Building on Open Finance: A Founder Playbook for Consent, Licensing and Distribution

A Board Framework for Data Rights, Regulatory Perimeter, Trust Architecture, Partner Economics and Scalable Market Entry

Authored by Chennakeshav Adya, Independent Researcher

August 2026

Abstract

Open finance gives a customer or authorised business a controlled way to direct financial data to a permitted service and, in some regimes, to initiate a financial transaction. The commercial opportunity spans cash-flow intelligence, affordability, lending, payments, insurance, treasury, financial management and embedded distribution. The founder challenge is that customer value, regulatory permission, consent evidence, technical trust and partner economics must operate as one system. A product can be useful and still fail because its activity falls outside the selected licence, its consent cannot be proved or revoked, its data quality is weak, its regulated partner owns the economics, or its acquisition model depends on a fragile channel.

This paper develops a board-ready founder playbook for building on open finance. It begins with an activity, entity and jurisdiction map; separates data access, analytics, advice, intermediation and transaction initiation; and places each activity behind a legal and operational gate. It treats consent as a lifecycle covering purpose, data, party, duration, authentication, use, renewal, revocation, deletion, audit and dispute. It then connects the consent record to identity, API security, data provenance, service resilience and accountability.

The framework uses current official evidence across several markets. The Central Bank of the UAE's Open Finance Regulation establishes an API Hub, Trust Framework and Common Infrastructural Services. It requires an Open Finance Licence for relevant services unless a person is deemed licensed, and it subjects data sharing and service initiation to express user consent, authentication and secure communication. The CBUAE reported that Al Tareq went live in 2025, with central infrastructure operating and initial banks and third-party providers meeting operational requirements. Saudi Arabia has a formal Open Banking Framework and began licensing fintech companies for open banking services. The United Kingdom's Data (Use and Access) Act 2025 provides powers for Smart Data schemes, while the Financial Conduct Authority is developing a wider open-finance roadmap. India requires a standardised, auditable consent artefact under the Account Aggregator framework. Australia's Consumer Data Right uses accredited data recipients and consented transfers. European Union financial-data-access rules remain a proposal at the date of publication. In the United States, a court stayed the compliance dates of the federal Personal Financial Data Rights Rule in October 2025; founders should treat that timetable as unsettled.

The recommended programme runs through five gates: prove the customer job; confirm the regulatory perimeter; demonstrate consent and trust; validate distribution economics; and authorise market scale. Six original figures and six implementation tables support licensing, consent, funding, unit economics, cap-table choices, market entry and governance. Financial values, funnel metrics, scorecard weights and time estimates are illustrative management assumptions. Legal, regulatory, privacy, cybersecurity, accounting, tax, competition and valuation conclusions require confirmation by qualified advisers for the relevant entity, activity and jurisdiction.

JEL Classification: G21, G23, G28, L14, L51, L86, M13, O33

Keywords: open finance, open banking, consent, data portability, fintech licensing, API distribution, embedded finance, founder economics, UAE, GCC, United Kingdom, India, Australia

1. Build a regulated trust product

Open finance should be designed as a regulated trust product. The product promise depends on the customer understanding which data will move, who will receive it, what service will be delivered and how authority can be withdrawn. The technical promise depends on identity, authentication, authorisation, secure communication, data integrity and service availability. The commercial promise depends on measurable customer value, a viable channel and economics that survive partner fees, data costs, compliance and support.

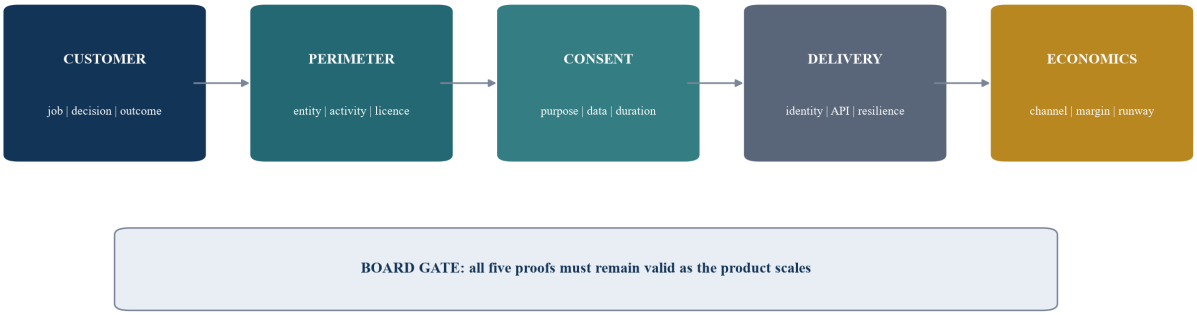
A founder should define the customer job before selecting an API or licence route. The job might be cash-flow forecasting for a small business, affordability evidence for a lender, account aggregation for a family office, payment initiation for a marketplace or renewal intelligence for an insurer. Each job should state the user, decision, required data, permissible use, output, frequency and accountable provider. This prevents the architecture from becoming a collection of data feeds without an operating decision.

The board should approve a product thesis with five linked proofs. Customer proof demonstrates a consequential problem and a valid decision enabled by the data. Perimeter proof maps every activity to the entity, country, licence, exemption or regulated partner. Consent proof demonstrates purpose, scope, authentication, renewal and revocation. Delivery proof demonstrates data quality, resilience, complaint handling and record retention. Economic proof demonstrates revenue, acquisition, partner cost, service cost, loss exposure and cash runway.

The CBUAE describes open finance as consent-driven, data-rich, collaborative, secure and customer-centric. Its framework includes data sharing and service initiation. That scope makes the founder's product definition a regulatory design input. The decision record should identify which component is a regulated financial service, which is a technical service, and which party makes the customer promise.

Figure 1. The open-finance trust product

BUILD THE SERVICE AS A REGULATED TRUST PRODUCT



Customer value, regulatory permission, consent, delivery and economics operate as one board-controlled system.

2. Map activities, entities and jurisdictions before building

The licensing perimeter follows activities performed by legal entities in particular jurisdictions. A product label such as financial wellness, underwriting intelligence or embedded treasury does not answer the perimeter question. The map should decompose the service into data collection, data sharing, account information, analytics, recommendations, arranging, lending, insurance distribution, payment initiation, custody, customer-money handling and outsourced technology.

