Regulatory Passporting across the GCC

The Expansion Cost Investors Underestimate

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

The Gulf Cooperation Council is building increasingly connected financial infrastructure. The AFAQ system connects the real-time gross settlement systems of GCC member states for cross-border payments in local currencies. National authorities are also developing payment-services, open-banking and open-finance regimes. These initiatives improve infrastructure, standards and market connectivity. They do not establish a general authorisation passport through which a fintech licensed in one GCC state may automatically conduct regulated business in every other member state.

Official rules illustrate the country-specific perimeter. The Central Bank of the UAE requires prior authorisation for regulated retail payment services and created a separate Open Finance licence, subject to defined deemed-licensed provisions. The Saudi Central Bank implements its Payments and Payment Services Law and has commenced licensing fintech companies for open-banking services. The Central Bank of Bahrain publishes a payment-services module with licensing, financial-resource, safeguarding, customer-protection and fraud-reimbursement requirements. Qatar Central Bank publishes a Payment Services Regulation and operates dedicated fintech licensing and supervision functions. The Central Bank of Kuwait publishes regulatory instructions for electronic payment service providers. The Central Bank of Oman publishes a licensing policy for payment-service providers and an Open Banking Regulatory Framework with licensing criteria and continuing obligations.

The European Union provides a useful external benchmark. Under the second Payment Services Directive, authorised payment institutions can use formal passporting mechanisms supported by technical standards, registers and home-host supervisory cooperation. The comparison clarifies what an actual passport needs: a legal basis, scoped rights, notification or approval process, home and host responsibilities, public registers, supervisory information exchange and enforceable conditions. Shared infrastructure or similar terminology alone is insufficient.

This paper develops a board-ready framework for fintech expansion across the GCC. It maps regulated activities and entry structures, separates infrastructure access from legal permission, builds a country requirements register, models duplicated and shared operating cost, sequences licensing and launch, and creates an evidence-based capital gate. Six figures cover the authorisation logic, regional infrastructure and licensing layers, market-entry architecture, regulatory cost stack, expansion critical path and board gate. Six tables provide a perimeter inventory, country evidence map, entry-route comparison, hypothetical cost model, control-variation register and diligence plan.

All monetary amounts, staffing assumptions, probabilities, durations and market-entry economics in the worked example are hypothetical management assumptions created solely to demonstrate the method. Actual requirements and outcomes depend on the activity, customer, product, legal entity, jurisdiction, regulator and application. This paper provides general information for professional audiences and does not provide legal, regulatory, tax, accounting, cyber-security, data-protection, investment or securities advice.

JEL Classification: G21, G23, G28, F36, L26, O16

Keywords: regulatory passporting, GCC fintech, payments, licensing, market entry, compliance, regulatory capital, expansion

1. Define passporting before underwriting it

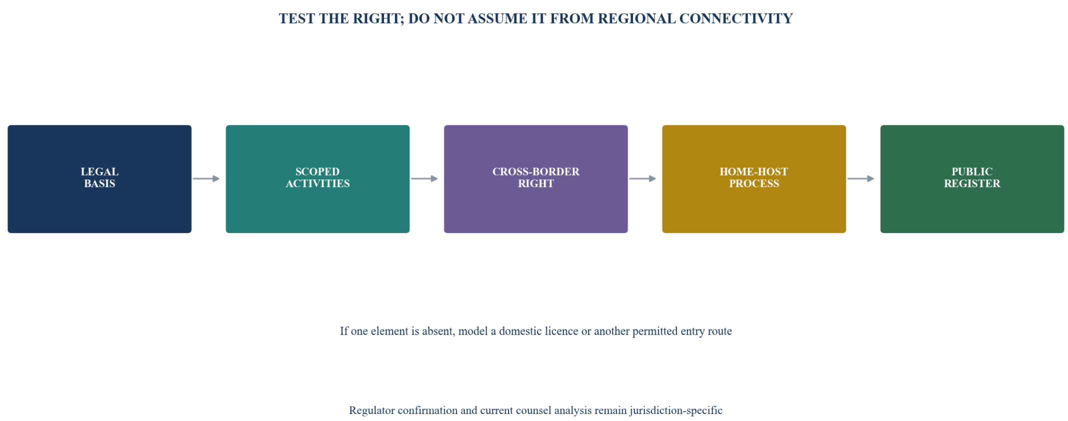
Regulatory passporting is a legal mechanism. It should identify which authorisation can be used, which activities are covered, where the firm can operate, which notifications or approvals apply, which authority supervises the firm and which host-country rules remain binding.

A regional strategy should therefore begin with a binary evidence question: does an enacted framework grant the proposed entity a cross-border right to perform the proposed regulated activity? If the answer is not supported by current law, regulation and regulator confirmation, the financial model should assume country-specific authorisation or an alternative permitted structure.

