# Arabic Data, Regional Reach: Valuing GCC FinTech AI Acquisitions

*A Valuation and Transaction Framework for Language Assets, Regulatory Access, Local Distribution, Model Governance and Scalable Regional Economics*

**Authored by Chennakeshav Adya**

Independent Researcher

September 2026

---

## Abstract

*Gulf financial technology businesses can create value by combining Arabic-language interaction, regional customer data, local banking infrastructure, regulatory permissions and distribution relationships. Artificial intelligence can support onboarding, customer service, fraud detection, credit, compliance, advice, collections and payments. The strategic attraction is clear: a buyer may acquire faster regional reach and a product adapted to local language and operating conditions. The valuation problem is harder. Arabic capability can be shallow, data rights can be narrow, regulatory access can be entity-specific, bank connections can require consent, and apparent local advantage can disappear during integration.*

*This paper develops a valuation and transaction framework for acquisitions of GCC fintech platforms using artificial intelligence. It separates language interface from decision quality, data possession from transferable rights, regulatory licence from usable product permission, and customer access from durable distribution. It connects Arabic-language performance, consent, data provenance, open-finance access, model governance, human accountability, cybersecurity, customer outcomes, cohort economics and integration readiness to enterprise value.*

*The analysis draws on current material from the Central Bank of the United Arab Emirates, Saudi Central Bank, financial free-zone regulators, regional data-protection authorities, the Bank for International Settlements, Basel Committee, Financial Stability Board, IOSCO, standards organisations and accounting and valuation bodies.[1][2][3][4][5][6][7][8][9][10] The sources show expanding open-finance and digital infrastructure alongside continuing requirements for consent, licensing, security, consumer protection, operational resilience and accountable use of AI.*

*A hypothetical acquisition illustrates a platform serving 420,000 active users across three GCC markets, with USD 24.0 million of annual revenue. Every user number, accuracy measure, conversion rate, cost, multiple, probability and valuation amount is a management assumption created solely to demonstrate the method. None is a forecast, market benchmark or valuation opinion.*

*The paper concludes that a buyer should pay for Arabic data and regional reach only when the target proves lawful and transferable data, material Arabic decision performance, valid permissions, durable bank and distribution access, monitored customer outcomes and contribution after localisation, compliance, model, security and integration cost. Six figures and seven tables convert this conclusion into a diligence plan, language-performance framework, model-governance test, unit-economic bridge, valuation method, transaction protections and a 180-day programme.*

*Financial-services, payments, credit, data, artificial-intelligence, competition, tax and corporate-law requirements vary by jurisdiction and activity. Qualified specialists should determine the rules and permissions applicable to a specific transaction or operating model.*

*JEL Classification: G21, G24, G34, L86, O33*

*Keywords: fintech, artificial intelligence, Arabic data, GCC, open finance, valuation, mergers and acquisitions, model governance*

**JEL Classification:** G21, G24, G34, L86, O33

**Keywords:** fintech, artificial intelligence, Arabic data, GCC, open finance, valuation, mergers and acquisitions, model governance

## 1. Define the acquisition decision

The investment question is whether local language, data, permissions and distribution produce transferable and collected economics. A target may demonstrate an Arabic interface, a large user base and relationships with banks. Those facts do not establish that the model performs well across dialects and financial tasks, that the buyer can lawfully use historical data, that regulated activity can continue after closing or that regional expansion will preserve unit economics.

The board should define the product perimeter before debating a revenue multiple. The target may provide information, account aggregation, payment initiation, lending, insurance distribution, investment functionality, fraud controls or regulated advice. One application can cross several regulatory perimeters. Arabic-language interaction can support the service while the economic and legal character follows the underlying financial activity.

The acquisition thesis should be written as a testable chain. Local data and language capability should improve understanding or decision performance. Improved performance should increase conversion, lower service cost, reduce loss or improve customer outcomes. Those results should reconcile to collected contribution after data, model, localisation, compliance, support, fraud and security costs. Diligence should identify evidence capable of disproving every link.

Value should be divided into collected stand-alone contribution, protected value dependent on transferable rights and permissions, funded improvement value, buyer-specific synergy and unproven option value. Expansion into another GCC market or regulated product should remain outside the central case until evidence supports permission, distribution and operating readiness.

### Investment-committee evidence pack

The investment committee should receive one reconciled evidence pack defining legal entities, licences, products, markets, users, data sets, language variants, models, bank connections, partners, revenue, direct cost, losses, complaints and vendors using consistent dates and populations. Each valuation assumption should have an owner, source and falsification test.

Sampling should combine random selection with Arabic-first users, dialect groups, code-switched interactions, vulnerable customers, high-value transactions, model overrides, complaints and failed journeys. The buyer should trace consent, input, model version, recommendation or decision, human action, customer communication, regulated outcome and cash.

The decision paper should identify what survives change of control. Customer terms, data rights, licences, bank consents, API credentials, model licences, cloud contracts and distribution agreements can determine continuity. Historical performance does not prove that the buyer obtains the same lawful operating position.

## 2. Separate four sources of regional advantage

Arabic capability is one potential advantage. A second is regulatory access through an authorised entity. A third is technical access to banks, payment systems and open-finance infrastructure. A fourth is

distribution through merchants, employers, government platforms, banks or consumer channels. These assets should be tested and valued separately.

Language capability ranges from translated labels to reliable understanding and generation across dialect, script, financial terminology and customer context. A polished interface can rely on English-centred decision logic. The buyer should test whether Arabic inputs change only presentation or materially support classification, risk, compliance and service outcomes.

Regulatory access is activity- and entity-specific. The UAE Open Finance Regulation creates licensing categories for data sharing and service initiation, while additional regulated activities require their own permissions.[1][2] Saudi Arabia moved from sandbox development to licensing open-banking providers in 2026.[4] A licence is valuable when it covers the product, customer and geography and can continue through the transaction.

Technical access depends on certified interfaces, consent journeys, security and operating relationships. Distribution depends on customer trust and counterparty contracts. A buyer should avoid paying twice when one claimed moat is merely a consequence of another temporary relationship.