For every activity, the founder should record the performing entity, customer location, data-holder location, regulated counterparty, contractual role and customer-facing representation. The map should show who receives the data, who determines the purpose, who makes a financial decision, who initiates a transaction, who handles a complaint and who bears liability. Cross-border delivery can create several connected perimeters.

The UAE Open Finance Regulation states that no juridical person may provide an Open Finance Service in the UAE without an Open Finance Licence unless it is deemed licensed. The application must identify whether the applicant seeks Data Sharing or Service Initiation permissions. The rulebook also defines a Technical Service Provider, yet a technology label does not establish that an activity falls outside licensing. Qualified UAE counsel should confirm the proposed structure.

Saudi Arabia's framework combines business rules, customer-experience guidelines, API specifications, operational guidelines, testing and certification. SAMA announced the start of licensing fintech companies to provide open banking services after the sandbox phase. In the United Kingdom, open-banking services and connected payments, credit, advice or insurance activities can engage different regulatory permissions. The founder should obtain written advice and, where appropriate, regulatory engagement before committing product architecture or launch dates.

Table 1. Activity and licensing-perimeter register

Activity	Evidence question	Potential regulated boundary	Board evidence
data access	whose financial data is accessed, under which authority and for what purpose?	open-finance or account-information permission, accreditation, recognised participant status or regulated-partner route	activity map, legal opinion, permission or partner agreement
analytics	does the product organise facts, determine eligibility, rank products or make a recommendation?	advice, credit, insurance, investment or consumer-protection boundary can arise from the output and presentation	model purpose, output samples, customer journey and legal analysis
service initiation	does the service cause a payment, transfer, order, placement, withdrawal or other transaction?	payment-initiation or wider open-finance licence can apply	transaction flow, authentication, liability map and permission
intermediation	does the founder introduce, arrange, negotiate or conclude a financial product?	credit, insurance, investment or payment intermediation can require separate authority	role description, agreements, disclosures and adviser confirmation
lending or underwriting	who decides, funds, prices, services and collects the credit?	lender, broker, servicer, credit-information and fair-treatment rules	credit policy, decision rights, funding agreement and customer terms
technical service	does the company provide infrastructure without controlling the regulated service or customer promise?	outsourcing and technology-risk duties can apply even when a separate licence is not required	responsibility matrix, service levels, audit rights and exit plan

Official rules establish the starting point; qualified advisers should confirm the exact entity, activity and jurisdiction.

3. Treat consent as a lifecycle

A consent screen is one moment in a longer control system. The lifecycle begins when the product explains the service, data, recipient, purpose and duration. It continues through identity verification, authentication, authority capture, data requests, usage, renewal, modification, revocation, deletion, complaints and audit. The consent record should be connected to every downstream use.

The CBUAE framework includes a Consent and Authorization Manager that supports the creation, management, enforcement and revocation of privacy directives. Its Open Finance Regulation requires express consent, appropriate authentication and secure communication. India provides a useful operational specification: the Account Aggregator Directions require a standardised consent artefact containing customer identity, requested financial information, purpose, recipients, notification address, creation and expiry details and the Account Aggregator's identity and signature. The framework also requires revocation functionality and an electronic artefact that can be logged, audited and verified.

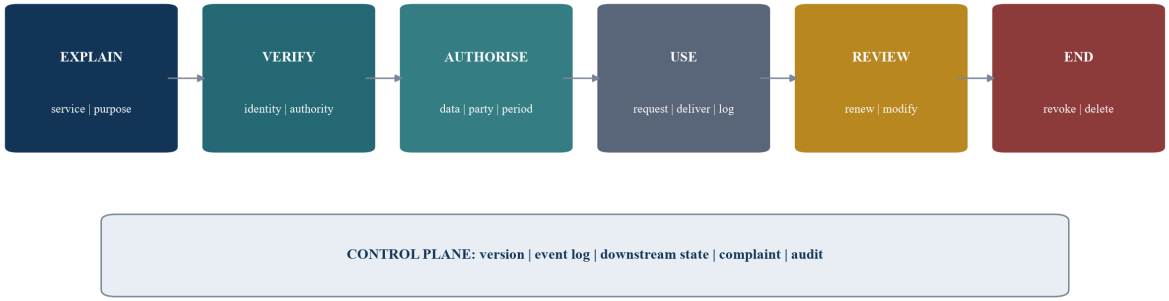
The founder should create a permission object rather than a static acceptance flag. The object should contain the user and authorising capacity, service, data categories, accounts or products, data holder, recipient, purpose, use frequency, start, expiry, authentication evidence and

jurisdiction. It should record every use, renewal, modification and revocation. Downstream processors should receive the current state and stop using data when authority ends, subject to any lawful retention duties confirmed by counsel.

Consent language should match the product operation. A purpose described as financial insights should not silently support unrelated marketing, model training or resale. Where another legal basis may apply under privacy law, the company should keep that analysis separate from the open-finance permission. The European Data Protection Supervisor has specifically warned against confusing proposed FiDA permission with GDPR consent.

Figure 2. Consent as an auditable lifecycle

MAKE AUTHORITY VISIBLE THROUGH THE FULL DATA JOURNEY



Every data use should resolve to current authority, stated purpose and an operational revocation path.

4. Engineer identity, authentication and authorisation

Identity answers who is acting. Authentication tests that claim. Authorisation determines what the verified person or organisation may approve. These controls must remain distinct, especially for businesses with directors, employees, delegates, advisers and changing signatory rights.

The product should define assurance requirements by action. Viewing a public product catalogue differs from sharing transaction data, adding a recipient, initiating a payment or changing a corporate mandate. Higher-risk actions may require stronger authentication, confirmation through the data holder, transaction-specific checks or another authorised person. The CBUAE Regulation requires reliable and effective authentication and, at minimum, two-factor authentication for relevant procedures, with additional measures in higher-risk circumstances.

Corporate customers require authority evidence. The company should determine whether the person can bind the entity, access each account and delegate authority. A single user login should not automatically establish organisational power. The process should capture role, legal entity, relevant account or product, authority source, expiry and changes. It should support removal when the person leaves or the mandate changes.