Commercial language can obscure this test. Regional connectivity, interoperability, common standards, a regulatory sandbox, an innovation hub or a memorandum of understanding may support expansion. None of those descriptions independently grants permission to hold customer money, initiate payments, acquire merchants, issue stored value, access financial data, extend credit or market a regulated product.

The board should keep four layers separate: regulatory permission, payment and data infrastructure, commercial distribution and operational delivery. A country can be connected at the infrastructure layer while retaining its own licensing perimeter, conduct rules, supervision and enforcement.

Figure 1. Regulatory-passport evidence test



Author framework. A passport exists only when a legal basis grants a scoped cross-border right and defines home-host supervision.

2. Start with the activity, not the app

A customer sees one interface. The law can see several activities. A fintech product may combine account information, payment initiation, merchant acquiring, remittance, stored value, card issuing, credit, foreign exchange, insurance distribution, investment functionality, data processing and technology services.

Each activity can have a different perimeter. The company should describe who contracts with the customer, who receives the instruction, who holds or controls money, who settles, who performs onboarding, who decides a credit or investment outcome, who handles complaints and who bears loss when a transaction fails.

The perimeter inventory should follow the transaction from acquisition to termination. Marketing can itself be regulated. A firm that relies on a licensed partner still needs to identify whether it acts as an agent, outsourced service provider, technical service provider, introducer, distributor or another legally recognised role. Labels in a commercial agreement do not determine the regulatory outcome.

Table 1. Regulated-activity perimeter inventory

Activity	Operating question	Evidence required	Expansion implication
Customer acquisition	who markets, solicits and contracts?	journey, terms, scripts and entity map	promotion restrictions and local contracting entity
Onboarding	who identifies, verifies and screens the customer?	KYC flow, vendor roles, decision rules and audit trail	local AML, sanctions and digital-onboarding requirements
Money movement	who receives, holds, initiates, acquires or settles funds?	funds flow, accounts, ledger, scheme and settlement map	payment, remittance, stored-value and safeguarding perimeter
Data access	who requests, receives, stores and reuses financial data?	consent, API, purpose, retention and deletion map	open-finance and data-protection permission
Credit or investment	who makes the decision and bears risk?	underwriting, suitability, funding and balance-sheet map	lending, crowdfunding, securities or advisory perimeter
Complaints and loss	who resolves disputes and reimburses the customer?	complaint, fraud, chargeback and redress process	conduct standards, reserves and service obligations

The inventory should be completed for every product and target country using current legal and regulatory advice.

3. Separate shared infrastructure from shared permission

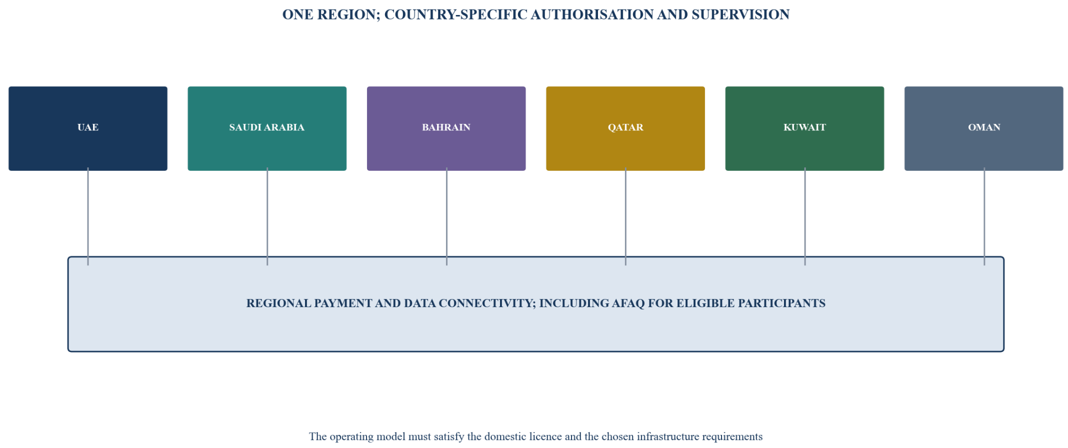
The Gulf Payments Company states that AFAQ connects the real-time gross settlement systems of GCC member states and supports cross-currency payments in local currencies with same-day settlement finality.[1] Its published participant requirements include a local settlement account, membership of the relevant domestic RTGS and compliance with AFAQ technical and operational requirements.[2]

AFAQ is material regional infrastructure. It can improve payment speed, settlement and connectivity for eligible participating institutions. Its operating design does not, by itself, authorise an unlicensed fintech to provide a regulated payment service to customers in every member state.

This distinction affects valuation and capital planning. Infrastructure connectivity can reduce integration cost for eligible participants and improve a service proposition. Domestic authorisation can still require a local entity, capital, leadership, safeguarding, policies, cyber controls, reporting, audit, complaint operations and ongoing regulatory engagement.

The technology roadmap should show both layers. One workstream connects the firm to banks, schemes, open-finance frameworks, domestic switches or regional settlement infrastructure. Another workstream establishes and maintains the legal right to serve customers. The launch gate requires both.

