recovery and failover mechanisms, including defined Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and explicit provisions for token and consent persistence during failover events

Rather than connecting third parties directly to core banking platforms, institutions must introduce abstraction layers that separate internal environments from ecosystem traffic.

5.2. Core architectural components

While technology stacks will vary across institutions, the following foundational components will consistently support safe and effective participation across the Nigerian banking ecosystem.

5.2.1. API Management Layer

The API layer functions as the structured gateway through which external participants interact with the bank.

A mature API capability should enable the bank to:

- Authenticate ecosystem participants before granting access
- Apply traffic controls to prevent system overload
- Monitor usage patterns in real time
- Version APIs without disrupting partner integrations
- Enforce access policies aligned with consent permissions

Importantly, API management is not merely a technical tool, it becomes the bank's primary mechanism for governing ecosystem interaction.

5.2.2. Consent Engine/Infrastructure

Consent sits at the operational heart of Open Banking. It is a real-time control layer that governs who can access what, for what purpose, and for how long. The bank's infrastructure must therefore support the capture, verification, enforcement, monitoring, and withdrawal of permissions with speed, clarity, and auditability.

What effective consent infrastructure enables:

A mature consent capability allows a bank to:

- **Bind access to permissions –** Every API call is permitted only if it maps to a valid, active consent grant (purpose, scope, duration and responsible party).
- **Maintain auditable records –** The bank can prove, at any point, who authorised what, when, through which channel, and under which disclosure terms.
- **Propagate consent status across systems –** Consent state is not trapped in one database; it is synchronised across API gateway, Identity and Access Management systems, core banking integration layers, monitoring tools, and partner interfaces.
- **Terminate access immediately on revocation –** Revocation triggers an enforced "kill switch" that invalidates tokens and blocks future calls without manual intervention.

5.2.2.1. Consent capture and disclosure layer

This is the customer-facing component that presents the permission request clearly and captures an explicit decision. Minimum requirements will look like:

- Purpose-led consent prompts (what data, why, for how long, and who is requesting it)
- Clear separation from general TandCs (consent must be a distinct decision)
- Support for partial permissions (e.g., balance only vs. full transactions)
- Channel consistency (mobile, web, branch-assisted flows where applicable)

For Example:
A lending app requests: "Last 6 months of transactions for loan qualification assessment that's valid for 30 days."

Customer sees: data categories, duration and revocation path, then authorises.

5.2.2.2. Consent verification and customer authentication

This confirms the customer is the one granting permission, using strong authentication aligned with bank security policies. Typical mechanisms will look like:

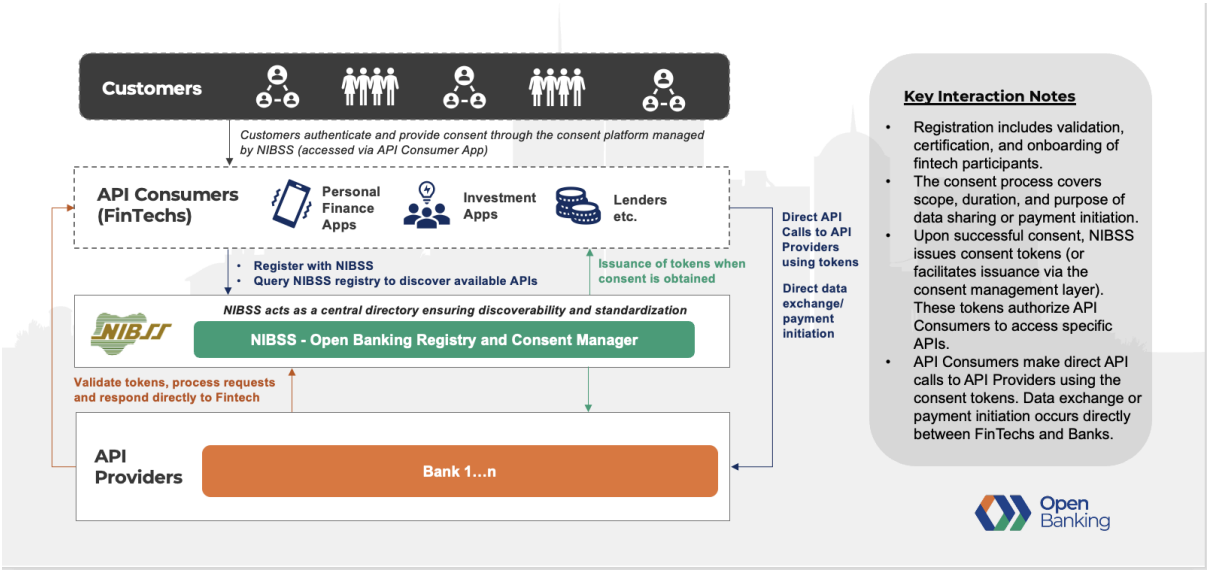
- Step-up authentication (OTP, app approval, biometric, hardware token depending on channel)
- Risk-based authentication (higher friction for higher-risk data/actions)
  Device binding or session integrity checks for digital channels

