GCC Post Quantum Security Platforms Sovereign Demand and Regional Scale

A Commercial Diligence M&A and Valuation Framework for National Capability Procurement Product Control and Cross Border Growth

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Post-quantum security is becoming a national capability question across the Gulf. Final cryptographic standards, government cyber strategies, encryption policy, critical-infrastructure obligations and long-lived sensitive data are moving the issue from research into procurement. The United Arab Emirates provides the clearest regional signal: its National Encryption Policy expressly addresses post-quantum cryptography, official communications require government entities to develop approved migration plans, and national institutions have announced deployment and scale programmes for discovery, cryptographic libraries and testing. Wider GCC strategy strengthens the regional direction, while Saudi Arabia, Qatar, Bahrain, Kuwait and Oman each bring distinct cryptographic, cloud, data-protection, cybersecurity and national-capability requirements. These adjacent frameworks do not amount to one uniform GCC post-quantum mandate.

This paper develops a commercial diligence, M&A and valuation framework for GCC post-quantum security platforms. It asks whether a vendor can convert national sponsorship and policy relevance into funded procurement, accredited products, accepted deployments, recurring support and collected cash. It separates sovereign demand from ordinary pipeline, and national control from mere local presence. It examines cryptographic discovery, migration planning, hybrid deployment, product assurance, source and build control, data residency, key management, security operations, local talent, systems integration, partner governance and customer acceptance.

The central analytical problem is regional repeatability. A platform can be strategically important in one country while remaining commercially non-portable elsewhere. Government sponsorship, a pilot, a laboratory agreement or participation in a national programme can establish capability and access. Regional scale requires separate evidence: legal permission, procurement ownership, country accreditation, product interoperability, delivery capacity, local operating control, customer referenceability, contract economics and renewal. An acquirer should therefore value country rights and revenue cohorts individually before attributing a regional platform premium.

A wholly hypothetical case illustrates the framework. The central three-market case assumes USD 106.00 million of annual revenue, USD 54.00 million of direct product, delivery and support cost, and USD 52.00 million of contribution before central overhead. A sponsored-pilot case assumes USD 36.00 million of revenue and USD 8.00 million of contribution. A scaled six-market platform case assumes USD 226.00 million of revenue and USD 126.00 million of contribution. A separate probability-weighted illustration produces an enterprise value of USD 677.50 million. All amounts are management assumptions for demonstrating the framework; they are not market observations, forecasts or valuation conclusions.

The paper concludes that sovereign relevance can support access, technical depth and durable customer relationships, while acquisition value depends on evidence that survives beyond a single sponsor or programme. The strongest platform has controlled technology, verified national delivery, reusable

product architecture, auditable partner boundaries, country-specific permissions, measurable cohort economics and a disciplined route from discovery to recurring assurance. Transaction consideration should follow those evidence states, with deferred value tied to accredited releases, accepted deployments, contribution, collections, renewals and successful entry into additional GCC markets.

JEL Classification: G24, G34, H56, L86, O31, O33

Keywords: GCC cybersecurity, post-quantum cryptography, sovereign technology, cybersecurity M&A, national procurement, cryptographic agility, regional platforms, technology valuation

Introduction

Public-key cryptography protects identity, key exchange, code signing, software updates, financial messages, government communications and critical infrastructure. A sufficiently capable quantum computer could undermine widely used public-key algorithms, although the timing and engineering path remain uncertain. The immediate business problem comes from long migration cycles and the possibility that encrypted information collected today may be decrypted later. Organisations must discover cryptographic dependencies, prioritise long-lived data and replace vulnerable mechanisms without disrupting essential services.

NIST finalised FIPS 203, FIPS 204 and FIPS 205 in 2024 [1-4]. Its subsequent programme covers implementation guidance, algorithm validation and cryptographic agility [5-8]. IETF publications now define hybrid terminology and mechanisms for TLS and SSH [9-12]. These developments give governments and buyers a stable technical basis for planning. They do not prove that a vendor can provide an accepted sovereign platform or reproduce a successful deployment across countries.

