

A PRACTICAL HYBRID BANKING ROLLOUT

Your institution. Connected.

A step-by-step path for banks, EMIs and license holders—from the first use case to an accountable operation.

START FOCUSED. EXPAND WITH CONFIDENCE.

01 / DEFINE

Choose the outcome.

Customers, services and operating scope.

03 / CONTROL

Set the policies.

Identity, roles, reviews and evidence.

05 / CONNECT

Test the services.

Providers, failure cases and reconciliation.

02 / DESIGN

Place the modules.

Core, wallets, hosting and connections.

04 / PROVE

Run the journey.

Onboarding through the first account.

06 / OPERATE

Launch in stages.

Owned decisions, monitoring and support.

CHOOSE YOUR STARTING POINT

Three starting points. One modular approach.

FIAT EMI

Improve the payment experience.

Start with account visibility, recipients, payment instructions and staff approvals. Retain the existing ledger, safeguarding arrangements and payment providers.

EXISTING BANK

Add wallets to e-banking.

Retain the core and customer relationship. Select custody, supported assets and wallet controls; expose approved positions and actions in the client workspace.

LICENSE HOLDER

Build the operating platform.

Assess Hybrid Core for a new operation. Set up the team, records and controls, then connect the providers required for the permitted services.

First decision

Which customer workflow will the first pilot complete—and which services stay outside it?

Define a pilot you can sign off.

Make the first release concrete before selecting every module.

Service scope	Client segment, countries, currencies, account types and first payment or wallet journey.	Output: an agreed service catalogue and exclusions.
Authority	Customer relationship owner, relevant license scope, contractual partners and approval responsibilities.	Output: named owners for onboarding, funds, custody and complaints.
Success	A small client cohort, volume limits, exception cases and measurable acceptance criteria.	Output: a pilot checklist with institution sign-off.
Delivery	Institution operations, compliance and technology leads working with OVRIDE and relevant providers.	Output: delivery plan, dependencies, support model and commercial scope.

STEP 02 / ARCHITECTURE & INTEGRATION

Decide where records and services live.

A Select the authoritative core

Keep the existing core, or configure Hybrid Core for a new operation. Define account IDs, currencies, balances and transaction states.

B Place the deployment

Choose on-premise, private cloud or hybrid. Record data location, keys, model access, backup and restore ownership.

C Map each connection

Document APIs, customer identifiers, permitted operations, status events and retry rules. Reconcile all changes with the authoritative records.

D Define the wallet model

Select custody and key controls, networks and assets. Keep wallet balances, fiat balances and pending transfers clearly distinct.

Approval to proceed

Signed architecture, data-flow map and interface contracts. An imported balance is not a reconciled ledger.

Set identity, controls and evidence.

WHO MAY ACT

Identity & roles

Register the Hybrid-ID application and exact return URLs. Assign operations, approval, compliance and audit roles. Request optional verification consent separately.

WHAT MAY PROCEED

Risk & review

Set country rules, required sanctions sources, recipient review, transaction limits and escalation paths. Validate required screening coverage before opening affected flows.

WHAT IS RETAINED

Audit & proof

Record reasons, actors and policy versions. Define private retention and proof publication. Verify confirmed Explorer evidence without exposing sensitive records.

Acceptance evidence

Role isolation · Required reviews · Blocked destinations · Versioned policy changes · Proof status

Prove the first client journey.

A familiar identity makes the start easier. The institution owns the decision.

01

Continue with Hybrid-ID

The client signs in and returns to the institution’s application.

02

Share what is needed

Request consent for supported verification metadata. Capture missing relationship details.

03

Review the application

An authorized officer inspects required checks, resolves exceptions and records a decision.

04

Open the workspace

After approval, create the appropriate account record and explain the enabled services.

“Use my Hybrid-ID to start an application with this institution.”

Target agent-assisted journey: the client sees and confirms the requested permissions. It is not an automatic approval.

STEP 05 / FROM PILOT TO CONNECTED SERVICES

Connect, reconcile and test failure.

CONNECT

One service at a time.

Start with a payment provider or wallet workflow. Agree status mappings, limits and credentials. Add cards or market execution only when in scope.

RECONCILE

Verify the whole result.

Compare account and provider records. Track pending, confirmed, returned and failed activity. Prove that retries cannot create duplicate financial effects.

REHEARSE

Test the difficult cases.

Use representative test data for rejected recipients, missing screening, expired access, provider outages and delayed events. Test backup and recovery.

Release gate

The institution accepts the evidence, unresolved issues, operating limits and rollback plan before activation.

ILLUSTRATIVE ROLLOUTS

Two institutions. Different first releases.

DUBAI-BASED BANK / ADD CRYPTO WALLETS

Keep the bank core in place.

1 Confirm the permitted service

Agree customer and asset eligibility, custody responsibility and any required approvals.

2 Connect a focused wallet view

Map bank customer IDs to wallet records. Show supported positions inside e-banking.

3 Enable a controlled pilot

Test signing approvals, transfer checks and reconciliation before expanding access.

PHILIPPINE COOPERATIVE BANK / MODERNIZE SERVICE

Begin with everyday member banking.

1 Map the existing operation

Confirm member onboarding, current core records and the initial payment services.

2 Configure identity and reviews

Set staff roles, relationship review, recipients, limits and an approved hosting design.

3 Pilot the member journey

Reconcile records and payment statuses; train staff on exceptions before broad rollout.

STEP 06 / OPERATE & EXPAND

Make the operation repeatable.

A successful launch has named owners, usable controls and a next step.

EVERY DAY

Operate with context.

Review exceptions, reconcile records, support clients and inspect required feed freshness. Escalate unresolved checks to the responsible team.

EVERY CHANGE

Keep decisions traceable.

Version policy amendments with an owner and reason. Check proof publication, access reviews, service changes and recovery readiness.

NEXT RELEASE

Grow the ecosystem.

Add a new currency, payment route, card programme or permitted asset only after the provider and operational checks are complete.

Bring to the first workshop

Your license scope, core and provider inventory, hosting constraints, and one priority client journey.

[Discuss implementation with OVRYDE](#)[Explore the architecture](#)[Preview the experience](#)