Figure 2. Regional infrastructure and domestic authorisation layers



Author framework. Connected rails support movement; domestic regimes determine which entity may provide which service.

4. Use an external passport benchmark

The European Banking Authority publishes technical standards on passporting under the second Payment Services Directive, a central register framework and home-host cooperation materials.[3] The EU model provides an external benchmark for identifying the components of formal passporting.

The benchmark should not be transplanted into a GCC legal conclusion. It is useful because it makes the required machinery visible: an authorised institution, home authority, host state, notification information, scoped services, establishment or cross-border mode, register entry, supervisory cooperation and conditions for intervention.

A management deck that calls a regional plan a passport should therefore cite the actual legal mechanism and show the approved scope. If no comparable mechanism applies, the deck should say that the firm is pursuing coordinated multi-country licensing or partner-led market entry.

Terminology matters to the board and investor because the cost profiles differ. A formal passport can reduce duplicate authorisation work while retaining host obligations. Coordinated licensing can reuse documentation but still require separate applications, capital, people and regulator engagement.

5. Map the six domestic regimes from official evidence

The UAE Open Finance Regulation requires an Open Finance licence unless the person falls within defined deemed-licensed categories. It states a minimum capital requirement of AED 1 million for an Open Finance Provider and permits additional capital requirements based on risk, size or complexity.[4] The UAE Retail Payment Services and Card Schemes Regulation separately requires prior licensing for in-scope retail payment services, subject to stated exemptions.[5]

Saudi Arabia's implementing regulations under the Payments and Payment Services Law establish licensing, supervision and oversight requirements for payment-service providers.[6] SAMA announced in 2026 that it had commenced licensing fintech companies to provide open-banking services after the sandbox phase.[7]

The Central Bank of Bahrain's payment-services module includes licensing, financial-resource, safeguarding, customer-protection and fraud-reimbursement requirements.[8] Qatar Central Bank publishes a Payment Services Regulation requiring in-scope providers to obtain authorisation and maintains fintech licensing and supervision functions.[9] The Central Bank of Kuwait publishes instructions addressed to electronic-payment providers and relevant supervised institutions.[10] The Central Bank of Oman identifies a payment-service-provider licensing policy and publishes an Open Banking Regulatory Framework that sets licensing criteria and continuing obligations.[11]

These official materials support a country-by-country underwriting approach. They do not determine the treatment of a particular product without a complete facts analysis.

Table 2. Official-evidence map for GCC fintech expansion

Market	Official evidence used	Board implication
UAE	CBUAE retail-payment and Open Finance regulations	test separate activities, deemed-licensed status, capital and phased framework access
Saudi Arabia	SAMA payments regulations and open-banking licensing announcement	map payment and open-banking permissions, local supervision and technical conformance
Bahrain	CBB payment-services rulebook module	budget licensing, safeguarding, customer protection, fraud and reporting controls
Qatar	QCB Payment Services Regulation and fintech supervision function	confirm licence scope, entity, financial resources, operating controls and inspection readiness
Kuwait	CBK electronic-payment regulatory instructions	identify provider category, activity scope, agent or outsourcing model and continuing requirements
Oman	CBO PSP policy and Open Banking Regulatory Framework	model domestic licensing, technology, data, KYC, cyber and continuing obligations

This is a source map rather than legal advice; requirements should be confirmed against current rules and regulator communications.

6. Choose the country entry architecture

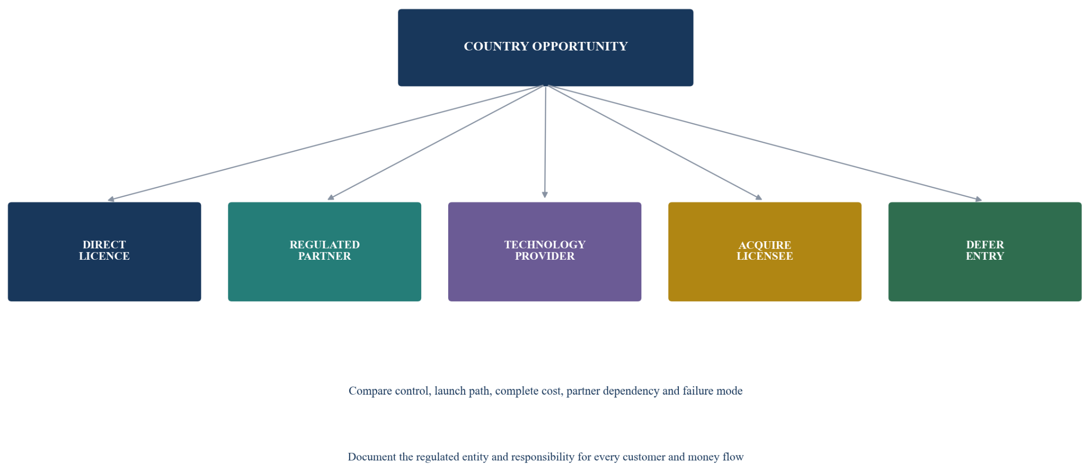
The company typically has five strategic routes: obtain a direct licence, operate through a regulated partner, provide technology without performing the regulated activity, acquire a licensed business or defer the market.