**Table 1. Regional-advantage diligence matrix**

| Advantage | Required evidence | Durability test | Principal valuation exposure |
|---|---|---|---|
| Arabic interaction | task-level performance by dialect and channel | stable outcomes after product and model change | shallow localisation |
| local data | provenance, consent, purpose and quality | lawful transfer and continued use | stranded corpus |
| regulatory access | licence, permission and correspondence | change-of-control and product perimeter | delayed or restricted operation |
| bank connectivity | certified API and service evidence | consent, credential and partner continuity | expensive reconnection |
| distribution | active contract and customer economics | assignment, concentration and renewal | channel dependence |
| operating knowledge | documented people, process and controls | retention and repeatability | key-person risk |

*Proposed framework; legal conclusions remain activity- and jurisdiction-specific.*

## 3. Reconstruct the Arabic-data evidence chain

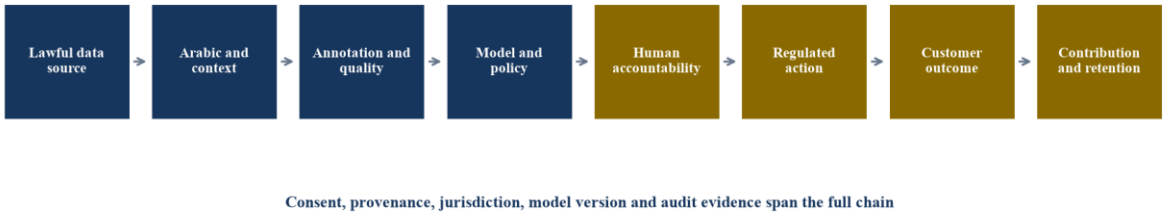
An Arabic data asset is an evidence chain rather than a file count. It begins with a lawful source and recorded purpose. It preserves language, dialect, script, channel, timestamp, product, jurisdiction and customer context. It connects annotation, quality control, model feature, output, human review, regulated action, customer outcome and retention or cash.

The chain should distinguish original Arabic, translated Arabic, transliteration and code-switched content. Modern Gulf interactions can combine Arabic and English, Latin-script Arabic, numbers, abbreviations and product names. Normalisation can improve model performance and remove information. The buyer should inspect both raw and transformed records and verify that provenance survives.

Consent and purpose are central. The UAE framework makes data sharing and transaction initiation subject to express user consent, authentication and secure communication.[1] Saudi open banking similarly centres secure customer-directed sharing.[4][5] Permission to deliver a service does not automatically establish permission to train a model, combine data sets or transfer historical data to an acquirer.

The buyer should reconstruct representative records from collection to outcome. It should test common and edge cases: formal Arabic, Gulf dialects, spelling variation, low-quality scans, voice transcription, right-to-left display, code-switching, ambiguous names and culturally specific expressions. Missing and rejected records belong in the population.

**Figure 1. Proposed Arabic-data-to-value evidence chain**




*The chain separates lawful acquisition, language quality, decision use, accountable action and realised value.*

## 4. Test language performance by economic task

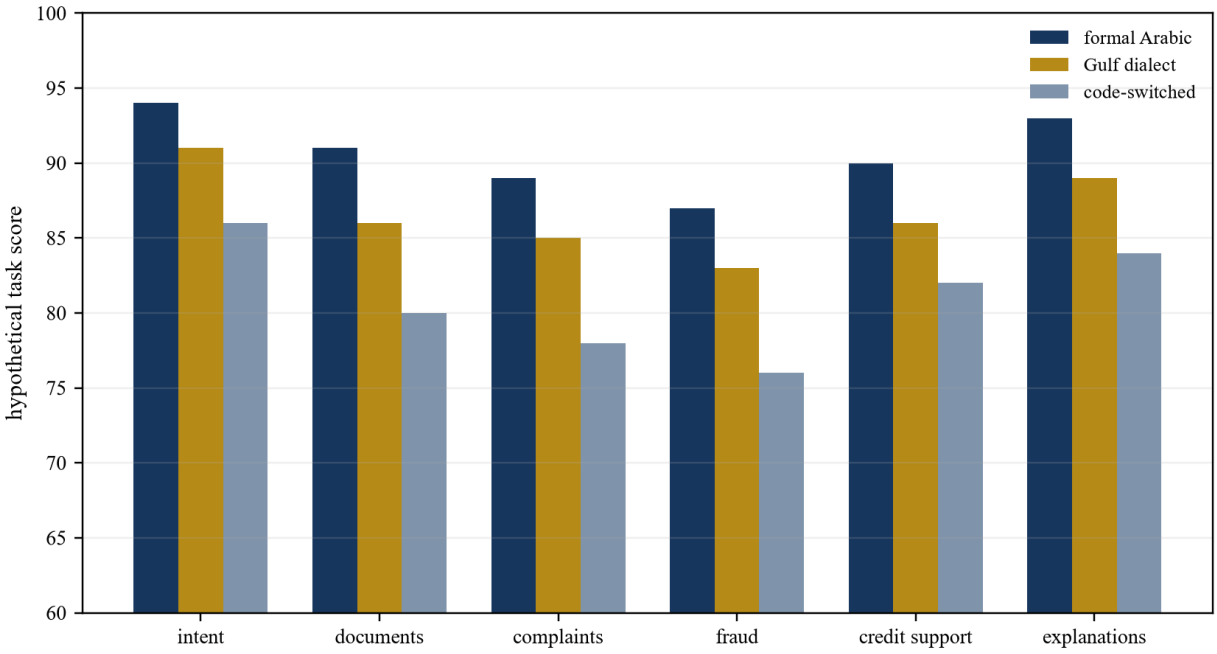
Generic language benchmarks provide limited acquisition evidence. The buyer should test the tasks that create or protect value: identity matching, document extraction, intent detection, product explanation, complaint classification, fraud review, credit support, transaction description and compliance escalation.

Performance should be segmented by dialect, script, channel, product, customer group and market. Aggregate accuracy can conceal weak results for a commercially important minority. Precision, recall, calibration and abstention should be selected according to consequence. A missed fraud alert differs from an awkward customer-service response.

The test set should be independent of development data and reflect production conditions. It should include rare events, incomplete inputs and changes over time. Human reviewers should be qualified in the language and financial task. Disagreement between reviewers should be measured rather than hidden.

The buyer should assess whether the system recognises uncertainty and routes cases appropriately. A model that abstains safely can be more valuable than one that answers every question. Escalation capacity and service level belong in unit economics.

**Figure 2. Hypothetical Arabic task-performance profile**




*Wholly hypothetical performance indices; the figure is methodological and is not a market benchmark.*

## 5. Evaluate data rights and provenance

Possession of data does not establish ownership, lawful use or transferability. The buyer should create a data-rights register covering source, customer relationship, consent, controller and processor role, purpose, retention, localisation, sharing, model-training use, deletion and change of control.

Data obtained through open-finance access may carry defined purposes and consent conditions. Sensitive or specially protected information can face additional restrictions. The acquisition model should identify revenue and model performance dependent on each data set and reduce value when continued use remains uncertain.

Provenance should extend to labels and derived features. Contractor annotation, synthetic augmentation, translation and third-party enrichment can introduce licence, confidentiality and quality issues. The target should demonstrate how a record can be removed or corrected across training, retrieval and production systems.

The buyer should test whether model quality survives a lawful-data constraint. A model that depends on data unavailable after closing may require retraining, customer re-consent or reduced functionality. Replacement cost, performance loss and delay should be funded explicitly.