Authentication data should be minimised and protected. The founder should avoid collecting bank credentials when the regulated framework provides secure redirects or token-based methods.

India's Account Aggregator Directions state that the aggregator should not access a customer's authentication credentials for accounts with financial-information providers. The security design should include credential boundaries, certificate validation, token management, session controls, device and fraud signals, recovery, monitoring and tested incident response.

5. Connect consent to the data and API architecture

An open-finance platform needs traceability from customer authority to every API call and data object. The architecture should pass the current permission identifier, participant identity, purpose and scope into access-control decisions. It should reject expired, revoked, mismatched or over-broad requests and retain an immutable event record appropriate to legal requirements.

The CBUAE framework combines a participant directory, digital certificates, an API portal, sandbox, API Hub, consent manager, service assurance, reporting and case-resolution tools. The API aggregator is intended to provide a harmonised point of implementation for underlying interfaces. This creates an infrastructure foundation; each provider still needs controls for its application, purpose, customer journey, downstream processing and service obligations.

The founder should maintain a data contract for every element. It should define source, meaning, format, currency, timing, quality rule, permitted use, transformation, lineage and retention. Financial data can be missing, duplicated, delayed, reversed, categorised differently or supplied under changing account status. A decision service should show how it handles these states. Model outputs should distinguish verified source data from derived features and management assumptions.

Resilience should be designed around customer harm and decision criticality. The architecture should address unavailable data holders, delayed callbacks, partial datasets, revoked permissions, duplicate transactions, certificate expiry, schema changes and dependency failure. Service levels, retry logic, fallback communications and manual resolution should be agreed with partners. Security monitoring should cover participant identity, abnormal access, excessive scope, token misuse and data exfiltration.

The board evidence pack should include the architecture, data inventory, processor map, threat model, test results, incident plan, recovery objectives, dependency register and exit strategy. Independent testing should match the risk and regulatory expectations.

Table 2. Consent and trust-control register

Control	Required evidence	Operating metric	Failure response
purpose and scope	customer wording, structured permission object and product mapping	permissions by purpose, scope exceptions and renewal rate	stop unauthorised use, notify owner, investigate and remediate
identity and authority	verification method, organisational mandate and authentication record	verification failure, step-up rate and authority expiry	suspend affected action and re-establish authority
participant trust	directory status, certificate, permission and counterparty validation	certificate failures, unknown participants and rejected calls	block request, rotate or revoke credentials and escalate
data quality and lineage	source contract, transformation record, validation and reconciliation	completeness, freshness, duplicates, reversals and unresolved differences	qualify output, pause decision or obtain corrected source data
revocation and deletion	customer control, event propagation, downstream confirmation and retention rule	revocation completion time and unresolved downstream state	stop access, quarantine use, correct processors and document outcome
resilience and incident	dependency map, test, recovery plan, communications and complaint path	availability, latency, recovery time, incidents and customer harm	activate response, inform relevant parties and complete root-cause review

Control design should be confirmed against the current scheme, privacy law and regulated activity.

6. Decide where the product sits in the value chain

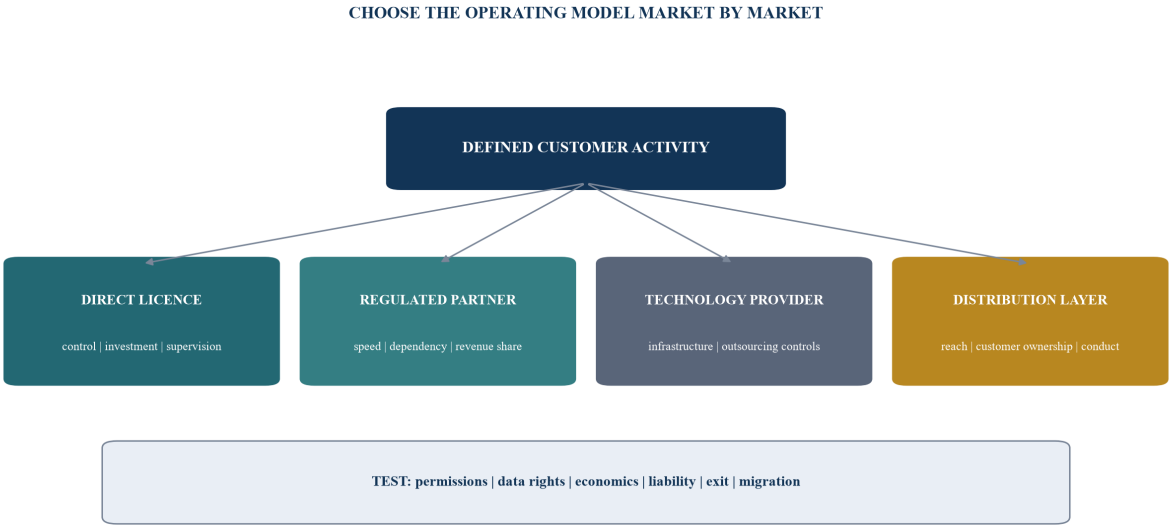
The founder can operate as a regulated open-finance provider, a technical service provider, an agent or distributor, a product layer supplied to a regulated institution, or a combination across markets. Each position changes control, capital, time to market, revenue share, liability, data rights and customer ownership.

A direct licence can support strategic control and a durable permission asset. It also requires governance, financial resources, regulatory engagement, compliance operations, security, reporting, audit and ongoing supervision. A regulated-partner route can accelerate access to customers and infrastructure. The partner may control approval, data access, pricing, onboarding, product change and termination. A white-label route can produce distribution while limiting the founder's visibility and data use.

The decision should be made service by service and market by market. The board should compare the rights needed to create customer value with the obligations and dependencies of each model. Contract review should cover regulatory roles, permitted data uses, intellectual property, model ownership, service levels, audit, subcontracting, complaints, customer communications, pricing, minimum commitments, liability, change control, termination and transition.

The founder should also decide who owns the consent relationship. If the regulated partner captures and controls the permission, the founder may be unable to reuse data, contact the customer or migrate the service. If the founder is the permissioned recipient, it may carry wider regulatory and privacy obligations. The product architecture and valuation case should reflect the enforceable contract, rather than an assumed customer relationship.

Figure 3. Licensing and operating-model decision map



The route is selected by activity, control requirement, capability, partner dependency and market evidence.