5.2.2.3. Consent registry (system of record that sits with NIBSS)

This is the Open Banking ecosystem record-keeping system for active and historical consents. The Open Banking Registry will be domiciled with NIBSS and accessible by all relevant parties.

What it must store:

- Customer identity reference
- Requesting party identity (TPP/app)
- Consent scope (data types, accounts, actions permitted)
- Purpose statement and disclosure version presented at time of approval
- Validity period and expiry timestamp
- Status history (granted, renewed, revoked, expired)
- Linkage IDs to tokens and access logs



[Design sample customer consent journey from Fintech to Bank and back]

5.2.2.4. Enforcement Layer (Real-Time Gatekeeping)

This is where consent becomes operational. Enforcement ensures every access request is checked against active consent rules.

Where enforcement should live

- At the API gateway (first-line blocking)
- Within IAM/token services (token scope validation)
- At critical downstream service boundaries (defence in depth)

What it enforces

- Scope: only approved data fields/endpoints
- Time: only within the consent validity window
- Purpose constraints: access tied to declared use case class (where supported)
- Rate and behaviour controls: anomaly detection + throttling

5.2.2.5. Consent Revocation and Kill-Switch Capability

Revocation is the moment where trust is tested. A bank must make revocation simple for customers and absolute for systems.

Customer-facing requirements

- Consent dashboard (see connected apps, permissions granted, expiry)
- One-tap “disconnect” (revocation without calling support)
- Clear communication on what revocation changes (e.g., “app will no longer refresh data”)

System requirements

- Immediate token invalidation (access tokens, refresh tokens)
- Real-time propagation (API gateway, IAM, Open Banking consent registry etc.)
- Partner notification (where required) with revocation timestamp

5.2.2.6. Auditability, Monitoring, and Reporting

Consent controls must be observable. If something goes wrong, the bank must trace it end-to-end.

Key Mechanisms

- Consent grant events and channel used
- Token issuance events linked to consent IDs
- API call logs mapped to consent scope
- Failed access attempts (scope violations, expired consent, unregistered party)
- Revocation events and confirmation of enforcement

5.2.3. Strong Authentication and Access Control

As data flows extend beyond institutional boundaries, identity assurance becomes central to risk management.
Banks should implement authentication frameworks that:

- Replace credential sharing with secure token-based access
- Validate both the third-party provider and the customer interaction
- Limit access strictly to authorised data scopes
- Expire permissions automatically when consent lapses

Robust authentication protects not only customer data but also the bank’s regulatory posture and reputational standing.

5.2.4. Sandbox and Developer Enablement

Ecosystem growth in Open Banking is closely tied to developer adoption. Before committing resources, partners evaluate how easily they can integrate, test, and deploy. A well-structured sandbox therefore functions as both a risk-control mechanism and a strategic enablement layer, allowing partners to validate integrations safely before interacting with live systems.

Beyond containment of production risk, sandbox environments signal institutional readiness and materially reduce onboarding friction. Banks that invest in developer experience often become preferred integration partners, supporting stronger ecosystem participation and higher API utilisation.

Banks should design sandbox environments to:

- Support safe experimentation without exposing production infrastructure or customer data.
- Accelerate partner onboarding through self-service access and clear integration pathways.
- Validate interoperability early, identifying schema, authentication, or workflow issues before go-live.
- Improve production stability by ensuring integrations are tested under realistic conditions.

5.2.4.1. Winning trust through Developer-first documentation

Banks can strengthen developer trust by providing clear, well-structured documentation with practical integration guidance. Documentation should function as part of the product, providing clear endpoint definitions, authentication requirements, error codes, and sample requests. Strong documentation reduces support overhead and builds developer confidence.

5.2.4.2. Structured path to production

Transitioning from sandbox to live access should follow defined readiness checkpoints such as technical certification, security validation, and operational review. Clarity in this progression helps partners plan deployments with confidence.