GCC demand must be examined through national institutions. The UAE approved a National Cybersecurity Strategy in 2025 and maintains a National Encryption Policy that covers data at rest, data in motion, key management, post-quantum cryptography and implementation controls [13,14]. Official announcements describe approved migration planning and national deployment activity [15-17]. Saudi Arabia publishes national cryptographic standards with post-quantum material and cybersecurity controls [22-26]. Qatar, Bahrain, Kuwait and Oman publish national strategies or adjacent cryptographic, cloud, data and capability frameworks [27-38]. The GCC Secretariat has adopted a regional cybersecurity strategy and cooperation mechanisms [19-21].

This paper treats those instruments as demand and governance signals. It does not treat them as interchangeable mandates or guaranteed revenue. The transaction question is whether a target converts relevant national need into controlled product, accepted deployment, contribution and repeatable regional growth.

1 Define sovereign demand as an evidence chain

Sovereign demand begins with an accountable public purpose. A government may need to protect classified information, citizen data, digital identity, financial infrastructure, energy systems, defence networks or long-lived public records. Policy can identify the obligation. A programme owner must translate the obligation into scope, funding, procurement, acceptance and operations. A vendor's position in that chain determines the commercial quality of its demand.

The evidence ladder should distinguish policy relevance, sponsorship, funded assessment, product qualification, production order, operational acceptance, invoice, collection and renewal. A policy citation supports strategic context. A ministerial or agency announcement can support institutional sponsorship. A signed contract identifies legal scope. A purchase order, acceptance certificate and bank receipt support commercial conversion. A renewal or extension shows that the customer continues to value the service.

Acquirers should reconstruct this ladder for every material programme. The record should name the contracting entity, budget owner, procurement route, security classification, delivery boundary, acceptance authority, source of funds, contract term and termination rights. Framework ceilings, memoranda of understanding, laboratory collaborations and unpaid demonstrations should remain separate from contracted backlog.

National sponsorship can still be valuable before revenue. It can provide access to systems, test environments, policy makers and demanding use cases. The valuation response should match the evidence state. Strategic access can support option value. It should not be modelled as recurring revenue until enforceable scope, accepted delivery and collection exist.

2 Translate the UAE mandate into addressable work

The UAE provides a structured post-quantum migration signal. The National Encryption Policy addresses cryptographic controls, key management and post-quantum considerations [14]. Official reporting states that government entities are required to develop approved migration plans [15]. The UAE Cyber Security Council and Advanced Technology Research Council have announced programmes involving a Crypto Discovery Tool, post-quantum libraries, enhanced quantum key distribution and a national laboratory path [16,17]. Dubai's electronic-security authority has also published post-quantum guidance [18].

These signals can create multiple procurement layers. Discovery tools identify algorithms, protocols, certificates, keys and dependencies. Advisory work prioritises data and systems. Product engineering implements hybrid or post-quantum mechanisms. Testing measures interoperability and performance. Assurance supports acceptance. Managed services monitor cryptographic posture, expiry, fallback and migration progress. Training and operating-model work develop local capability.

A target should map its revenue to these layers. Discovery revenue can be episodic unless the product maintains a living inventory. Migration projects can be large while requiring intensive specialists. Libraries can create strategic control but may carry limited direct revenue. Appliances and platforms can create licence, maintenance and support income. National laboratories and accreditation may strengthen assurance while extending the time to commercial acceptance.

The buyer should test whether the target owns a reusable product or provides programme labour. Both can be valuable, yet their economics differ. Reusable connectors, rules, test suites, policy mapping, reporting and deployment automation support scale. Senior engineers performing bespoke discovery and migration create capacity constraints. The transaction model should price the actual operating system behind the national promise.

3 Separate national control from local presence

Sovereign customers can require local data handling, approved personnel, national operations, source access, key control, continuity and authority during incidents. A local office or reseller does not establish those capabilities. Diligence should define the required control state for each product and customer.

Technology control has several levels. A customer may have the right to use a product, observe its operation, diagnose faults, modify source, reproduce a build, operate independently and maintain continuity after supplier failure. These rights are cumulative only when contracts, technical access, people and tooling align. Source escrow without a reproducible build can provide little continuity. A local operations centre without authority over releases can remain dependent on a foreign engineering team.