7. Design distribution around a consequential workflow

Open-finance distribution becomes stronger when the service sits inside a recurring, consequential workflow. Examples include daily treasury, monthly close, credit application, supplier payment, insurance renewal, investment reporting or household financial planning. A workflow creates a reason to connect data, return, act and pay.

The founder should define the trigger, decision, user, cadence, evidence and outcome for each channel. A bank channel may provide trusted access and a large installed base, while involving procurement, integration, risk review and shared economics. An accounting-platform channel can reach small businesses at a point of verified financial activity. A marketplace can connect payment or credit services to a transaction. An adviser channel can add interpretation but requires authority, suitability and conduct analysis where regulated advice arises.

Distribution agreements should align incentives with customer outcomes. Revenue based solely on approvals or transaction volume may encourage weak targeting. The model can include platform fees, usage, verified savings, service tiers or shared economics, subject to legal and conduct review. The company should disclose material commercial relationships where required and prevent the ranking or recommendation logic from being distorted by payment.

Channel concentration belongs in the board risk register. One partner can become the source of customers, data, permission, identity, payments and revenue. The founder should test termination, pricing changes, delayed approvals, product restrictions and migration. Direct customer understanding, portable product evidence and more than one viable channel can improve resilience, where contracts and regulation permit.

The distribution plan should track activation through verified outcomes. Measures can include eligible users, permission completion, valid data coverage, decision completion, customer action, retained use, paid conversion and service cost. A high connection count without recurring value is not distribution proof.

Table 3. Distribution-model economics and control

Channel	Value offered	Core dependency	Economic test	Control question
bank or insurer	customer utility, retention, data-enabled decision or embedded service	procurement, integration, regulated approval and installed-base access	contracted fee or revenue share less integration, service and support	who controls customer, consent, product change and termination?
accounting or ERP platform	cash-flow, lending, payments or reconciliation in an operating workflow	platform APIs, data rights and user adoption	active paying entities less platform and support cost	can the founder evidence purpose and authority across both platforms?
marketplace or vertical SaaS	financing or payment at a transaction point	transaction data, merchant quality and partner funding	contribution per completed service net of losses and partner share	does the customer understand each party and total product cost?
adviser or professional network	interpreted intelligence and implementation support	adviser authority, training and conduct	revenue per active relationship less enablement and review	does the output cross into regulated advice or intermediation?
direct digital	product control, customer learning and brand	acquisition cost, trust, onboarding and service operations	lifetime contribution relative to acquisition and cash payback	can the company acquire customers without unsupported claims or dark patterns?
public or ecosystem infrastructure	broad participation and standard access	eligibility, certification, policy and scheme economics	adoption and service margin after compliance and infrastructure cost	are scheme changes, fees and recertification included in the plan?

Commercial terms and metrics are illustrative categories; the operating model should use executed contracts and verified performance.

8. Build unit economics from permission to paid outcome

Unit economics should follow the customer journey. Begin with eligible users or businesses, then measure permission initiation, completed authentication, valid data connection, usable data coverage, completed decision, customer action, paid conversion, retained use and support. Each transition has a cost and a failure reason.

Revenue should be tied to an enforceable event: subscription period, verified transaction, platform licence, usage or contracted service. Partner shares, API charges, scheme fees, payment costs, fraud, losses, customer support, disputes, compliance review, cloud, model operations and data remediation belong in contribution margin. Integration and regulatory costs can create a long payback even when gross software margins appear high.

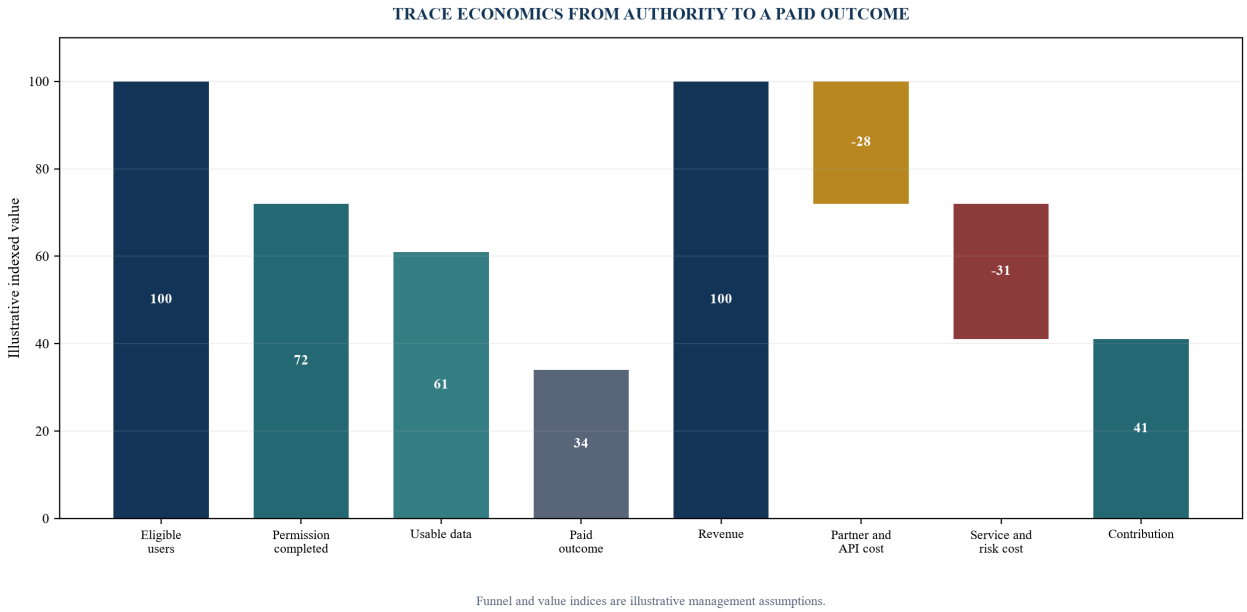
The founder should separate data availability from decision value. More accounts or attributes can raise complexity without increasing the customer's outcome. The product team should identify the minimum reliable data set for each decision, then test whether additional data improves accuracy, speed, inclusion or economics. Any automated decision should have an evidence, fairness and challenge framework appropriate to the activity and jurisdiction.