A direct licence offers control over customers, product, economics and regulatory relationship. It can require local substance, capital, governance, senior managers, policies, assurance, safeguarding and reporting. Time to launch depends on application readiness, regulator review, conditions, testing and operational certification.

A partner model can accelerate access when responsibilities are genuine and clearly documented. The licensed institution should control the regulated activity required by law. The fintech still needs contract management, outsourcing controls, customer disclosures, data governance, service resilience and an economic model that supports the partner's risk and compliance burden.

A technology-provider model narrows the activity to software or support. It needs rigorous perimeter discipline. Product features, money flows, customer communications or discretion can move the firm into regulated territory. Acquisition can provide an existing licence and operating platform; change-of-control approval, licence scope, legacy controls, capital and integration risk remain material.

Figure 3. Country market-entry architecture



Author framework. Each route should be tested against control, timing, fixed cost, economics and regulatory responsibility.

Table 3. Market-entry route comparison

Route	Strategic control	Cost and timing	Principal risk	Best-fit condition
Direct licence	high control over proposition and customer	higher fixed cost; regulator-led timetable	incomplete application, delayed conditions or weak local substance	market can support durable scale and regulated capability
Regulated partner	shared control through contract and oversight	potentially faster; revenue share and integration cost	partner concentration, approval, termination and role ambiguity	partner has genuine licence scope, appetite and operating capacity
Technology provider	control over software; limited regulated role	lower regulatory build when perimeter is maintained	product behaviour crosses into regulated activity	firm can deliver value without customer funds or regulated discretion
Acquire licensee	control after approval and integration	purchase price, diligence, change of control and remediation	licence scope, legacy liabilities and culture	target has relevant permission, clean controls and strategic fit
Defer entry	preserves capital and management capacity	opportunity cost; no immediate regulatory build	competitor advance	market economics do not clear the risk-adjusted hurdle

Relative assessments are directional and require company-specific evidence.

7. Build the complete regulatory cost stack

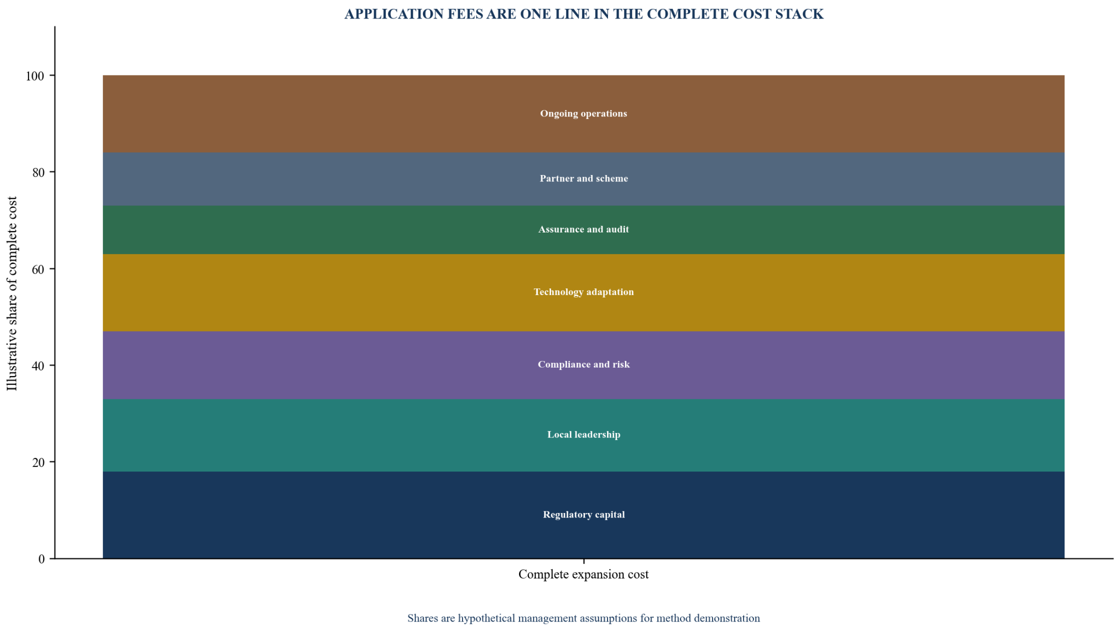
Application fees and minimum capital are only visible components. The expansion budget should include perimeter and legal work, entity establishment, governance, fit-and-proper assessment, local leadership, compliance, financial crime, safeguarding, risk, cyber security, data protection, audit, insurance, policies, regulator reporting, complaints, fraud operations, vendor assurance and continuing supervision.