The target should produce a control matrix covering source, build, signing keys, cryptographic modules, cloud tenancy, telemetry, vulnerability response, data, support, suppliers and disaster recovery. Each row should name legal ownership, physical location, technical operator, approval authority, recovery route and evidence date. Customer commitments should reconcile to the target's actual rights.

An acquirer may strengthen control through local build infrastructure, restricted repositories, national key custody, trained operations, duplicate suppliers and documented disengagement tests. These investments can support qualification and retention. They also create cost, governance and export-control questions that must enter valuation.

4 Build the cryptographic inventory before underwriting scale

A post-quantum platform needs visibility into customer cryptography. The inventory should cover applications, networks, endpoints, certificates, public-key infrastructure, code signing, software updates, hardware security modules, cloud services, identity, databases, backups, operational technology and supplier connections. It should identify algorithms, protocol versions, key lengths, libraries, firmware, ownership, data lifetime and remediation dependencies.

Automated discovery can improve coverage, yet every tool has boundaries. Encrypted traffic, embedded devices, proprietary protocols, dormant applications and supplier-managed systems can escape scanning. Diligence should test the product in an environment with known ground truth and reconcile discovered records to configuration, certificate and asset sources. False negatives create hidden migration exposure. False positives consume scarce programme resources.

The commercial test is maintainability. A one-time report may support an assessment project. A continuously updated inventory can support recurring software or managed assurance. The target should show connectors, refresh frequency, change detection, exception handling, ownership workflow and evidence retention. It should explain how new algorithms, protocols and supplier versions enter the ruleset.

Country scale requires adaptable policy mapping. The underlying technical inventory can be common while classification, reporting, residency, approval and retention rules differ by customer and jurisdiction. A strong platform separates the reusable technical core from configurable national controls.

5 Prove product and protocol interoperability

Standards conformance is necessary and incomplete. Production systems depend on clients, servers, gateways, hardware, operating systems, cloud services, certificate chains, network paths and operational procedures. A target can implement a final algorithm correctly while a deployment fails because message sizes, fragmentation, latency, memory, firmware or middleboxes are incompatible.

The test matrix should specify algorithm, parameter set, protocol, RFC, implementation, product release, hardware boundary and validation status. It should cover negotiation, authentication, fallback, downgrade resistance, session resumption, observability, rollback and failure recovery. Hybrid modes require exact identification of both components and their composition [9-12]. Proprietary combinations can create temporary utility and future rework.

Regional scale depends on repeatable test evidence. A national customer may approve a specific architecture, release and supplier combination. Another country may use different identity, network, cloud, HSM and accreditation systems. The target should maintain reusable harnesses and country-specific acceptance profiles rather than claiming that one pilot proves GCC compatibility.

Strong evidence includes version-controlled test cases, independent implementations, customer-representative environments, defect histories, regression results and signed production acceptance. Commercial claims should remain within that evidence boundary.

6 Design cryptographic agility as an operating capability

Cryptographic migration will continue after the first post-quantum deployment. Algorithms can be revised, implementations can fail, protocols can evolve and customer priorities can change. NIST treats

cryptographic agility as the ability to replace and adapt cryptographic mechanisms without unacceptable disruption [7,8]. A regional platform should demonstrate that capability in architecture and operations.

The target should separate algorithm choice from business logic, maintain versioned interfaces, automate inventory and policy decisions, support multiple providers and preserve rollback. It should track where cryptography is compiled into software, configured in infrastructure or embedded in hardware. Update mechanisms and code signing must remain trustworthy throughout migration.

Agility also has commercial value. Customers may buy continuing assurance when the platform monitors posture, identifies affected assets, tests new releases and manages exceptions. This creates a recurring service beyond initial migration. The buyer should verify that the product reduces repeat effort and that contracts allocate change responsibility.

A claim of agility needs evidence from controlled replacement exercises. Diligence should inspect the time, people, defects, downtime and customer approvals required to change an algorithm or provider. Architecture diagrams alone do not establish operational agility.

7 Compare GCC country entry conditions

The GCC provides strategic alignment and cooperation, including a regional cybersecurity strategy and information-sharing mechanisms [19-21]. Commercial entry remains national. Each country has its own authorities, procurement systems, cloud and data rules, critical-infrastructure relationships, national champions and supplier expectations.