**Table 2. Data-rights and provenance register**

| Data class | Rights evidence | Quality evidence | Valuation response |
|---|---|---|---|
| customer interaction | terms, consent and purpose | language, channel and timestamp | value only permitted continued use |
| open-finance data | regulated access and user authority | completeness and refresh | adjust for consent and access continuity |
| identity document | lawful basis and retention | extraction and verification result | price remediation and deletion duty |
| transaction history | source and processing purpose | bank reconciliation | separate service use from training use |

| Data class | Rights evidence | Quality evidence | Valuation response |
|---|---|---|---|
| annotations | assignment and reviewer controls | agreement and error sampling | deduct re-annotation cost |
| derived features | documented lineage | stability and bias tests | reduce opaque dependent value |
| third-party corpus | licence and restrictions | domain and dialect relevance | exclude non-transferable benefit |

*Proposed register; legal enforceability requires transaction-specific review.*

## 6. Map licences and product permissions

The target's licence should be mapped to every customer journey. Data aggregation, payment initiation, lending, insurance, investments and advice can require different permissions. Marketing language and technical capability should be compared with actual regulated activity.

The UAE Open Finance Regulation permits licensed data-sharing and service-initiation activity and sets limitations unless additional licences are held.[1][3] The rulebook identifies consumer consent, authentication, security, AML, fraud and technology-risk requirements.[2][3] Saudi Arabia's framework combines business rules, technical standards, testing and certification.[4][5]

The buyer should review licence conditions, regulatory correspondence, inspections, incidents, complaints, outsourcing, capital, insurance and key-person requirements. It should identify products operated through a partner licence and revenue dependent on that relationship.

Change-of-control analysis should begin early. Approval, notice, local ownership, governance, data location or management requirements can affect timing and structure. Valuation should separate current authorised revenue from expansion that requires a future permission.

## 7. Test bank connectivity and open-finance access

Connectivity can be a genuine asset when interfaces are certified, secure, stable and supported by transferable relationships. It can also be a collection of bespoke integrations with high maintenance cost. The buyer should inventory each bank, product, API, message, certificate, consent journey, service level and incident.

The UAE Open Finance Framework includes a trust framework, API hub and common infrastructure for data sharing and transaction initiation.[1] The CBUAE reported that the initiative went live in 2025 with initial banks and third-party providers meeting operational requirements.[6] Saudi Arabia's open-banking programme includes a laboratory and conformance testing.[4][5]

The buyer should measure economic coverage rather than connection count. A connection to one major bank can matter more than several low-use interfaces. Coverage should link to active customers, consent, transaction value, revenue and contribution.

Integration diligence should test credential ownership, certificate expiry, bank consent, change control, version migration, rate limits, outage handling and reconciliation. A technical connector without a durable operating right should receive limited value.

## 8. Reconstruct model governance and human accountability

The model inventory should identify purpose, owner, version, data, validation, limits, dependencies and downstream decisions. Arabic-language components, generic foundation models, deterministic rules and third-party services should be separated.

Human accountability should be visible in the workflow. A reviewer needs appropriate language and financial competence, access to evidence, authority to change or stop an outcome, time and quality assurance. Formal approval without meaningful intervention provides weak protection.

Validation should cover conceptual soundness, language and data quality, implementation, task performance, calibration, bias, stability, explainability, security and use. Independent challenge can be organisational or procedural; it must have sufficient competence and authority.

Change control should define when a new model, prompt, corpus, dialect, product, jurisdiction or interface requires testing and approval. Vendor updates should not silently alter regulated outcomes. The buyer should compare approved and production configurations.

**Figure 3. Proposed GCC fintech AI governance stack**


*Accountability and evidence should increase with customer consequence and regulatory materiality.*

## 9. Detect bias, exclusion and customer harm

Performance should be tested across language, nationality, gender, age, income, disability, digital confidence and other relevant groups where lawful and appropriate. The purpose is to identify differential error or access, not to assume that every difference is improper.

Arabic users can experience exclusion when a product nominally supports Arabic while important disclosures, complaints or verification remain English-centred. Right-to-left layout, document capture, names and transliteration can create operational errors. The buyer should test the complete journey rather than isolated model output.

Credit, fraud and compliance models require careful outcome analysis. False positives can block legitimate customers; false negatives can create loss and regulatory exposure. Human overrides should be measured by group, reason and outcome.

Remediation cost belongs in valuation. Data repair, retraining, customer communication, review, reimbursement and regulator engagement can turn a technical gap into a material cash requirement. Immature cohorts should receive lower forecast confidence.

## 10. Price operational resilience and cybersecurity

Regional fintech platforms depend on cloud infrastructure, identity providers, banks, payment systems, model vendors, data services and telecommunications. The buyer should map the critical service and test failure at each boundary.

The UAE Open Finance Regulation requires technology and cyber-risk management, including reliability, robustness, stability and availability.[3] Broader Basel operational-resilience and third-party principles provide relevant governance and continuity benchmarks.[11][12]

Service-level statistics should be reconstructed from raw monitoring and incidents. Contractual uptime can exclude maintenance and downstream failures. Month-end, campaign or payment peaks should be tested separately. Recovery should restore data consistency, customer access and regulated action, not merely infrastructure.

Cyber diligence should focus on identity, privileged access, secrets, model endpoints, data stores, payment initiation and customer communication. Arabic content creates no separate exemption from secure design. The target should preserve logs, test incident response and maintain executable vendor exit plans.

## 11. Test product localisation beyond language

Localisation includes product design, legal terms, identity, payments, calendars, currencies, cultural expectations, customer support and dispute handling. Translation can improve access while leaving the product economically or operationally foreign. The buyer should test whether local design changes produce measurable customer outcomes.

The diligence team should walk each material journey from marketing and onboarding through identity, consent, decision, payment, servicing, complaint and exit. For every step, it should record the language shown, the decision made, the data consumed, the responsible entity and the evidence retained. A bilingual interface can still route customers into an English-only exception process, an overseas support queue or a rule designed for a different market.

Identity and name handling deserve specific attention. Arabic names can have spelling variants, prefixes, transliteration differences and ordering conventions. Matching rules that work on English data can create duplicate customers, failed screening or incorrect risk aggregation. The target should show how uncertainty is managed and when human review occurs.

Product rules can vary by market. Salary cycles, Islamic-finance structures, credit-bureau access, payment methods, public-sector identity infrastructure and consumer-protection requirements affect workflow. A shared platform should preserve local rules without creating ungoverned custom code.

Customer communication should be tested for substantive parity. Important terms, prices, risks, consent, complaint routes and adverse decisions should remain clear across languages and channels. A platform that uses Arabic for acquisition and English for consequential disclosures can create conduct and retention risk.

Disclosure quality should be tested for meaning, timing and reproducibility. The buyer should identify which language version governs, how changes are approved and whether the system can reproduce the exact disclosure accepted by a customer. Automated translation can support workflow, but accountable product and legal owners should approve consequential content.