Technology cost can be country-specific. Customer journeys, identity sources, consent language, data storage, payment connections, reconciliation, reporting taxonomies, complaint workflows and record retention may vary. Even when the product code is shared, evidence, configuration and assurance can be duplicated.

The board should separate three cost groups. Regional platform cost can support every country. Country fixed cost exists before scale. Variable cost follows customers or transactions. This separation makes the expansion hurdle visible and prevents regional overhead from hiding loss-making markets.

Regulatory capital also has an opportunity cost. It can be trapped in a local entity, unavailable for group product investment and subject to additional buffers or safeguarding arrangements. The model should reflect cash location and permitted use rather than counting all group cash as freely deployable.

Figure 4. Fintech regulatory expansion cost stack



Author framework. The complete stack includes capital, people, controls, technology, assurance and continuing operations.

8. Model one country without disguising assumptions

Consider a hypothetical fintech evaluating a new market. Management assumes an 18-month period from preparation through controlled scale, with regulatory and operating expenditure incurred before material customer revenue. Every amount below is a hypothetical management assumption and does not represent an observed licence cost, market quote or offer.

The model should distinguish cash expenditure, capital committed to the entity, non-cash central-team allocation and partner revenue share. Regulatory capital is not automatically an expense; it is cash constrained for a defined purpose and carries a funding cost. The cash model should show when it must be injected and whether it can be recovered after exit or licence surrender.

The base case should include delays. A licence decision can arrive after the original product window. Conditions can require hiring, system testing, policy changes or capital. Partner integration can follow regulatory approval. Customer acquisition should begin after the permitted launch point rather than on the application date.

Table 4. Hypothetical country expansion economics

Cost or outcome	Preparation months 1-6	Application months 7-12	Launch months 13-18	Downside implication
Legal, regulatory and entity	900	500	200	repeat work if scope or structure changes
Local leadership and control staff	650	1,350	1,650	key hires may precede revenue
Technology and integration	500	1,100	900	additional certification or localisation
Assurance, audit and insurance	150	450	550	remediation before launch or renewal
Regulatory capital injected	0	3,700	0	cash restricted in local entity
Commercial and customer operations	100	350	1,500	delayed launch raises acquisition cost
Hypothetical net revenue	0	0	1,800	lower adoption or partner capacity
Cumulative cash before capital recovery	(2,300)	(9,750)	(12,750)	funding need rises with delay and fixed cost

All amounts, durations and probabilities are hypothetical management assumptions; AED thousands unless stated.

9. Build a country variation register

A regional control framework should establish the strongest common baseline the group can operate consistently. Country overlays should then record the legal or operational reason for every variation. This approach supports governance without pretending that all obligations are identical.

The register should cover authorisation, legal entity, capital, governance, senior management, customer eligibility, onboarding, AML and sanctions, safeguarding, outsourcing, cloud, data location, cyber reporting, consent, disclosures, pricing, complaints, fraud reimbursement, record keeping, regulatory returns, audit and incident notification.

Each requirement needs a source, owner, implementation evidence, test and review date. Legal advice should be version-controlled. Regulator correspondence and application commitments should be converted into operational requirements. A licence condition has little value if it remains in an email and never reaches the product backlog or monthly control calendar.

Table 5. Country control-variation register

Control domain	Regional baseline	Country overlay	Evidence	Release gate
Legal entity and permission	approved group entity and activity map	domestic entity, branch, partner or exemption basis	licence, scope letter, register and counsel memorandum	contracting entity and permitted journey confirmed
Customer onboarding	identity, screening and risk-rating standard	local identity, data and enhanced-diligence rules	test cases, vendor assurance and audit trail	all customer types pass approved scenarios
Funds and safeguarding	complete funds-flow and reconciliation standard	local accounts, trust, segregation or safeguarding method	bank documents, ledger tests and reconciliation	no unexplained balances; access controls approved
Data and cloud	group classification, access, encryption and retention	local storage, transfer, consent and notification requirements	architecture, contracts, assessments and logs	security, privacy and regulatory approvals complete
Conduct and complaints	clear terms, fair outcomes and case management	local language, disclosures, time limits and reimbursement rules	approved content and case simulations	end-to-end complaint and fraud tests pass
Reporting and incidents	group control calendar and escalation	regulator templates, deadlines and notification triggers	dry runs, owners and board reporting	first three reporting cycles prepared before launch

Exact obligations and thresholds should be taken from current authoritative sources and approved advice.

10. Protect one product while managing local variants

Uncontrolled localisation creates cost, defects and inconsistent customer outcomes. Excessive standardisation can breach local requirements or produce an unusable service. The operating model needs a governed middle path.

The product architecture should separate the common engine from configuration. Common components can include ledger logic, identity orchestration, screening, transaction monitoring, consent records, reporting data and audit logging. Country configuration can include eligible customers, product availability, limits, disclosures, language, pricing, routing, data handling and complaint timelines.