Pricing should reflect the customer value and responsible risk allocation. A lender may pay for verified affordability or cash-flow insight. A small business may pay for time saved, avoided fees or better liquidity visibility. A platform may pay for retention or transaction uplift. Management

should avoid valuing unproven data exhaust or future cross-sell as current revenue.

The board should review a cohort bridge. The bridge should compare actual permission completion, valid data, service use, revenue, partner cost and support by source and market. The illustrative values in Figure 4 demonstrate the method only. The company forecast should use observed cohorts and approved assumptions.

Figure 4. Permission-to-contribution unit economics



Indexed values are illustrative management assumptions; company decisions require verified cohorts and executed commercial terms.

9. Price regulatory, data and partner dependencies into the plan

The cost base should include the work required to remain permitted and reliable. Licensing or accreditation can require legal advice, application work, governance, financial resources, fit-and-proper assessments, compliance staff, policies, audit, reporting, insurance, cybersecurity, testing and annual maintenance. Product changes can trigger notification, approval or recertification.

Partner cost should be modelled as more than a revenue share. Integration, onboarding, due diligence, security review, minimum commitments, scheme fees, customer support, disputes and change requests can consume founder cash. The agreement may allow the partner to change price, suspend access or require rework. Management should run base, downside and termination scenarios.

Data quality has an economic cost. Missing accounts, inconsistent descriptors, delayed updates and changed schemas can create manual review, poor decisions, customer complaints and model drift. The forecast should include observability, reconciliation, exception resolution and support. Service architecture should identify which data defects are detected, disclosed, repaired or routed to the source.

Regulatory capital and safeguarding obligations should be assessed where the selected activity requires them. Founders should keep operating runway separate from restricted capital or customer-money arrangements. A fundraising plan that treats all cash as freely deployable can

overstate execution capacity.

10. Sequence funding around evidence gates

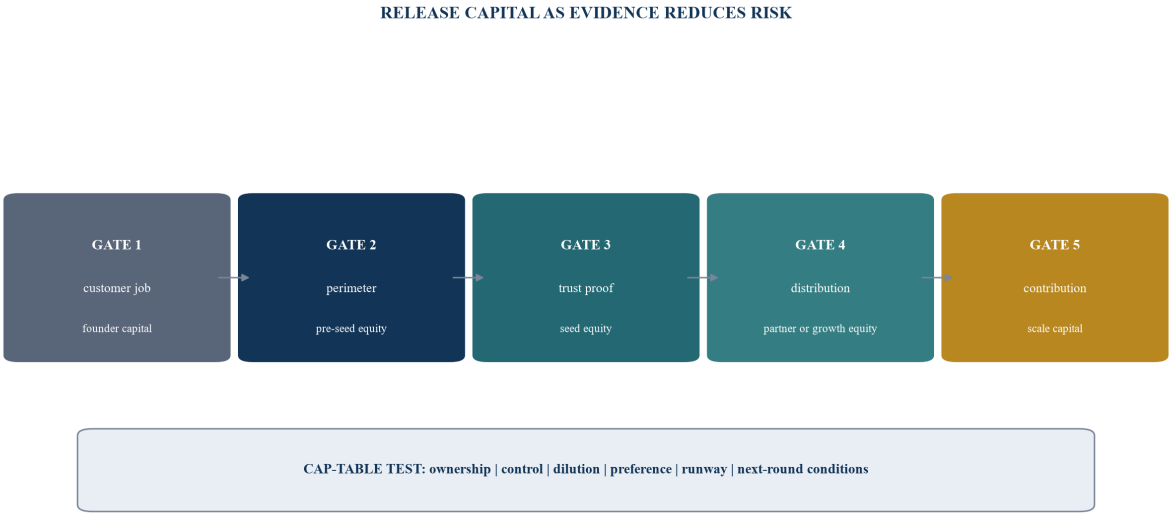
Open-finance companies can consume substantial capital before scaled revenue. The funding roadmap should connect each capital tranche to evidence that reduces product, regulatory, technical, distribution and economic risk. A larger round without clearer gates can fund parallel dependencies that remain unresolved.

The first gate proves the customer workflow and willingness to engage. Evidence can include observed processes, authorised design partners and a defined outcome. The second gate confirms perimeter advice, entity design and regulator or scheme path. The third gate proves consent, authentication, data quality, security and conformance in a controlled environment. The fourth gate proves distribution through an executed partner or a repeatable direct cohort. The fifth gate proves contribution, service reliability and governance before wider scaling.

Funding instruments should match uncertainty and negotiating position. Equity absorbs product and market risk and affects founder ownership. A convertible or similar instrument can delay price while creating discount, cap, interest, maturity and control implications. Venture debt can extend runway where revenue visibility and equity support can service its fixed obligations. Partner funding or implementation fees can validate demand while introducing exclusivity, roadmap or pricing rights. Qualified legal, tax and financial advisers should confirm the terms.

The board should maintain a use-of-funds bridge by gate. Regulatory, security and integration work should have named deliverables, acceptance evidence and decision dates. Hiring should follow the capability needed for the next gate. Management should keep downside runway and avoid treating unsigned pipeline as available cash.

Figure 5. Funding and cap-table choices through evidence gates



Percentages and timing are illustrative management assumptions; financing terms require company-specific modelling and advice.

11. Govern cap-table and investor rights as operating constraints

The cap table influences the founder's ability to navigate licensing, partner negotiations and later funding. Ownership should be modelled on a fully diluted basis, including issued shares, options, warrants and convertible instruments under their possible conversion terms. Management should show the effect of caps, discounts, interest, option-pool increases and future rounds.

Strategic investors can add distribution, data, regulatory credibility or infrastructure. Their rights can also limit partnerships with competitors, product scope, geographic expansion or exit. The company should value only enforceable contributions and model exclusivity, most-favoured terms, data rights, roadmap control and termination.