Payments and collections require local evidence. The proposition may depend on salary timing, domestic transfer rails, merchant settlement, direct debit, card tokenisation or bank-specific reconciliation. Reported software margin can exclude manual treasury work, prefunding, reconciliation staff and failed-payment handling. Those costs should be traced to the products and cohorts that create them.

Customer support can reveal hidden product debt. Contact reasons, language, resolution time, repeat contact, escalation and redress should be segmented. A high Arabic contact rate can indicate healthy adoption, weak product clarity or both. The commercial test is whether service demand is understood, controllable and included in contribution economics.

**Table 3. Product-localisation diligence catalogue**

| Dimension | Diligence test | Evidence | Valuation relevance |
|---|---|---|---|
| names and identity | variants, transliteration and duplicates | matched outcomes and exception logs | onboarding loss and compliance cost |
| terms and disclosures | substantive bilingual parity | approved versions and comprehension test | conduct and complaint exposure |
| product rules | local eligibility and limits | versioned policy and approval | permission and error risk |
| Islamic-finance features | product and contract mapping | qualified review and customer records | addressable market and liability |
| payment behaviour | local rails and salary cycles | transaction and settlement evidence | conversion and retention |
| service and complaints | Arabic response and escalation | case records and resolution quality | support cost and customer trust |

*Proposed tests; requirements remain product- and jurisdiction-specific.*

## 12. Rebuild unit economics after localisation and control

Revenue should be reconciled by product, market, customer cohort, language journey and channel. Subscription, transaction, interchange, financing, referral and implementation revenue have different durability and regulatory dependencies. Gross transaction value should not be confused with target revenue or contribution.

Revenue presentation should be reconciled to contract, transaction flow and collected cash. A pass-through payment can appear as gross revenue even though the target retains only a fee. Financing income can embed credit and funding risk. Implementation fees can support current cash while having weak recurrence. The model should identify the event that earns revenue and every party with a claim on it.

Direct cost should include data access, bank connectivity, cloud, model inference, Arabic annotation, localisation, customer support, compliance, fraud, cybersecurity, insurance and regulatory capital where applicable. Regional expansion can duplicate legal, control and support cost before scale produces benefit.

Acquisition cost should include channel economics and incentives. A bank or government partner may supply customers at low reported marketing cost while retaining commercial leverage, data access or termination rights. Founder relationships can create a similar effect. The buyer should calculate economics under the current arrangement and under a replacement-cost case; the difference measures dependency.

Localisation and control cost should be separated into recurring, step-fixed and remedial categories. Recurring costs include regulated operations, monitoring, support and data access. Step-fixed costs arise when a jurisdiction needs a legal entity, licence, hosting environment or team. Remedial costs address historical gaps. This classification prevents recurring compliance work from being presented as temporary.

Cash conversion should be reconciled to contribution. Settlement reserves, partner collateral, receivables, disputed transactions, customer-money segregation and regulatory capital can absorb cash even while accounting margin grows. The valuation model should show working capital, restricted cash and capital requirements by product and market.

The hypothetical case serves 420,000 active users and generates USD 24.0 million of annual revenue. Data, connectivity and cloud cost USD 3.6 million; model, annotation and localisation cost USD 2.4 million; customer operations cost USD 3.0 million; fraud, compliance and security cost USD 3.2 million; partner and distribution cost USD 2.8 million. Contribution before central cost, tax and capital is USD 9.0 million.

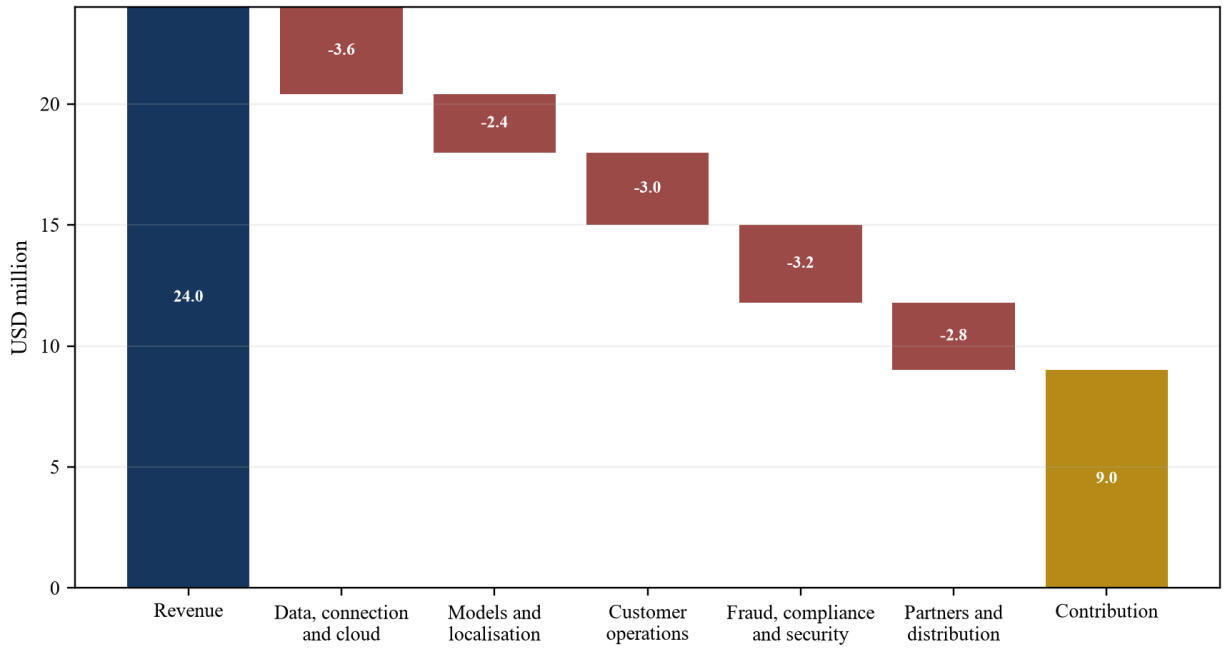
Every amount is hypothetical. The example does not claim an achievable scale or margin. Its purpose is to put language, data, permissions and control cost inside contribution rather than below a headline software margin.

### Cohort-profitability method

Cohorts should be segmented by country, product, acquisition channel, language journey, customer risk and onboarding period. Revenue retention can conceal rising partner, fraud or support cost. Contribution retention shows whether the relationship remains economically valuable.

The buyer should compare Arabic-first, English-first and mixed-language journeys where lawful and meaningful. A difference can reflect customer mix, channel or product rather than language quality. Attribution should use matched populations and explicit limitations.