Saudi Arabia publishes National Cryptographic Standards and sector-wide cybersecurity controls [22-26]. Qatar's national strategy, assurance standard and cryptographic standard establish a structured control environment [27-30]. Bahrain's strategy emphasises resilience, governance, partnerships, workforce and local innovation [32,33]. Kuwait's cloud and data-classification frameworks shape hosting and information handling [35,36]. Oman's programme emphasises cybersecurity industry and capability development [37,38]. These instruments support diligence questions; they do not prove specific post-quantum procurement.

The market-entry file for each country should identify authority, regulated sectors, data classification, hosting, cryptographic approval, supplier registration, local-content expectations, contracting route, dispute terms, payment history and referenceability. It should also identify whether a local partner is mandatory, commercially useful or unnecessary.

Country sequencing should follow evidence. A platform with an accepted UAE deployment may choose Saudi Arabia for scale, Qatar for concentrated infrastructure demand, or smaller markets for focused references. The decision should compare accessible customers, qualification burden, delivery capacity and contribution rather than relying on population or headline technology spending.

8 Diligence local partners and national champions

Local partners can provide market access, customer trust, registration, Arabic delivery, security-cleared staff, facilities and operating continuity. They can also obscure customer ownership, reduce contribution, weaken data control and create dependency. The acquirer should examine each relationship at contract and operating level.

The partner register should state legal entity, owners, role, territory, exclusivity, customers, opportunity ownership, revenue share, service obligations, data access, intellectual-property rights, personnel approval, audit, subcontracting, liability, termination and transition. Memoranda and broad alliance announcements should remain outside committed distribution value.

Customer contracts should align with partner contracts. The platform should not promise response times, source access or national operations that the partner is not obliged or able to provide. Cash collection should reconcile from end customer through partner deductions to the target's bank account. A high reported booking can have weak economics after commissions, local delivery and delayed payment.

Regional scale improves when partner interfaces are standardised. Training, certification, reference architectures, secure support channels, quality reviews and common commercial rules can make country delivery more repeatable. The acquirer should still retain direct visibility into customer acceptance and risk.

9 Measure sovereign procurement quality

Government and critical-infrastructure procurement can create durable contracts and demanding reference customers. It can also involve long qualification, budget cycles, performance guarantees, local-content commitments, security restrictions and payment milestones. Revenue quality depends on the precise instrument.

The diligence team should distinguish policy allocation, approved budget, tender, framework, call-off, task order, prototype, grant, subscription, licence, maintenance and managed service. A framework ceiling is not backlog. A funded pilot is not a production rollout. A research award is not recurring customer revenue. Each item should have an enforceable amount, term, acceptance criteria and payment route.

Bid economics require full cost. Direct cost can include presales engineering, bid bonds, performance bonds, local staff, secure facilities, hardware, cloud, laboratories, assurance, customer-specific integration, travel, support and warranty. Delayed acceptance can consume working capital. Currency and tax may affect country contribution.

The buyer should analyse procurement cohorts from tender to collection. Useful measures include qualification duration, bid conversion, contract-to-acceptance time, acceptance-to-cash time, change orders, support effort, gross contribution and renewal. These measures show whether sovereign demand can become an investable platform.

10 Reconcile product economics to delivery reality

Headline software margin can misstate post-quantum platform economics. The customer buys an accepted security outcome. Direct cost therefore includes the product, infrastructure, cryptographic modules, test environments, partner share, customer engineering, accreditation, vulnerability response and ongoing support required to deliver that outcome.

The central hypothetical case assumes USD 106.00 million of revenue. UAE sovereign and critical-infrastructure programmes contribute USD 42.00 million of revenue and USD 24.00 million of contribution. Saudi regulated and national programmes contribute USD 36.00 million and USD 18.00 million. Qatar contributes USD 13.00 million and USD 5.00 million. Bahrain, Oman and Kuwait together contribute USD 15.00 million and USD 5.00 million. Direct cost totals USD 54.00 million, leaving USD 52.00 million before central overhead. These values are management assumptions.

The sponsored-pilot case assumes USD 36.00 million of revenue and USD 8.00 million of contribution. Bespoke integration, laboratories, senior engineers and partner costs consume most of the gross value. The scaled six-market case assumes USD 226.00 million of revenue and USD 126.00 million of contribution after product reuse, accredited releases, trained partners and recurring assurance improve unit economics. Neither case is a forecast.