Every country release should cite the requirement it implements and the test that proves it. A regulatory change should enter one central intake process, be assessed for every market, assigned to accountable owners and closed with evidence. The register should show which countries remain on an earlier product or control version.

This discipline also supports transaction diligence. An investor or buyer can trace market revenue to the licence, operating entity, partner, control version and continuing obligation that makes the revenue lawful and durable.

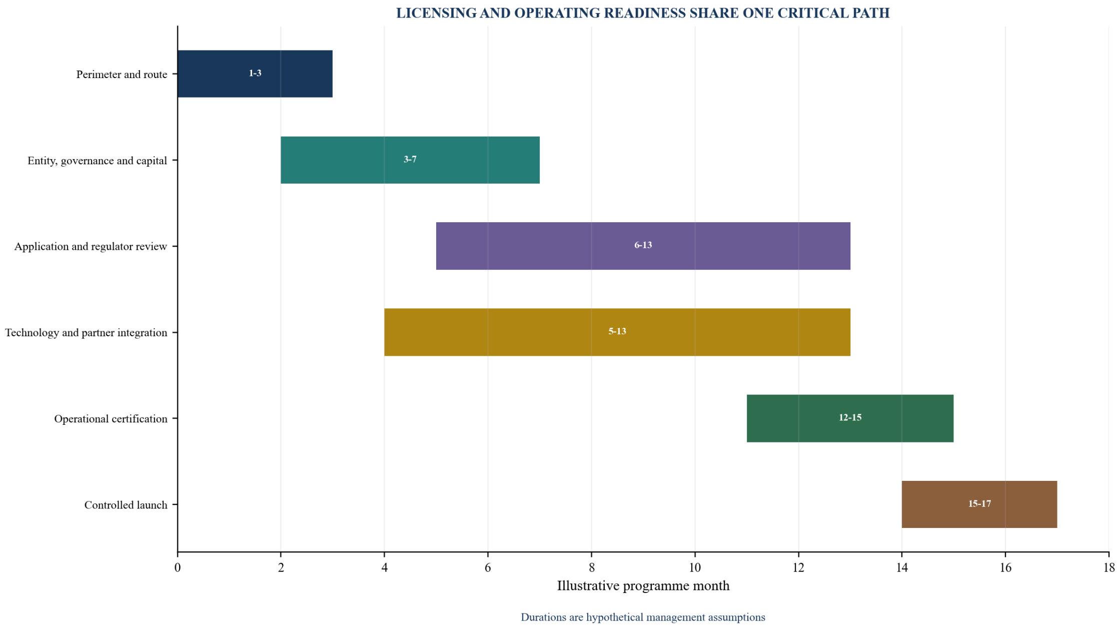
11. Sequence the application and operating build

The licensing plan should run as an integrated programme rather than a legal workstream separated from product and finance. Phase one confirms the activity perimeter and entry route. Phase two produces the business plan, governance, capital plan, policies, technology architecture, outsourcing map and financial model. Phase three manages submission, questions, interviews and conditions. Phase four completes operational testing and controlled launch.

Critical dependencies should be dated. A local chief executive, compliance officer, risk leader, auditor, bank account, safeguarding arrangement, insurance policy, office, cloud assessment or scheme certification can sit on the critical path. The project plan should reflect recruitment notice periods and third-party approvals.

Regulatory questions should update the operating model and budget. If the regulator expects a different entity, partner role, capital position or data architecture, management should rebaseline economics before continuing. Sunk application cost should not justify an unattractive market.

Figure 5. Regulatory expansion critical path



Author framework. Timings are illustrative; the real plan should use regulator, hiring, partner and technology evidence.

12. Fund expansion by evidence gates

The board should avoid releasing the entire country budget at approval. Capital can be committed in stages tied to evidence.

The first gate funds perimeter analysis and regulator engagement. The second funds the application after the entry route, entity, leadership, capital and operating model are credible. The third funds build-out after the application enters a defined process and critical conditions are understood. The fourth funds commercial scale after authorisation, certification and controlled-launch evidence.

Each gate needs a stop case. The company should pause when the permitted activity is too narrow, capital or localisation destroys returns, a partner cannot assume the required responsibility, regulator timing misses the strategic window or group management cannot operate the additional control burden.

Stage gates preserve option value. They allow management to reuse regulatory analysis and platform capabilities while containing market-specific loss.

13. Underwrite time as a capital variable

Regulatory time affects cash burn, hiring cost, product relevance and competitive position. It should be modelled as a probability distribution rather than a single launch date.

The base case can include management's best supported sequence. A moderate delay should extend local payroll, advisors, technology and partner retainers while deferring revenue. A structural delay should assume redesign or resubmission. Every duration remains a management assumption until supported by the regulator's actual process and the company's progress.

The financing plan should carry the downside without relying on immediate market revenue. If the group would need an equity round before a delayed country launch, the expansion decision is also a financing-risk decision.