**Figure 4. Hypothetical annual contribution bridge**




*Wholly hypothetical USD millions; central cost, tax and capital remain outside the displayed contribution.*

## 13. Measure adoption and customer outcomes

Downloads, registrations and interactions show activity while they do not prove economic adoption. The buyer should measure funded accounts, completed transactions, repeat use, product retention, complaint outcomes and contribution. Metrics should use stable active-user definitions.

Language adoption should be measured at journey level. A customer can select Arabic and revert to English during identity, payment or complaint steps. Drop-off should be attributed to the specific stage and compared with matched cohorts. Unsupported channels and agent handoffs should remain visible.

Customer outcomes depend on product. Payments can be assessed through completion, fraud and dispute. Credit requires affordability, performance and treatment. Advice requires suitability and continuing service. A single engagement metric cannot represent them all.

The target should connect model performance to operations. Better intent detection can shorten service time and increase escalation. Better document extraction can reduce manual input and create review cost. Value follows the net outcome after control and customer impact.

## 14. Price distribution and counterparty concentration

Regional reach can depend on banks, merchants, employers, government platforms, app stores, telecom operators and payment networks. The buyer should map acquisition, service and revenue dependencies by counterparty. Several customer contracts can share one upstream risk.

Distribution quality should be measured by acquired active users, retention, contribution and ownership of the relationship. A target that relies on a bank-branded channel can have strong economics while possessing limited direct customer access. Data and cross-sell rights should follow contract evidence.

Partner contracts should be tested for exclusivity, minimums, pricing, service levels, audit, data use, assignment, change of control and termination. Informal executive relationships should not be capitalised as durable distribution.

Concentration should include technical and regulatory sponsors. Loss of a bank connection or licensed partner can affect many revenue lines. The valuation should model transition time, replacement cost, customer attrition and reduced functionality.

**Table 4. Regional distribution and dependency matrix**

| Counterparty | Economic role | Evidence | Downside test |
|---|---|---|---|
| bank | data, payment, custody or channel | contract, consent and service record | consent or connection loss |
| merchant | acquisition and transaction flow | active cohort and contribution | volume and exclusivity change |
| employer | salary-linked distribution | eligible, active and retained users | contract renewal and employee churn |
| government platform | identity or service access | operating agreement and acceptance | policy or interface change |
| app platform | customer acquisition | source and conversion history | ranking, fee or access change |
| licensed partner | regulatory perimeter | agreement and supervisory evidence | termination or permission restriction |

*Proposed matrix; concentration should be measured by revenue, contribution and critical service.*

## 15. Evaluate regional expansion as a new operating model

GCC markets share language and commercial connections while maintaining different legal, regulatory, banking and customer conditions. A product proven in one market is evidence for adaptation, not proof of regional scalability.

The buyer should build a market-entry gate covering licence, legal entity, data location, bank access, identity, product rules, customer support, model validation, vendor contracts and economics. Each gate should have evidence, cost, owner and timing.

Language performance should be revalidated. Dialect, terminology, customer behaviour, documents and fraud patterns can change. A model trained on one country's population can create lower performance or unfair outcomes elsewhere.

Expansion value should use probability-weighted cash flow after local cost. A memorandum of understanding, sandbox acceptance or potential customer provides weaker evidence than permission, executed distribution and collected contribution. Seller consideration should follow mature evidence.

## 16. Value the platform by evidence layer

A single revenue multiple can hide the assets and dependencies that create value. The buyer should triangulate discounted cash flow, cohort economics, comparable-company evidence, transactions, replacement cost and scenario analysis using consistent revenue and risk definitions.

Layer one is collected contribution from current authorised products. Layer two is protected continuity supported by transferable data, contracts, permissions and people. Layer three is evidenced improvement with funded actions. Layer four is buyer-specific distribution or product synergy. Layer five is future-market or autonomous-AI option value.

Language data, technology, customer relationships, contracts, licences and trade names can be separate intangible assets with different useful lives and transfer conditions. IFRS 3 and IAS 38 provide relevant accounting frameworks.[48][49] Purchase-price allocation should not substitute for investment valuation, while it can expose assumptions about separability and durability.

The income approach should begin with the smallest defensible operating unit. Revenue and contribution should be forecast by product, jurisdiction, channel and cohort where drivers differ. Retention, loss, take rate, pricing and direct cost assumptions should tie to observed populations. Terminal economics should reflect data and model maintenance, partner bargaining power and regulatory cost.

Comparable-company evidence requires business-model normalisation. Two fintech businesses can report similar revenue while one bears credit risk, another passes through network fees and a third sells subscription software. The analyst should align gross versus net presentation, capital intensity, loss exposure, recurring share, customer concentration and jurisdiction before applying a multiple.

Transaction evidence needs the same discipline. Announced consideration can include earn-outs, rollover, assumed debt, preferred instruments or strategic rights. Public disclosure may omit revenue quality, loss profile and regulatory conditions. Each transaction multiple should carry an evidence score when the denominator or consideration is incomplete.

Replacement cost is useful only for assets that can be recreated legally and operationally. Software-development spending does not recreate consented Arabic data, production feedback, regulatory permissions, bank connectivity, customer trust or a trained local team. Historical expenditure also does not prove value. The buyer should estimate time, lawful access, failure risk and foregone contribution as well as build cost.

The investment committee should maintain a risk ledger showing where each uncertainty enters volume, margin, timing, terminal value, discount rate or transaction protection. This avoids counting the same licence delay, partner loss or remediation cost in both projected cash flow and a broad risk discount.

**Table 5. Evidence-layer valuation architecture**

| Layer | Evidence threshold | Method | Protection |
|---|---|---|---|
| current contribution | invoices, collections and direct cost reconcile | cohort DCF | ordinary warranties |
| protected continuity | rights, permissions and contracts survive | retention-adjusted DCF | consent condition and covenant |
| evidenced improvement | measured baseline and funded action | probability-weighted NPV | completion funding and milestone |

| Layer | Evidence threshold | Method | Protection |
|---|---|---|---|
| buyer synergy | named owner, capacity and integration plan | buyer-specific NPV | excluded from seller base value |
| regional option | permission and market evidence incomplete | staged option analysis | contingent consideration |