The acquirer should reconcile contribution by customer, product version, country and deployment stage. Central engineering and national delivery costs should be allocated transparently. A profitable national programme should not hide loss-making regional expansion.

11 Test revenue cohorts and repeatability

Revenue cohorts should follow customers from initial discovery through recurring operation. A useful sequence is paid inventory, migration architecture, product qualification, production deployment, managed assurance and renewal or expansion. Each transition requires evidence and consumes time and capacity.

The buyer should measure the proportion of customers that advance, the duration between stages, the direct cost at each stage and the reasons for loss or delay. Cohorts should be segmented by country, sector, product and procurement type. Government pilots can behave differently from bank or telecom programmes. A platform may have strong technical conversion and weak procurement conversion.

Repeatability exists when new customers use substantially the same product, test assets, delivery method and support model. Bespoke configuration can remain necessary, particularly for sovereign systems, yet the reusable core should increase. Engineering hours per accepted asset, defect recurrence, partner effort and time to accreditation should improve across cohorts.

Renewal is the final commercial test. Managed inventory, assurance, update and support can produce continuing value. The contract, usage, invoice, cash and service cost should reconcile. A renewal described as strategic without collected revenue provides limited valuation evidence.

12 Assess intellectual property and supply dependencies

Platform value can reside in cryptographic libraries, discovery logic, policy rules, test suites, migration automation, secure build systems, integration methods, customer configurations and specialist knowledge. Diligence should link each asset to the product or delivery step it supports.

Ownership analysis should cover founders, employees, contractors, universities, public research programmes, customers and open-source licences. Government-funded development may carry rights or restrictions. Customer contracts may allocate bespoke deliverables. Open-source components can accelerate assurance and interoperability while imposing notice, redistribution or patent obligations.

The software bill of materials should reconcile to released products. Cryptographic libraries, compilers, hardware, HSMs, cloud services and third-party scanners should have owners, versions, support status and substitutes. Supplier discontinuation or licensing changes can affect national commitments.

An acquirer should reproduce the product from controlled source, verify signing and release, restore critical environments and test supplier substitution. Legal ownership without practical build and operational control provides incomplete protection.

13 Protect specialist talent and national capability

Post-quantum delivery requires cryptography, secure software, networks, PKI, embedded systems, hardware, cloud, operational technology, assurance and programme management. Scarcity can make a small number of specialists the principal asset. Diligence should identify actual technical authority through code history, design decisions, customer records and incident response.

Each critical capability should have at least two accountable people, maintained documentation and a succession route. Security clearance, nationality, location and customer approval may limit where individuals can work. Contractors and academic relationships can provide depth while creating continuity and rights exposure.

National capability commitments should be measurable. Training numbers alone provide little evidence. Useful measures include independently operated deployments, local release authority, local incident response, reproducible builds, accredited staff, supported customer environments and documented knowledge transfer.

Retention design should preserve technical authority, research, customer trust and secure-development discipline. The first hundred days should avoid a sales-led integration that removes specialists from delivery or weakens national controls.

14 Examine security liability and claim boundaries

A post-quantum vendor can affect confidentiality, authentication, availability and software trust. A missed cryptographic dependency can leave exposure. A failed change can interrupt critical services. A flawed implementation can introduce vulnerability. Contract and insurance review should match this risk.

The data room should include warranties, indemnities, liability caps, service levels, security schedules, incident terms, professional-indemnity and cyber cover, claims and near misses. Broad promises that a system is quantum-safe should be mapped to product, version, algorithm, protocol, cryptographic boundary and validation evidence.

The target's own controls require equal scrutiny. Repositories, build systems, signing keys, secrets, privileged access, support channels, customer architecture and vulnerability reports can be high-value targets. Secure development, separation of duties, monitored access, incident response and recovery should be evidenced through records and tests.

Transaction documents should allocate known exposures and unresolved commitments. Escrow, holdback, specific indemnity or remediation covenants may be appropriate where evidence supports them. Future marketing claims should require technical and legal approval.