14. Treat partner dependency as credit and control risk

A regulated partner can provide market access, safeguarding, settlement, customer accounts or regulated decision-making. The board should underwrite the partner's licence scope, financial capacity, compliance record, technology, service levels, customer appetite, change process, subcontractors and termination rights.

The responsibility matrix must follow actual conduct. It should allocate onboarding, sanctions screening, monitoring, customer communications, money handling, reconciliation, complaints, fraud, regulatory reporting, audit support and incident notification.

The fintech should model a partner exit. Customer migration can require consent, new accounts, revised terms, regulator engagement and technical work. Data portability and transaction records should be addressed before launch. A single-country partner can also limit regional standardisation if its architecture becomes embedded in the core product.

15. Build regulatory management information before launch

The country chief executive and group board need a monthly view of authorisation, capital, safeguarding, customers, transactions, complaints, fraud, financial crime, technology incidents, outsourcing, regulatory reporting and open remediation.

Definitions should match the licence and rules. A group measure may not satisfy a local regulatory return. Data lineage should connect each reported number to the system, owner, reconciliation and approval.

Management information should be tested before live customers arrive. Dry runs expose missing fields, inconsistent definitions and manual processes. The first regulatory deadline should not be the first time the company attempts to create the return.

16. Reconcile valuation with licence reality

Investors can assign a premium to regional addressable market and a scalable platform. The valuation case should distinguish markets that are live and authorised, markets with accepted applications, markets with signed regulated partners, markets under assessment and markets that are only strategic ambition.

Revenue multiples should reflect durability. Country revenue supported by a current licence, tested controls and diversified distribution differs from revenue dependent on one cancellable partner or an uncertain interpretation. Expansion investment should be reconciled to country contribution after local fixed cost and capital charge.

A regional total-addressable-market slide should therefore be paired with a permission-adjusted market map. It should show what the company can lawfully sell now, what it can sell after a defined gate and what remains outside the current plan.

17. Run a 180-day regulatory expansion programme

During the first thirty days, management should freeze the proposed product and complete the activity, customer, entity, funds, data and responsibility maps. It should obtain current country advice and identify regulator engagement routes.

During days 31 to 60, the team should compare direct licence, partner, technology-provider, acquisition and deferral routes. Finance should build the fixed, variable, capital and delay cases. The board should select one target market and route.

During days 61 to 120, the company should build the application evidence, governance, capital plan, policies, technology architecture, partner documents and implementation backlog. Country leaders and control owners should be appointed subject to applicable approval.

During days 121 to 180, management should submit or advance the formal process, answer regulator questions, test integrations, dry-run reporting and prepare the controlled-launch plan. The board should reapprove the country economics before the next capital tranche.

18. Diligence the expansion case

Investors and directors should test both permission and execution. The diligence room should contain current laws and rules, perimeter advice, regulator correspondence, application materials, licence and register evidence, entity documents, capital plan, senior-manager files, policies, funds flow, safeguarding, technology architecture, data map, outsourcing register, partner contracts, testing, reporting and remediation.

Documents should reconcile. The business plan, application, investor deck, financial model and product backlog should describe the same activities, entity, customer, funds flow and launch timetable. A mismatch can indicate scope drift or weak governance.

Table 6. Regulatory expansion diligence plan

Workstream	Core evidence	Principal question	Escalation trigger
Perimeter	activity map, advice and regulator communication	is every proposed activity permitted through the chosen route?	unresolved or changing legal interpretation
Licence and entity	application, conditions, register and corporate records	does the entity hold the right represented to customers and investors?	scope gap, condition overdue or unapproved change
Capital and finance	capital rule, bank evidence, forecast and downside	can the entity remain compliant through a delay?	forecast buffer below board threshold
Customer and funds	journeys, terms, accounts, safeguarding and reconciliation	are customers and money handled by the correct entity?	unexplained money, disclosure gap or partner-role drift
Technology and data	architecture, testing, access, security and privacy evidence	does the deployed system match approved design and local requirements?	critical defect, unauthorised transfer or overdue remediation
Operations and reporting	policies, people, MI, returns, complaints and incidents	can the firm operate the licence continuously?	missed report, control failure or repeated manual override

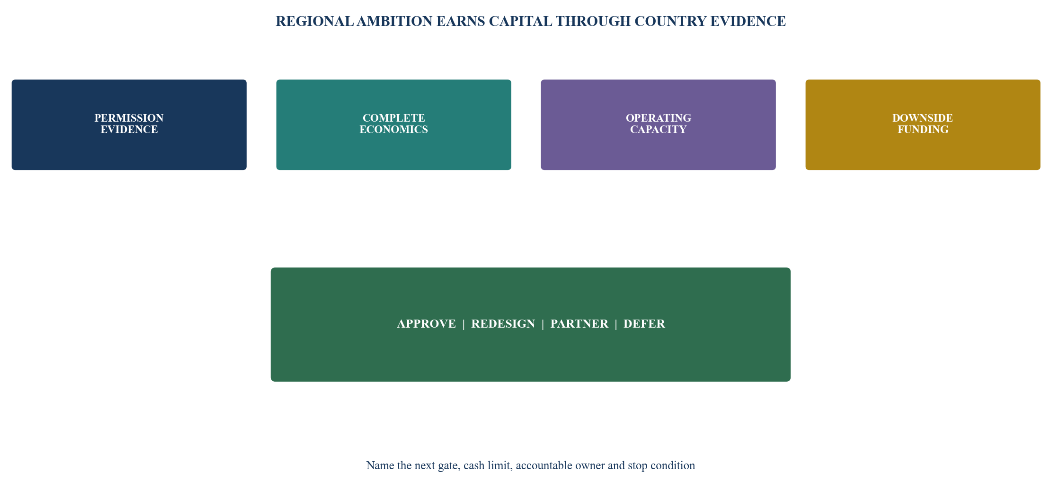
The board should assign an evidence owner and ageing threshold to every workstream.