*Proposed architecture; amounts and weights remain transaction-specific.*

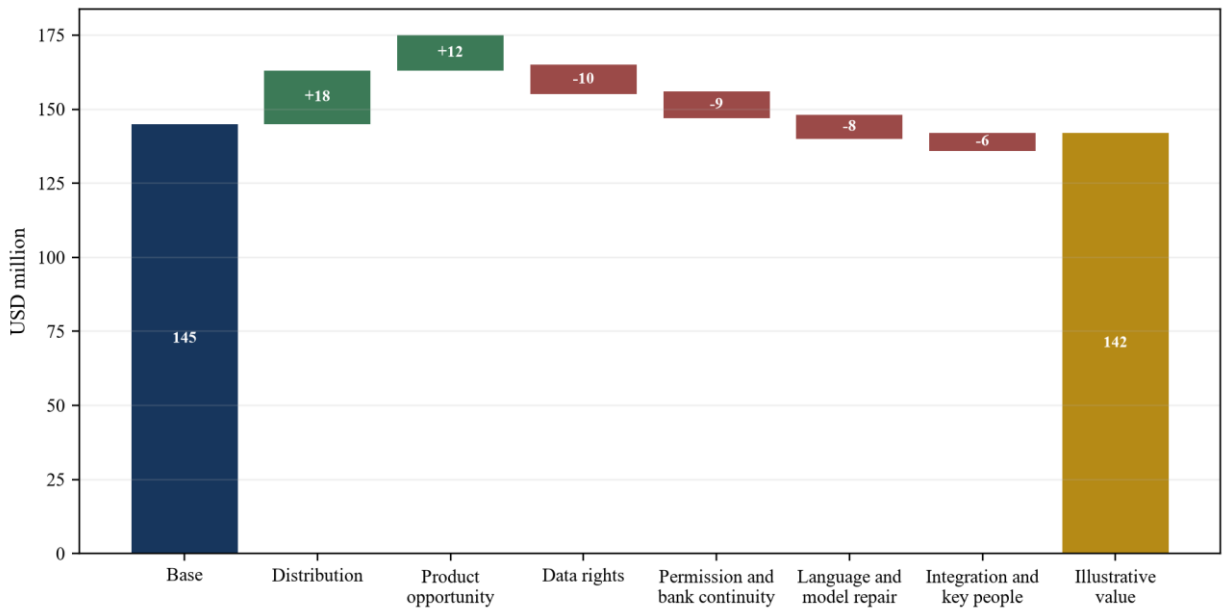
## 17. Apply a local-moat discount transparently

The valuation committee should avoid one opaque risk premium. Specific deductions can address weak Arabic task performance, uncertain data rights, non-transferable permissions, partner concentration, incomplete model governance, customer-outcome risk, key-person dependence and integration cost.

The hypothetical bridge begins with enterprise value of USD 145 million supported by stand-alone contribution and market assumptions. Verified local distribution and product opportunities add USD 18 million and USD 12 million. Data-right uncertainty reduces value by USD 10 million; permission and bank-continuity risk by USD 9 million; model and language remediation by USD 8 million; integration and key-person risk by USD 6 million. The illustrative value is USD 142 million.

Every amount is hypothetical. The bridge demonstrates method and is not a valuation opinion. A transaction requires buyer returns, capital structure, tax, market evidence and legal analysis.

**Figure 5. Hypothetical local-moat valuation bridge**




*Wholly hypothetical USD millions; the bridge is methodological and is not a valuation opinion.*

## 18. Test sensitivities and downside cases

Sensitivity should expose variables management can influence: active-user retention, partner pricing, localisation cost, fraud loss, support productivity, model quality and expansion timing. Market multiples should be separated from operating drivers.

Downside cases should include loss of a bank connection, delayed approval, data re-consent, partner termination, model degradation, security incident and failed market entry. The model should show liquidity needs as well as enterprise value.

Forecast benefits should not exceed the addressable product and customer population. A strong Arabic model creates little incremental value where decisions remain English-only or human capacity limits adoption. The buyer should cap benefit using operational evidence.

**Table 6. Hypothetical contribution sensitivity**

| Net revenue; USDm | Localisation and control cost USD 8m | USD 9m | USD 10m | USD 11m |
|---|---|---|---|---|
| 20 | 7.0 | 6.0 | 5.0 | 4.0 |
| 22 | 9.0 | 8.0 | 7.0 | 6.0 |
| 24 | 11.0 | 10.0 | 9.0 | 8.0 |
| 26 | 13.0 | 12.0 | 11.0 | 10.0 |

*Wholly hypothetical annual USD millions; no cell is a forecast or market benchmark.*

## 19. Translate evidence into transaction protections

Representations can address licences, data provenance, consent, model ownership, intellectual property, bank and partner contracts, cybersecurity, incidents, customer outcomes and financial metrics. Definitions should match the diligence populations.

Conditions can require regulatory approval, bank or partner consent, transfer of model rights, delivery of reproducible test results, closure of a material control gap or funding of remediation. Interim covenants should govern material model, data, product and partner changes.

Escrow, indemnity, retention and insurance should match enforceable exposure. Contingent consideration can be tied to retained contribution, permissions, Arabic task performance, partner continuity and mature customer outcomes. User growth alone provides weak protection.

Definitions should be engineered before remedies. Active customer, transaction, revenue, contribution, model incident, complaint, permission and partner continuity should correspond to data the buyer can reproduce after closing. An earn-out based on a seller dashboard creates dispute risk when population rules, refunds, failed transactions or allocated costs remain undefined.

Disclosure schedules should identify regulated products, competent authorities, material correspondence, permissions, data sets, processing purposes, subprocessors, models, incidents, bank dependencies and customer redress. The buyer can then connect each exception to a financial or operational response.

Interim covenants should protect the evidence base between signing and closing. Material changes to model version, training data, customer terms, pricing, bank routes, licences, key staff, cloud architecture and security controls can alter value. The covenant should permit ordinary-course operation while requiring notice and consent for changes that invalidate diligence or create new approval needs.

Contingent value should reward durable economics. Measures can include collected contribution from a defined cohort, renewal of a named bank relationship, effective permission, independently tested Arabic task performance or successful migration without material customer harm. Each measure needs an observation window, audit right, cost-allocation rule, change-control provision and dispute path.

**Table 7. Evidence-to-protection matrix**

| Evidence gap | Price response | Protection | Release evidence |
|---|---|---|---|
| uncertain data rights | exclude dependent benefit | representation and restricted use | lawful transfer and purpose |
| pending permission | defer market value | approval condition | effective permission |
| bank or channel consent | probability-weight revenue | consent and covenant | accepted transfer |

| Evidence gap | Price response | Protection | Release evidence |
|---|---|---|---|
| weak dialect performance | remediation deduction | completion funding | independent production test |
| immature outcome cohort | lower forecast confidence | retention or earn-out | seasoned contribution and outcomes |
| security gap | funded deduction | condition, escrow and indemnity | tested remediation |
| key-person dependence | continuity adjustment | retention and transition | documented repeatable operation |

*Proposed matrix; legal drafting and remedies remain transaction-specific.*

## 20. Design integration around customer and model continuity

Integration can change the evidence that supported value. Legal entity, licence, bank connections, identity, data location, model, product rules, customer terms and support can move. Each change should be mapped to consent, approval, testing and customer communication.

Data migration should preserve Arabic text, direction, encoding, provenance, consent and deletion state. Normalisation should not silently alter names, amounts or contractual content. Reconciliation should occur at record and customer level.

Model migration is a controlled change. The combined firm should compare old and new outputs on matched cases, investigate differences and monitor outcomes. Upstream mapping or population change can alter performance even when model code remains stable.