Table 4. Funding and cap-table decision register

Decision	Evidence required	Value question	Risk question
instrument	priced equity, convertible, venture debt or partner funding terms	which risk is funded and what milestone becomes possible?	what fixed, conversion, security or control obligation is created?
dilution	current and fully diluted cap table under base and downside cases	is founder and employee ownership aligned with the execution plan?	do caps, discounts, pools or future rounds produce unexpected outcomes?
governance	board seats, observer rights, information and reserved matters	does the investor improve decision quality and access?	can rights delay product, licence, financing, partnership or exit decisions?
regulated ownership	controller thresholds, fit-and-proper evidence and notifications	can the structure support permission and later capital?	which investor or transfer requires regulatory review or approval?
strategic rights	distribution, data, integration, exclusivity and roadmap commitments	is the strategic value enforceable and measurable?	does concentration restrict other channels, products or acquirers?
runway	gate-based use of funds, downside case and restricted cash	is capital released against evidence and accountable delivery?	does the company have cash to remediate delay, recertification or partner loss?

Terms are evaluated as operating and regulatory constraints, with specialist confirmation where required.

12. Enter markets through a comparability map

Open-finance regimes should not be treated as interchangeable. The founder should compare scope, participant model, licensing or accreditation, consent, authentication, infrastructure, data sets, initiation rights, commercial access, liability, privacy and implementation status. The product can then use a common control core with market-specific rules.

The UAE provides a central framework that includes a Trust Framework, API Hub and Common Infrastructural Services. The CBUAE reported that Al Tareq went live in 2025, with payment initiation, e-KYC, payment-token services, standardised consent journeys, Confirmation of Payee, data-sharing APIs and insurance-quote services among the functionality described. The exact products, participant access and rollout stage should be verified with current official materials and counterparties.

Saudi Arabia operates an Open Banking Framework with formal business and technical standards, testing and certification. The United Kingdom has a mature open-banking base and a 2025 Act providing powers for Smart Data schemes; the FCA's open-finance work extends the policy direction beyond payment accounts. India has a licensed Account Aggregator model with a detailed consent artefact and restrictions on the aggregator's handling of data and credentials. Australia uses the Consumer Data Right, including accredited data recipients and authorised representatives.

The European Commission proposed FiDA to extend customer-directed access across wider financial data and introduce permission dashboards and financial-data-sharing schemes. The proposal's final legal form and timing should be checked before reliance. The U.S. federal rule is also unsettled: the CFPB states that a court stayed compliance dates in October 2025 while reconsideration work continued.

Market priority should follow a scored evidence case: customer workflow, accessible data, permissible operating model, qualified partner, implementation readiness, revenue, acquisition, service cost and capital. Market size alone is insufficient.

Table 5. Multi-market entry map

Market	Official framework position	Founder design implication	Launch gate
United Arab Emirates	CBUAE Open Finance Regulation in force; Al Tareq reported live in 2025	map Data Sharing, Service Initiation, deemed-licensed and technical-service roles; integrate Trust Framework and consent requirements	written perimeter advice, applicable permission, scheme access, conformance and partner readiness
Saudi Arabia	SAMA Open Banking Framework with business rules, technical standards, lab and licensing pathway	align use case, customer journey, certification, data privacy and licensed participant model	regulatory route, lab or certification evidence, operating partner and production approval
United Kingdom	regulated open banking with wider Smart Data powers under the Data (Use and Access) Act 2025	map payment, data, credit, advice and conduct permissions; monitor open-finance implementation	FCA perimeter, permission or partner route, Consumer Duty analysis and interface readiness
India	RBI Account Aggregator framework with standardised consent artefact and licensed NBFC-AA role	separate Account Aggregator, financial-information provider and financial-information user responsibilities	valid participant status or agreements, consent architecture, permitted data use and security readiness
Australia	Consumer Data Right with accredited data recipients and authorised representatives	select accreditation or sponsorship route; implement CDR consent, data and information-security rules	approved participation route, consumer-data controls, conformance and operating evidence
European Union	FiDA remained a legislative proposal at publication	avoid assuming proposal provisions are effective; monitor final scope, permission dashboards, schemes and licensing	current legal-status confirmation, PSD and sector permissions, GDPR basis and market-specific readiness
United States	CFPB states federal rule compliance dates were stayed by court in October 2025	treat federal timetable as unsettled and map state, bank, contract and consumer-protection requirements	current counsel opinion, partner authority, data-rights basis and change-monitoring plan

This table records official framework status at publication; the founder must reverify rules, effective dates and approvals before launch.

13. Productise privacy, data minimisation and customer control

Privacy should be expressed in product choices. The service should request the minimum data required for a stated decision, retain it for a defined period and give the customer usable control. Additional data can be requested when a new purpose is explained and authorised. Internal convenience is not a customer purpose.

The product team should maintain a data inventory that links every element to purpose, source, legal analysis, recipient, model feature, retention, deletion and customer communication. Sensitive attributes and derived inferences require particular review. Model training, product research, marketing and partner reporting should be analysed separately from delivering the requested service.

Customer dashboards should show active permissions, recipients, data categories, purpose, last access, expiry and revocation. The product should explain the effect of withdrawal, including which future service stops and which records may remain under applicable legal duties. Revocation should propagate to processors and partners, with exceptions investigated.

The UAE's open-finance infrastructure expressly includes centralised consent management. India's directions require consent attributes, revocation and auditability. The proposed EU FiDA framework uses permission dashboards, while the EDPS has stressed clarity around permission, data minimisation and data-protection legal bases. These examples support a product pattern: visible authority, limited use and operational control.

The board should receive privacy and consent measures alongside commercial metrics. Examples include scope per use case, permission completion, revoked permissions, downstream confirmation time, unauthorised-access events, retention exceptions, complaints and remediation. High conversion obtained through confusing design creates legal and trust exposure.

14. Establish data, model and decision accountability

Open-finance data often feeds scores, forecasts, recommendations and automated actions. The company should document how source data becomes a decision. The record should identify the data set, transformation, feature, model or rule, output, user, action and accountable owner. It should distinguish customer facts, third-party data, derived values and management assumptions.

Data quality controls should test completeness, freshness, reconciliation, duplicate handling, reversals and currency. A missing current account can distort affordability. A delayed transaction can distort cash flow. A category error can distort a financial-wellness recommendation. The product should qualify or stop an output when evidence falls below the approved threshold.

Model governance should match consequence. The company should define intended use, prohibited use, training and validation data, performance, stability, bias or exclusion risks, human review, monitoring, challenge and change control. An open-finance permission does not by itself authorise every use of the data or establish that an automated decision is fair.