6.0. Data Management, Storage, and Security

In an Open Banking environment, banks operate as ***regulated custodians of customer financial data***. Participation therefore requires disciplined data management practices that preserve confidentiality, ensure integrity, and support controlled accessibility. Effective data stewardship is not only a regulatory obligation it is foundational to ecosystem trust.

Banks should approach data management as an integrated capability spanning storage architecture, access governance, protection standards, and operational traceability.

6.1. Secure Storage and Controlled Access

Customer data should be stored within architectures designed to protect sensitive financial information across its full lifecycle from creation to archival or deletion.

Banks are expected to:

- **Segregate sensitive data environments**, reducing exposure to internal and external threats.
- **Implement strong encryption** for data both in transit and at rest, aligned with industry security standards.
- **Apply role-based access controls**, ensuring employees and systems can only access data necessary for their function.
- **Enforce least-privilege principles**, limiting the operational blast radius of compromised credentials or internal error.

Access governance should extend beyond employees to include third-party connections, with authentication and authorisation mechanisms designed to prevent unauthorised data retrieval.

6.2. Data Minimisation and Purpose Limitation

Open Banking reinforces the principle that data shared should be proportionate to the service being delivered. Excessive data exposure increases risk without improving customer outcomes.

Banks should ensure that:

- Only the **minimum dataset required** for a permitted use case is exposed via APIs.
- Data requests are **bound to explicit customer consent** and defined purposes.

- Retention periods reflect regulatory requirements and operational necessity rather than convenience.

Purpose limitation helps prevent function creep, strengthens compliance posture, and supports defensible data governance.

6.3. Integration and Data Management Layers

Direct exposure of core banking systems introduces unnecessary operational risk. Instead, banks should deploy structured data layers that enable controlled external interaction while preserving system resilience.

Typical architecture includes:

- **Integration Layer:** Acts as a controlled interface between internal systems and external participants, translating core data into standardised API formats while enforcing authentication and rate limits.
- **Management Layer:** Provides orchestration, monitoring, and policy enforcement governing how data flows, which permissions apply, and when access should be constrained or terminated.
- **Abstraction from Core Systems:** Separating Open Banking interfaces from core processing environments reduces the likelihood that partner activity will affect transactional stability.

Well-designed layers allow banks to scale participation without compromising operational continuity.

6.4. Auditability and Traceability

Open Banking requires that every data interaction be verifiable and reconstructible. Banks must therefore maintain detailed records that support internal review, partner assurance, and regulatory oversight.

Institutions should be able to provide evidence for:

- **Who accessed the data** (participant identity).
- **What data was accessed** and under which category.
- **When access occurred** and how long it persisted.
- **Why access was permitted**, linked directly to customer consent.

Comprehensive audit trails enable faster dispute resolution, support incident investigations, and reinforce institutional accountability.

6.5. Security as an Operational Discipline

Security in Open Banking is not a static control but an evolving operational responsibility. As participation scales, banks should continuously review protection standards, test defensive controls, and refine access governance to address emerging threats.

Institutions that treat data security as core infrastructure (rather than as a compliance checkpoint) are better positioned to maintain customer confidence and support sustainable ecosystem growth.

7.0. Organisational and cross-functional readiness

Open Banking cannot be implemented as a standalone technology programme. It requires coordinated execution across functions that have historically operated independently. This is precisely why the establishment of an Open Banking Centre of Excellence (CoE) is critical to the successful implementation of initiatives.

7.1. Open Banking Centre of Excellence (CoE)

Open Banking introduces new operational dependencies that span technical delivery, regulatory interpretation, customer experience, and partner management. Banks should ensure that the following functions are actively integrated into the centre of excellence with a single senior point of oversight ensuring collaboration:

- **Technology**: responsible for API architecture, security controls, performance, and system resilience.
- **Legal and Compliance**: interpret regulatory obligations, structure participation agreements, and oversee data protection adherence.
- **Risk Management**: assess third-party exposure, operational vulnerabilities, and systemic implications of data sharing.
- **Branch Operations and Relationship Management**: manage day-to-day workflows including consent handling, dispute resolution, and incident coordination.
- **Branding and Communications:** manage brand perception and customer communication where Open Banking is concerned.
- **Product**: identify viable use cases, align Open Banking capabilities with customer value, and guide commercial outcomes.
- **Customer Support**: serve as the primary interface for customer concerns related to consent, data sharing, and third-party access.

The objective is not merely representation from each function, but active collaboration supported by shared accountability.