Customer continuity comes first. Access, payments, applications, complaints and support should remain available. Synergy should be released after replacement controls and capacity are proven.

The integration architecture should distinguish preserve, connect, migrate and retire decisions. Preserve applies where the target's regulated or language capability is valuable and stable. Connect uses governed interfaces while systems remain separate. Migrate moves a controlled population after matched testing. Retire follows evidence that obligations, records and customer access have transferred.

Model inventory should include rules, statistical models, machine-learning services, vendor components and human overrides. For each item, the team needs purpose, owner, version, input population, output consumer, validation, monitoring and fallback. A model can remain technically available while losing value because an upstream field changes, a vendor contract ends or experienced reviewers leave.

Parallel operation provides evidence when consequences are material. Old and new systems can process matched cases without immediately changing customer outcomes. Differences should be classified by data, rule, model, rounding, language, timing and operator action. Migration should require acceptable financial reconciliation, customer outcomes, security and operational capacity.

Synergy tracking should use a double-entry discipline: every benefit needs an operational change, and every change needs cost, dependency and customer-risk entries. Distribution uplift requires eligible population, consent, channel capacity, product fit and conversion evidence. Technology savings require retirement of contracts or capacity. Headcount savings require a redesigned process with maintained controls.

## 21. Retain knowledge and local accountability

Regional capability often resides in people who understand regulators, banks, language, product and operating exceptions. The buyer should map critical roles, authority, relationships, documentation and succession. Employment title is a weak proxy for actual dependency.

Retention should focus on capability transfer and accountability. Transition plans should document models, annotations, bank interfaces, policy decisions, incident history and partner obligations. Access and signing authority should move through controlled processes.

The combined organisation needs named owners for each regulated product, data set, model and customer outcome. Centralisation can improve control while reducing local response if authority and expertise are removed too quickly.

## 22. Execute a 180-day programme

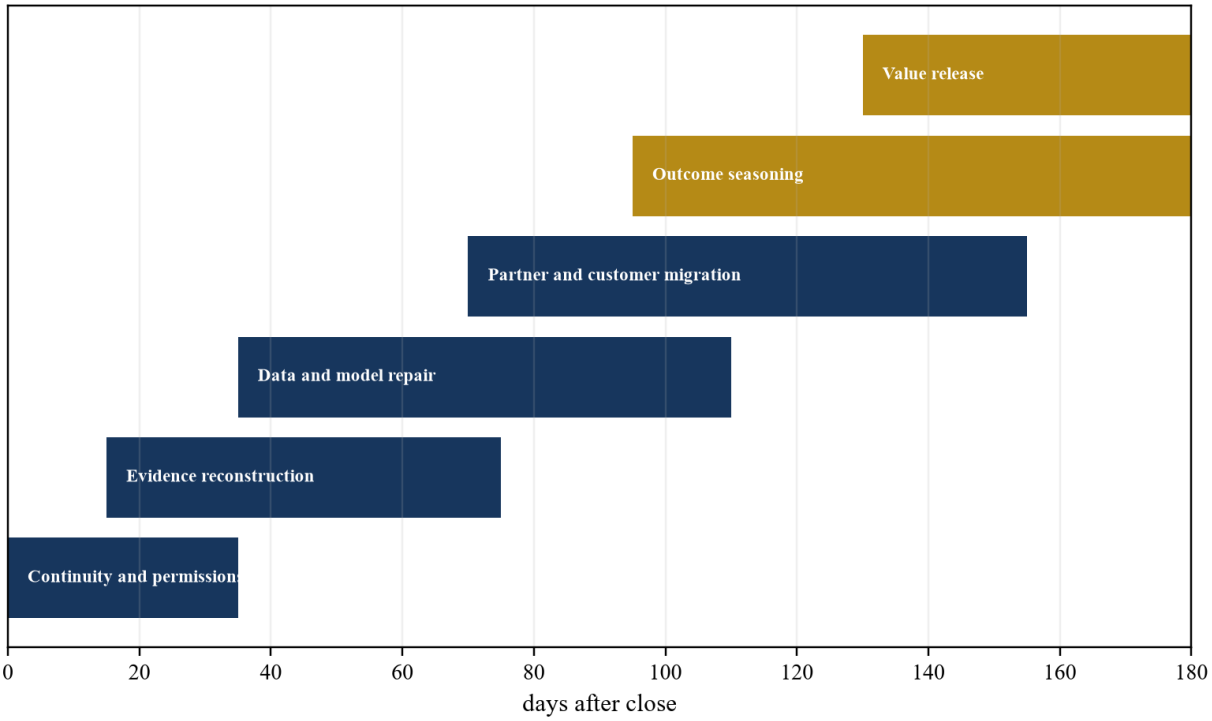
Days one to thirty should preserve licences, data, consent, bank access, models, logs, partner contracts and customer service. Governance, change restrictions and incident paths should be established. Revenue and contribution should reconcile to source records.

Days thirty to seventy should complete Arabic task tests, reconstruct customer journeys, validate data rights, map permissions and consents, and identify material gaps. High-risk functionality should be restricted where evidence remains incomplete.

Days seventy to one hundred and twenty should remediate priority data, model, security and product controls; obtain consents; and pilot integration on reversible cohorts. Language and outcome tests should cover changed systems.

Days one hundred and twenty to one hundred and eighty should season results, verify partner continuity and contribution, complete migration gates and release contingent value only after evidence passes.

**Figure 6. Proposed evidence-gated 180-day programme**




*Timing should follow transaction, regulatory, bank, customer and technology constraints.*

## 23. Decision and conclusion

Arabic data and regional reach deserve value when they produce verified customer outcomes and durable contribution within transferable legal and operating rights. Language coverage, user numbers, licences and bank logos can support that result; each requires evidence.

The buyer should separate language, data, permission, connectivity and distribution advantages. It should test performance by economic task and population, reconstruct consent and provenance, verify product permissions, measure partner concentration and price the full localisation and control stack.

A regional moat is durable when the combined firm can lawfully use the data, operate the model, maintain permissions, serve customers, retain partners and reproduce outcomes after closing. Missing rights or undocumented local knowledge can turn apparent advantage into remediation and delay.

A premium is supportable when current contribution reconciles, Arabic capability improves material tasks, data rights transfer, permissions and partners continue, outcomes are monitored and integration is evidence-gated. Price protection, narrower scope, funded remediation or contingent value is appropriate when those conditions remain incomplete.

## Frequently asked questions

Q: What creates an Arabic-data moat in GCC fintech? A: A defensible moat combines lawful and relevant data, strong performance on material Arabic tasks, transferable rights, customer adoption, model governance and durable contribution.

Q: Is an Arabic user interface sufficient evidence of localisation? A: No. The buyer should test identity, disclosures, product rules, support, complaints, payments and decision performance across dialects, scripts and channels.