Customer explanations should be designed for the action. A forecast can show source dates and uncertainty. A credit recommendation can identify principal factors and a review path where required. A payment instruction should show amount, recipient and authority before confirmation. Complaint and correction processes should reach the data or decision owner.

The board should review model performance with commercial outcomes and customer harm. Approval rate, revenue or engagement should be accompanied by data coverage, error, overrides, complaints, adverse outcomes and remediation. Material changes should revisit perimeter, consent and partner approval.

15. Contract the ecosystem for accountability and exit

Open finance is delivered through an ecosystem of data holders, schemes, identity providers, cloud services, regulated institutions, analytics providers and distributors. Contracts should reflect the actual flow of authority, data, service and money.

The responsibility matrix should identify the customer promise, permission capture, authentication, API operation, data quality, decision, transaction, complaint, refund, incident,

regulatory report and record. Each responsibility should have an evidence source and escalation. Ambiguous ownership is especially dangerous where a customer sees one interface but several institutions perform the service.

Exit should be designed before dependency becomes material. The plan should address customer communication, active permissions, data return or deletion, transition assistance, credentials, models, outstanding transactions, disputes, regulatory notice and continuity. The founder should know whether it can migrate customers and data to another partner under consent, contract and law.

The board should test a severe partner scenario. The scenario can assume immediate suspension, data interruption, pricing change, licence issue or acquisition by a competitor. Management should show customer impact, obligations, cash effect, alternative capacity and decision rights. The scenario values resilience before the company becomes dependent.

Table 6. Board governance and launch checklist

Gate	Required evidence	Accountable owner	Board decision
customer value	defined workflow, authorised design evidence, outcome measure and customer communication	product and commercial leaders	approve use case, segment and success measure
regulatory perimeter	activity-entity-jurisdiction map, legal advice, permission or partner structure and change triggers	CEO, compliance and legal advisers	approve structure and conditions before build commitment
consent and trust	permission object, identity and authentication, API security, data lineage, revocation, incident and complaint tests	technology, security, data and compliance leaders	approve controlled production subject to evidence thresholds
distribution	executed agreement, customer ownership, rights, partner service, concentration and exit plan	commercial and operating leaders	approve channel release, exposure limit and fallback
economics and funding	observed funnel, contribution bridge, gate-based use of funds, cap table and downside runway	CFO and CEO	approve capital tranche, hiring and next evidence gate
market launch	current framework status, local controls, conformance, partner readiness and customer support	country and programme owners	approve launch scope, stop rules and review date
scale	retained outcomes, service reliability, complaints, model performance, contribution and governance capacity	board sponsor and executive committee	continue, remediate, limit or stop scaling

Each gate requires current evidence and a named owner; unresolved legal conclusions remain with qualified advisers.

16. Run a 120-day founder programme through five gates

Days one to twenty establish customer and perimeter evidence. The team defines the workflow, customer outcome, entities, activities, jurisdictions and partners. It obtains written legal advice for the proposed structure, opens required regulatory or scheme engagement and identifies data and permission requirements. Gate one approves a specific use case and valid path to operation.

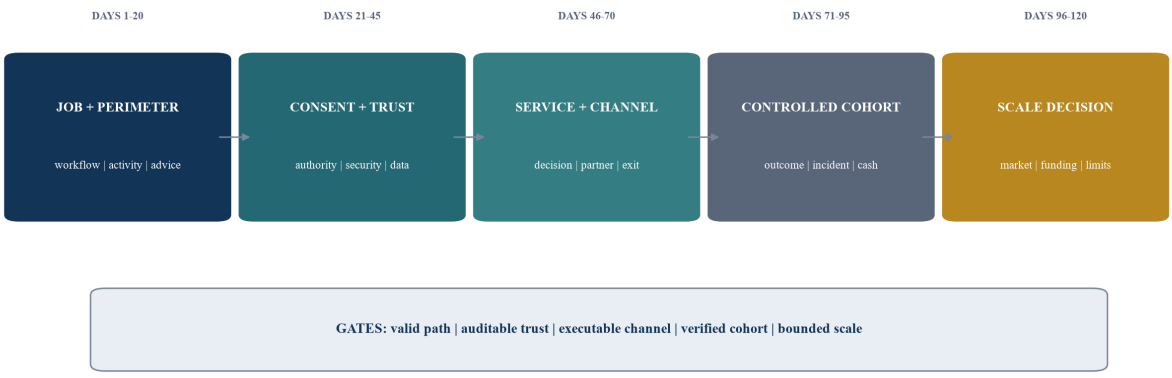
Days twenty-one to forty-five build the consent and trust design. Product, legal, compliance, security and data teams create the permission object, customer journey, authentication, API architecture, data contracts, threat model, incident plan and processor map. The team tests revocation and downstream state. Gate two requires an auditable journey and closed critical security findings.

Days forty-six to seventy prove the service and distribution route. The founder integrates controlled data, validates quality, tests the decision, documents model governance, configures complaints and agrees partner responsibilities. Commercial teams negotiate customer ownership, economics, service, change and exit. Gate three requires completed testing and an executable route to users.

Days seventy-one to ninety-five run a controlled cohort. The company measures permission completion, valid data, decision completion, outcomes, support, incidents and partner service. Financial reporting reconciles revenue, partner cost, service cost and cash. Gate four authorises remediation or a bounded expansion.

Days ninety-six to one hundred and twenty prepare scale. The board reviews market status, permission, conformance, operating capacity, funding, cap table, downside runway, partner concentration, retained outcomes and contribution. Gate five authorises a market and cohort limit with stop rules.

Figure 6. The 120-day open-finance launch roadmap



Each phase ends with evidence that the board can approve, qualify or return for remediation.

17. Measure trust, outcomes and contribution together

The scorecard should connect permission, service, customer outcome, risk and cash. A commercial dashboard alone can reward activity that creates weak consent, service incidents or unprofitable support. A compliance dashboard alone can miss whether the product solves a valuable problem. The board needs one reconciled view.

Trust measures can include permission completion, scope, renewal, revocation, authentication failure, unauthorised requests, customer complaints and incident recovery. Delivery measures can include valid data coverage, freshness, latency, decision completion, uptime and partner performance. Outcome measures should reflect the stated job, such as forecast accuracy, time saved, avoided failure, improved cash visibility or completed transaction.