7.2. Ownership and decision rights

Ambiguity in decision-making can materially slow implementation and increase risk exposure. Banks should therefore define ownership structures early, ensuring that critical decisions are made at the appropriate level and with sufficient context.

Key areas requiring explicit ownership include:

- Approval of third-party connectivity
- Data exposure policies
- Consent experience design
- Incident escalation thresholds
- API pricing and commercial models
- Customer communication standards

Clear decision rights reduce execution friction and support faster responses during operational events.

7.3. Governance structures for coordination

Given the strategic and regulatory implications of Open Banking, most institutions will benefit from establishing a formal governance model.

Recommended structures include:

- **Executive Steering Committee**
  Provides strategic direction, approves risk appetite, and aligns Open Banking participation with broader institutional priorities.
- **Open Banking Centre of Excellence**
  Coordinates implementation across functions, tracks milestones, and ensures dependencies are actively managed.
- **Risk and Compliance Oversight Forums**
  Periodically review third-party exposure, data governance posture, and regulatory alignment.

Governance should be designed to enable progress while maintaining control, avoiding both excessive centralisation and fragmented execution.

8.0. Customer education and engagement

Customer trust is a foundational condition for Open Banking adoption. Even where infrastructure is mature, participation will remain limited if customers do not understand how their data is used or feel uncertain about the risks.

Banks therefore play a critical role in translating technical change into clear, customer-relevant narratives.

8.1. Explaining Open Banking in clear terms

Communication should focus on control, security, and tangible benefit rather than technical mechanics.

Effective messaging typically emphasises that:

- Customers **choose if and when** their data is shared.
- Permissions are **specific, time-bound, and revocable**.
- Data sharing enables **better financial tools**, faster services, and more personalised offerings.

Avoiding technical jargon helps reduce perceived complexity and lowers psychological barriers to participation.

For Example:

Technical Explanation (Less Effective): *"Our platform uses secure APIs to retrieve financial data from participating institutions after authentication."*

Customer-Friendly Explanation: *"You can choose to securely connect your bank account so the app can show all your finances in one place. Your bank will ask you to approve the connection, and you can disconnect it at any time."*

The explanation focuses on choice and convenience, rather than infrastructure.

8.2. Managing trust, expectations, and misconceptions

In markets like Nigeria where there is heightened sensitivity to financial fraud, being proactive with reassurance is essential. Banks should anticipate common concerns and address them directly. Transparency strengthens credibility and reduces resistance.

Typical misconceptions include:

- ***"The bank is selling my data."*** *Clarify that data is only shared with customer authorisation and for defined purposes.*
- ***"Sharing data means losing control."*** *Reinforce that customers can withdraw consent at any time.*
- ***"The bank is responsible for everything a third party does."*** *Clearly explain the boundaries of responsibility while highlighting safeguards built into the ecosystem.*

8.3. Preparing frontline and support teams

Frontline employees often shape customer perception more than formal policy statements. Training should therefore extend beyond awareness to practical readiness especially where it concerns physical interaction with customers.

Support teams should be able to:

- Explain Open Banking confidently in simple language
- Guide customers through consent review or revocation
- Recognise and escalate potential fraud scenarios
- Address disputes involving third-party access
- Reassure customers during service disruptions

Institutions that equip their teams effectively are better positioned to convert curiosity into adoption. Well-prepared banks recognise that technology enables Open Banking but people operationalise it. Aligning teams, governance, and customer engagement practices ensures that participation is both controlled and commercially sustainable.

9.0. Cost structure and revenue opportunities

9.1. Cost of API access

Open Banking monetization goes beyond charging for data access; it is ultimately driven by the economic value created through its use.

Global experience suggests that Open Banking frequently begins with a form of “freemium” access in order to encourage participation, lower entry barriers, and stimulate innovation. For example, UK regulators required certain mandatory APIs (account information, transaction history, and payment initiation) to be provided free of charge in order to promote competition.

However, access to bank infrastructure rarely remains cost-free over the long term. As participation scales, banks might introduce pricing structures that balance ecosystem adoption with the cost of building and maintaining secure, highly-available APIs.