Q: How should open-finance access affect valuation? A: Access supports value when licence, customer consent, certification, security, bank connectivity and change-of-control continuity are evidenced.

Q: How should Arabic model performance be tested? A: Tests should use independent production-like data segmented by dialect, script, product, customer group, jurisdiction and consequence, with qualified human review.

Q: Why can regional expansion destroy value? A: Each market can require new permissions, data arrangements, bank integrations, product rules, models and operating capacity. Forecast value should include those costs and probabilities.

Q: How should data rights affect the purchase price? A: Benefit dependent on a data set should receive full value only when provenance, lawful purpose, transfer, retention and continuing model use are evidenced.

Q: Which transaction protections address incomplete evidence? A: Conditions, covenants, representations, indemnities, escrow, reserves, retention and contingent consideration can be linked to permissions, consents, performance and outcomes.

Q: What should happen during the first 180 days? A: The buyer should preserve continuity, reconstruct evidence, transfer rights, repair material controls, pilot migrations, season outcomes and release value only after defined gates pass.

## References


**[1]** Central Bank of the UAE, Open Finance Regulation https://rulebook.centralbank.ae/en/entiresection/5689
**[2]** Central Bank of the UAE, Open Finance minimum requirements https://rulebook.centralbank.ae/en/entiresection/6170
**[3]** Central Bank of the UAE, Open Finance limitations https://rulebook.centralbank.ae/en/entiresection/6135
**[4]** Saudi Central Bank, Open Banking Programme https://www.openbanking.sama.gov.sa/index-en.html
**[5]** Saudi Central Bank, licensing of open-banking fintech companies https://sama.gov.sa/en-US/MediaCenter/News/Pages/news-1135.aspx
**[6]** Central Bank of the UAE, Annual Report 2025 https://www.centralbank.ae/media/4qbn11cl/annual-report-2025-en.pdf
**[7]** Central Bank of the UAE, FinTech and digital transformation https://www.centralbank.ae/en/our-operations/fintech-digital-transformation/
**[8]** Saudi Central Bank, Open Banking Policy https://www.sama.gov.sa/en-US/Documents/Open_Banking_Policy-EN.pdf
**[9]** Saudi Central Bank Rulebook, payment service access https://rulebook.sama.gov.sa/en/article-95-1

**[10]** UAE regulatory authorities, guidelines for financial institutions adopting enabling technologies https://www.centralbank.ae/en/news-and-publications/news-and-insights/press-release/uae-regulatory-authorities-jointly-issue-guidelines-for-financial-institutions-adopting-enabling-technologies/
**[11]** Basel Committee, Principles for operational resilience https://www.bis.org/bcbs/publ/d516.htm
**[12]** Basel Committee, Principles for sound management of third-party risk https://www.bis.org/bcbs/publ/d605.htm
**[13]** Bank for International Settlements, regulating AI in finance https://www.bis.org/fsi/publ/insights63.htm
**[14]** Financial Stability Board, artificial intelligence and financial stability https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/
**[15]** IOSCO, AI and machine learning by intermediaries and asset managers https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf
**[16]** Abu Dhabi Global Market, Data Protection Regulations 2021 https://www.adgm.com/operating-in-adgm/office-of-data-protection/legislation
**[17]** Dubai International Financial Centre, Data Protection Law https://www.difc.com/business/operating/data-protection
**[18]** Saudi Data and Artificial Intelligence Authority, Personal Data Protection Law https://sdaia.gov.sa/en/SDAIA/about/Files/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf
**[19]** United Arab Emirates, Personal Data Protection Law https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws
**[20]** Bahrain, Personal Data Protection Authority https://www.pdp.gov.bh/
**[21]** Qatar Central Bank, FinTech Strategy https://www.qcb.gov.qa/en/Pages/FinTech.aspx
**[22]** Central Bank of Bahrain, regulatory sandbox https://www.cbb.gov.bh/fintech/
**[23]** Central Bank of Oman, fintech regulatory sandbox https://cbo.gov.om/Pages/Fintech.aspx
**[24]** Saudi Central Bank, Cyber Security Framework https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf
**[25]** Central Bank of the UAE, Consumer Protection Regulation https://www.centralbank.ae/en/our-operations/consumer-protection/
**[26]** Saudi Central Bank, Consumer Protection Principles https://rulebook.sama.gov.sa/en/consumer-protection-principles
**[27]** Bank for International Settlements, Project Aperta https://www.bis.org/about/bisih/topics/open_finance/aperta.htm
**[28]** Bank for International Settlements, open finance and APIs https://www.bis.org/publ/othp66.htm
**[29]** Financial Action Task Force, opportunities and challenges of new technologies for AML and CFT https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-aml-cft.html
**[30]** Financial Action Task Force, digital identity guidance https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html
**[31]** National Institute of Standards and Technology, AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework
**[32]** National Institute of Standards and Technology, Generative AI profile https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
**[33]** National Institute of Standards and Technology, Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework
**[34]** International Organization for Standardization, ISO IEC 42001 https://www.iso.org/standard/81230.html
**[35]** Organisation for Economic Co-operation and Development, AI principles https://oecd.ai/en/ai-principles
**[36]** UNESCO, Recommendation on the Ethics of Artificial Intelligence https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
**[37]** World Bank, Global Financial Inclusion Database https://www.worldbank.org/en/publication/globalfindex
**[38]** International Monetary Fund, Financial Access Survey https://data.imf.org/fas
**[39]** GSMA, State of the Industry Report on Mobile Money https://www.gsma.com/sotir/
**[40]** Arab Monetary Fund, Arab Regional Fintech Working Group https://www.amf.org.ae/en/arab-regional-fintech-working-group
**[41]** Cambridge Centre for Alternative Finance, global fintech regulation https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/
**[42]** European Union, Artificial Intelligence Act https://eur-lex.europa.eu/eli/reg/2024/1689/oj
**[43]** European Union, General Data Protection Regulation https://eur-lex.europa.eu/eli/reg/2016/679/oj
**[44]** Board of Governors of the Federal Reserve System, SR 11-7 model risk management https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm
**[45]** Bank of England, Model risk management principles https://www.bankofengland.co.uk/prudential-regulation/publication/2023/may/model-risk-management-principles-for-banks-supervisory-statement
**[46]** International Organization for Standardization, ISO 27001 information security https://www.iso.org/isoiec-27001-information-security.html
**[47]** International Valuation Standards Council, International Valuation Standards https://ivsc.org/standards/
**[48]** IFRS Foundation, IFRS 3 Business Combinations https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/
**[49]** IFRS Foundation, IAS 38 Intangible Assets https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/
**[50]** IFRS Foundation, IFRS 10 Consolidated Financial Statements https://www.ifrs.org/issued-standards/list-of-standards/ifrs-10-consolidated-financial-statements/

## About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.