Commercial measures should follow cohorts. The company should track eligible users, activated permissions, paid outcomes, retention, revenue, partner share, service cost, support, loss and acquisition. Cash measures should show collections, partner settlements, restricted cash, regulatory investment and runway. Forecast-to-actual differences should update funding decisions.

Stop rules should be approved before scale. Examples can include unresolved unauthorised access, material customer harm, failure to propagate revocation, loss of permission or partner authority, unacceptable service interruption, model failure, adverse complaint pattern or cash runway below the approved threshold. Exact thresholds are company-specific management decisions.

18. Make the board decision explicit

The final board pack should contain the customer workflow, activity and entity map, written perimeter advice, licensing or partner path, consent journey, data and API architecture, security evidence, model documentation, partner contracts, market-entry map, unit economics, cap table, funding plan, risk register, operating scorecard and 120-day record. Each item should identify its owner, date, source and unresolved matter.

The board should approve a bounded decision. It can authorise one service, entity, market, partner, customer cohort and capital tranche. Conditions should state required permission, scheme or partner acceptance, security closure, complaint capacity, service level, contribution evidence and review date. Expansion should require the next evidence gate.

Management should document what remains uncertain. A pending regulation, court stay, partner procurement process, licence application, customer forecast or fundraising scenario should be presented with its current status and consequence. The company should avoid presenting a planned permission, proposed partnership or forecast conversion as achieved.

The board should also approve accountability. Named executives should own the customer promise, regulatory perimeter, consent, security, data quality, model, partner, complaints, economics and cash. A change in product use, data, entity, market, transaction rights or distribution should trigger reassessment.

Open finance can become a valuable distribution and decision infrastructure when authority, data and economics remain aligned. The founder's advantage comes from solving a consequential

workflow with reliable evidence, inside a structure that customers, partners, regulators and investors can understand.

Implementation conclusion

The founder playbook begins with a customer decision and maps every activity to the entity, permission and jurisdiction that performs it. It converts consent into an auditable lifecycle, connects authority to API and data controls, and makes partner roles and exit rights explicit.

Commercial scale follows verified outcomes. Distribution should sit inside a recurring workflow, unit economics should run from permission to paid contribution, and funding should be released against evidence gates. Market entry should reflect current official regimes and their different implementation states.

The 120-day programme gives the board five decisions: validate the customer job and perimeter; approve consent and trust; accept an executable service and channel; verify a controlled cohort; and authorise bounded scale. Financial values, scorecard thresholds and timing remain illustrative management assumptions until supported by company evidence and approved decisions.

References

[1] - Central Bank of the UAE. Open Finance.
https://www.centralbank.ae/en/our-operations/fintech-digital-transformation/open-finance/

[2] - Central Bank of the UAE Rulebook. Open Finance Regulation.
https://rulebook.centralbank.ae/en/rulebook/open-finance-regulation

[3] - Central Bank of the UAE Rulebook. Introduction and Scope, Open Finance Regulation.
https://rulebook.centralbank.ae/en/rulebook/introduction-and-scope-2

[4] - Central Bank of the UAE Rulebook. Schedule 1, Details of the Open Finance Framework.
https://rulebook.centralbank.ae/en/rulebook/schedule-1-%E2%80%93-details-open-finance-framework-0

[5] - Central Bank of the UAE. Annual Report 2025.
https://www.centralbank.ae/media/4qbn11cl/annual-report-2025-en.pdf

[6] - Central Bank of the UAE. CBUAE Issues the Open Finance Regulation, 27 June 2024.
https://www.centralbank.ae/media/rxfeelkt/cbuaei-2.pdf

[7] - United Arab Emirates Legislation. Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data. https://uaelegislation.gov.ae/en/legislations/1972

[8] - Saudi Central Bank. Open Banking in Saudi Arabia. https://www.openbanking.sama.gov.sa/index-en.html

[9] - Saudi Central Bank. SAMA Commences Licensing of Fintech Companies to Provide Open Banking Services. https://sama.gov.sa/en-US/MediaCenter/News/pages/news-1135.aspx

[10] - Saudi Central Bank Rulebook. Article 95, Payment Service Provider access and open banking.
https://rulebook.sama.gov.sa/en/article-95-1

[11] - UK Government. Data (Use and Access) Act 2025.
https://www.gov.uk/government/collections/data-use-and-access-act-2025

[12] - UK Legislation. Data (Use and Access) Act 2025, Explanatory Notes.
https://www.legislation.gov.uk/ukpga/2025/18/notes/division/4/index.htm

[13] - Financial Conduct Authority. Open Banking and Open Finance.
https://www.fca.org.uk/firms/open-banking-open-finance

[14] - Financial Conduct Authority. PS22/9, A New Consumer Duty.
https://www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty

[15] - Reserve Bank of India. Master Direction, Non-Banking Financial Company - Account Aggregator Directions, 2016, updated 6 September 2024. https://systemhealth.rbi.org.in/Scripts/BS_ViewMasDirections.aspx_id%3D10598%281%29.html

[16] - Australian Competition and Consumer Commission. The Consumer Data Right. https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right

[17] - Australian Competition and Consumer Commission. Competition and Consumer, Consumer Data Right Rules 2020. https://www.accc.gov.au/system/files/CDR%20Rules%20-%20Final%20-%206%20February%202020.pdf

[18] - European Commission. Proposal for a Regulation on a Framework for Financial Data Access, COM(2023) 360 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A0360%3AFIN

[19] - European Data Protection Supervisor. Opinion on the Proposal for a Regulation on a Framework for Financial Data Access. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52023XX01054

[20] - Consumer Financial Protection Bureau. Personal Financial Data Rights. https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/personal-financial-data-rights/

[21] - Consumer Financial Protection Bureau. 12 CFR Part 1033, Personal Financial Data Rights. https://www.consumerfinance.gov/rules-policy/regulations/1033/

[22] - Bank for International Settlements. API Standards for Data-Sharing. https://www.bis.org/publ/bppdf/bispap132.htm

[23] - World Bank. Financial Consumer Protection. https://www.worldbank.org/en/topic/financialinclusion/brief/financial-consumer-protection

About the Author

Authored by Chennakeshav Adya, Independent Researcher