Common approaches may include:

- Tiered per-call or per-transaction pricing
- Threshold-based fees for higher-volume usage
- Monthly platform or subscription fees for dashboard/API access
- Premium pricing for sensitive or high-risk endpoints
- Outcome-based pricing for verified actions or payments

9.2. Assumptions on Certification and Open Banking Registry (OBR) Registration fees

While no formal guidance has been issued by the Central Bank of Nigeria on certification and OBR fee structures, a number of plausible approaches may be adopted to serve the ecosystem:

- Certification may operate on an annual basis, with a fee structure that scales with institutional size.
- For API consumers (ACs), a flat fee structure may apply reflecting their role and operational scale.
- Tier 0 entities may initially be exempt from certain fees to encourage early-stage innovation and reduce entry barriers.

- Institutions signing on to the OBR may be required to pay a fee. These fees may be administered by NIBSS or another designated operator, which would oversee the technical management of the registry.
- Transactions may continue under existing CBN fee structures, meaning transfers are handled by underlying payment systems such as NIBSS, UP, Interswitch, and Etranzact without change.
- Checks for customer profiles, account details, KYC data, and balances may initially be free, supporting frictionless data sharing.
- Pulling transaction statements may attract a modest fee while the creation of mandates, virtual accounts, and similar features remain free, with transactional activity on these instruments charged according to prevailing CBN rules.

Please Note: The above listed fee structures are educated assumptions on the part of Open Banking Nigeria and in no shape or form constitute a formal guidance on CBN fee structures.

9.3. Revenue Opportunities

9.3.1. Usage-based monetisation

Revenue is linked to measurable infrastructure activity, including:

- API calls that expose account or transaction data
- Payment initiation events
- Identity and verification requests
- Volume of connected third-party applications

This model aligns revenue with operational load and allows income to scale naturally as ecosystem participation increases. For many banks, usage-based pricing will form the commercial foundation of Open Banking.

9.3.2. Outcome-based monetisation

Revenue is tied to successful financial outcomes rather than technical access. Examples include:

- Payments successfully initiated through partner channels
- Loans originated using third-party data
- Accounts opened via embedded journeys
- Merchant transactions processed through bank rails

Outcome-based models align bank incentives with ecosystem performance and encourage deeper partner integration. Over time, these models often generate higher lifetime value than per-call pricing alone.

9.3.3. Value-added service monetisation

Beyond raw data exposure, banks can monetise enhanced capabilities that improve partner decision-making or reduce operational risk.

Examples include:

- Income verification and affordability signals
- Account validation and fraud indicators
- Risk scoring insights
- Premium data packages with higher reliability guarantees
- Advanced reporting and reconciliation services

Value-added services reposition the bank from a data source to a decision-enablement partner. This is typically where differentiation and stronger margins begin to emerge.

9.3.4. Embedded finance enablement

Some of the most significant Open Banking revenue opportunities arise when banks embed financial capabilities directly into third-party platforms.

Examples include:

- Banking services embedded within fintech apps
- Merchant checkout financing
- Payroll-linked financial products
- Platform-based lending
- Account issuance within digital ecosystems

In these models, the bank participates economically in the partner's growth rather than charging solely for access.

Institutions that develop strong embedded finance capabilities often transition from infrastructure providers to ecosystem anchors.

9.3.5. Revenue sharing and ecosystem economics

As Open Banking matures, banks increasingly generate value not only through access pricing but through economic participation in ecosystem outcomes.

Revenue-sharing models are most effective where financial value is co-created across multiple participants particularly in journeys where the bank provides regulated infrastructure while partners drive distribution or customer experience.

Rather than capturing value in isolation, banks participate proportionately in the economic activity they enable.

9.3.6. Use-cases for revenue sharing

Revenue participation is typically strongest in models where the bank remains central to the financial transaction or risk structure.

Common applications include:

- **Account-to-account payment flows:** Banks may share in merchant service fees when payments are initiated through partner platforms.
- **Embedded finance journeys:** When financial products are distributed within third-party ecosystems (such as marketplaces, payroll platforms, or vertical SaaS) banks often participate in lending margins, interchange equivalents, or float economics.
- **Digitally originated lending:** Where fintech partners support origination, underwriting insights, or customer acquisition, revenue may be split across interest income or fees
- **SME platform integrations:** Financial tools embedded into accounting, inventory, or commerce platforms can create recurring transaction streams in which the bank participates.

Banks should avoid mechanically adopting market splits without evaluating their structural contribution. Actual economics should reflect:

- risk ownership
- funding responsibilities
- operational cost
- customer acquisition burden

10. Partnership strategy and ecosystem participation

Open Banking changes how banks work with external partners. Instead of being occasional integrations, partnerships become part of the bank's operating model influencing distribution, customer access, and revenue generation.

The goal is therefore not to partner widely, but to partner deliberately.