19. Use a board gate that can reject expansion

The board paper should state the market objective, activity perimeter, entry route, licence path, capital, people, partners, technology change, complete cost, launch timetable, downside and stop case.

Approval should require evidence that the firm can obtain and operate the permission, finance the delay case, maintain customer protection and produce an attractive country contribution after local fixed cost and capital charge.

Figure 6. GCC regulatory expansion board gate



Author framework. Expansion proceeds only when permission, economics, operating capacity and downside resilience align.

20. Recognise what can become regional

Country-specific licensing does not prevent regional scale. It changes how scale is built. A company can reuse product components, policies, data models, control evidence, vendor diligence, financial models and regulatory programme management across markets.

Regional infrastructure such as AFAQ can improve the movement and settlement layer for eligible participants. Common API and security standards can reduce technical fragmentation. Supervisory cooperation can improve consistency over time. These benefits should be underwritten from official scope and actual access.

The valuable capability is regulatory repeatability: a disciplined system that identifies the perimeter, selects an entry route, builds evidence, manages local variants, operates the licence and measures country economics. That capability can reduce the marginal cost and risk of each subsequent market while respecting domestic authority.

Conclusion

The Gulf is developing connected payment and data infrastructure alongside country-specific fintech regimes. The expansion plan should reflect both developments.

A genuine passport requires a legal basis, scoped cross-border rights, a home-host process, supervisory cooperation and registration. In its absence, management should model domestic licensing or another permitted entry structure in every target market.

The complete cost includes capital, local leadership, controls, technology variants, assurance, partners, reporting and the cash burn created by regulatory time. A regional platform can share core capabilities while country overlays govern the differences.

The board should release capital through evidence gates and retain the authority to redesign, partner, defer or reject a market. Regional scale becomes credible when each country proposition is lawful, operationally controlled and economically attractive.

References

[1] Gulf Payments Company, AFAQ services and business model, https://www.gulf-payments.com/en/our-services/

[2] Gulf Payments Company, AFAQ FAQs and participant requirements, https://www.gulf-payments.com/en/faqs/

[3] European Banking Authority, Payment services and electronic money, including technical standards on passporting under PSD2, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money

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

[5] Central Bank of the UAE, Retail Payment Services and Card Schemes Regulation, https://rulebook.centralbank.ae/en/rulebook/312-retail-payment-services-and-card-schemes-regulation

[6] Saudi Central Bank, Implementing Regulations of Payments and Payment Services Law, https://rulebook.sama.gov.sa/en/implementing-regulations-payments-and-payment-services-law

[7] 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

[8] Central Bank of Bahrain, Payment Service Requirements, Volume 5, February 2026, https://www.cbb.gov.bh/wp-content/uploads/2026/02/Volume-5_PSP-Module_5-Feb-26.pdf

[9] Qatar Central Bank, Payment Services Regulation, https://www.qcb.gov.qa/Services/Financial%20Technology/PSR%20Final%20-%20English.pdf

[10] Central Bank of Kuwait, Regulatory instructions for electronic payment services, https://www.cbk.gov.kw/en/supervision/cbk-regulations-and-instructions/regulatory-instructions-e-Payment-services

[11] Central Bank of Oman, Fintech Regulatory Sandbox and payment-service-provider licensing evidence, https://cbo.gov.om/pages/FRSForm.aspx

[12] Central Bank of Oman, Open Banking Regulatory Framework, https://cbo.gov.om/sites/assets/Documents/CC/Open%20Banking%20Regulatory%20Framework_Oman.pdf

[13] Saudi Central Bank, Operating Rules for Cross Currency Payments using AFAQ Service, https://rulebook.sama.gov.sa/en/operating-rules-cross-currency-payments-using-afaq-service

[14] Central Bank of the UAE, AFAQ GCC RTGS, https://www.centralbank.ae/en/our-operations/payments-and-settlements/afaq-gcc-rtgs

About the Author

Chennakeshav Adya is an independent researcher and Managing Partner of Matchpoint Partners. His work examines strategy, capital formation, valuation, transactions and operating execution across private and public markets.