While banks may interact with many ecosystem participants, the following two relationships typically shape outcomes more than others.

10.1. Customer-facing Fintechs

These partners help banks reach customers in new ways through lending platforms, savings tools, payment experiences, and embedded finance journeys. When governed well, they expand distribution without requiring the bank to build every customer experience internally.

For Example:

An e-commerce platform integrates pay-by-bank functionality into its checkout flow.

The fintech partner manages:

- *payment initiation*
- *customer consent interface*
- *merchant integrations*

The bank processes:

- *the underlying account-to-account payment*
- *underlying customer consent flows*
- *settlement and clearing*

The bank participates in digital commerce transactions that might otherwise have been processed entirely through card networks.

10.2. Aggregators and connectivity platforms

These providers simplify integration and can speed up ecosystem participation. However, they may also sit between the bank and downstream partners. Banks should therefore be clear about when speed is worth the trade-off and when maintaining direct relationships is strategically preferable.

Not every integration needs to be owned but decisions about proximity to customers should always be intentional.

For example:

A bank wants to participate in the Open Banking ecosystem but does not yet have the capacity to integrate individually with dozens of fintech partners. Instead, the bank connects to a connectivity platform that already provides standardised API access to many fintech applications.

The bank can enter the ecosystem quickly without managing numerous individual integrations.

10.2. Structuring Partnerships

Because Open Banking involves regulated data and financial access, partnership agreements should be designed with operational resilience in mind.

Banks should ensure clarity around:

- how data can be used
- expected service levels
- responsibility if something goes wrong
- how the relationship can be exited without disrupting customers

Over-reliance on any single partner should be avoided. Dependency risk is easier to prevent than to unwind.

11. Capability development for Open Banking success

Open Banking is not delivered by technology alone. It requires banks to strengthen internal capabilities across engineering, operations, governance, and culture. Institutions that invest early in capability development are better positioned to operate reliably, support ecosystem growth, and capture long-term value.

Capability building should therefore be treated as a strategic programme not a side initiative.

11.1. Building internal technical competence

Banks must evolve toward an **API-first operating model**, where services are designed for secure external consumption rather than closed internal use.

This requires deliberate investment in skills and engineering discipline.

Key priorities include:

- Upskilling engineering and product teams on modular architecture, API lifecycle management, and secure integration practices.
- Embedding security into development workflows, ensuring controls such as strong authentication, encryption, and access governance are designed from the outset rather than layered on later.
- Engineering for resilience, with infrastructure capable of supporting high availability, predictable latency, and safe failover.

Many banks will benefit from establishing a dedicated Open Banking Centre of Excellence responsible for API strategy, partner integrations, and developer experience. Concentrating expertise reduces fragmentation and accelerates maturity.

11.2. API maturity and operational excellence

APIs quickly become critical infrastructure. Their stability directly affects partner operations and customer experience. Operational predictability builds ecosystem confidence and confidence drives adoption.

Banks should focus on:

- Designing stable, well-versioned APIs so enhancements do not unintentionally disrupt partner services.
- Maintaining continuous performance monitoring, supported by automated alerts and defined incident-response procedures.
- Establishing clear change and deprecation policies, typically providing partners sufficient transition time before retiring older versions.

11.3. Winning developer trust

In an Open Banking environment, developers become an important stakeholder group. Their experience integrating with a bank often determines whether that institution becomes a preferred partner.

Banks can strengthen developer trust by providing:

- Clear, well-structured documentation with practical integration guidance
- Streamlined onboarding processes
- Sandbox environments that mirror production conditions closely enough for meaningful testing
- Proactive communication on maintenance windows, outages, and upcoming changes

11.4. Cultural and organisational shift

Perhaps the most demanding aspect of Open Banking is organisational rather than technical. Banks are moving from controlled, inward-facing systems toward a more connected operating posture.

This shift typically requires:

- Stronger collaboration across technology, compliance, product, and risk functions, replacing sequential approvals with coordinated decision-making.
- Platform-oriented thinking, where success is measured not only by proprietary products but also by the health and reach of the surrounding ecosystem.
- Incentive structures that support long-term outcomes, such as partner adoption, API reliability, and sustainable revenue rather than short-term activity metrics alone.

Capability development is ultimately about readiness for sustained participation. Open Banking is not a one-time launch but an evolving operating model.

Banks that build strong technical foundations, disciplined operational practices, and collaborative internal cultures position themselves to participate with confidence and grow alongside the ecosystem rather than react to it.