15 Value national sponsorship and regional options separately

Valuation should separate current operating cash, national capability assets and regional options. Current cash value comes from accepted products and services with measurable contribution. Capability value can include controlled technology, accredited facilities, specialist teams and trusted customer access. Regional option value depends on additional country permissions, customers, delivery capacity and repeatability.

The hypothetical evidence-state model uses four scenarios. A local capability state has enterprise value of USD 140.00 million and a 20 per cent probability, producing USD 28.00 million of weighted value. An accredited national product state has enterprise value of USD 420.00 million and a 35 per cent probability, producing USD 147.00 million. A repeatable three-market platform has enterprise value of USD 900.00 million and a 30 per cent probability, producing USD 270.00 million. A scaled six-market platform has enterprise value of USD 1,550.00 million and a 15 per cent probability, producing USD 232.50 million. Total weighted value is USD 677.50 million. These are wholly hypothetical management assumptions.

Probabilities should be replaced with transaction-specific evidence. The model demonstrates how value moves when accreditation, customer acceptance, country entry and contribution are proven. It does not select a purchase price.

Consideration can follow the same structure. Base value can pay for verified current capability and cash flows. Deferred consideration can depend on accredited releases, production acceptance, contribution, collections, renewals and entry into named markets.

16 Structure the acquisition around evidence gates

The acquisition agreement should convert diligence findings into conditions, price mechanics and post-close measures. Rights and build control can be closing conditions. Customer and regulatory consents can protect continuity. Working-capital mechanisms can address delayed sovereign collections. Specific indemnities can address identified claims or licence issues.

Earn-outs should use measures the combined company can control and audit. Accepted revenue, collected cash and contribution can be stronger than bookings. Product milestones require exact releases, test environments and acceptance authorities. Country-entry milestones should identify legal permission, signed customer scope and collection rather than an office opening or partner agreement.

Management incentives should balance growth and control. A target rewarded only for revenue may accept bespoke commitments that weaken margins and product focus. Measures can include contribution, customer acceptance, recurring revenue, product reuse, security performance and staff retention.

The integration plan should preserve national commitments. Source, data, keys, support, staff and incident authority may need controlled separation. The acquirer should document which functions integrate immediately and which remain ring-fenced pending customer or authority approval.

17 Execute the first hundred days

Days one to fifteen should protect customer and national continuity. The buyer should confirm contracts, support ownership, signing authority, repositories, build systems, keys, facilities, critical staff, live incidents and customer communications. No material control should move without an approved transition.

Days sixteen to thirty-five should reconcile the evidence base. Teams should validate country pipeline, backlog, acceptance, invoices, collections, partner deductions, delivery capacity, product versions, claim boundaries and direct cost. The valuation model should be updated with verified information.

Days thirty-six to sixty-five should stabilise product and partner governance. The combined company should approve the architecture, release process, vulnerability handling, test matrix, partner certification, support boundaries and country entry criteria. Priority hiring and retention should close named capability gaps.

Days sixty-six to one hundred should establish scale gates. Each proposed market should have an authority map, customer thesis, procurement route, product fit, partner decision, delivery plan, economics and stop rule. Expansion capital should release only when those conditions are evidenced.

18 Investment committee decision framework

The investment committee should answer five questions. First, does the target control technology and delivery required by its national commitments. Second, has sovereign relevance converted into funded and accepted customer outcomes. Third, are product and contribution economics visible after all delivery costs. Fourth, can the operating model satisfy distinct national requirements without rebuilding the business in every market. Fifth, can the buyer protect trust while integrating and scaling.

Approval should identify evidence gaps and their transaction response. Missing rights can become a condition. Uncertain pipeline can remain outside base value. Concentrated talent can require retention and succession. Bespoke delivery can limit the multiple or require product investment. Country options can move into deferred consideration.

The strongest acquisition case combines national trust with commercial discipline. Policy and sponsorship create access. Controlled technology and accredited delivery create capability. Accepted products, contribution and collections create operating value. Repetition across countries creates a regional platform.

This sequence provides a defensible basis for M&A. It allows a buyer to support strategically important capability while keeping valuation aligned with evidence.

19 Govern the platform through measurable outcomes

Post-close governance should preserve a direct line from national obligation to customer outcome. The board should receive a country dashboard covering policy changes, procurement stage, contracted value, delivery status, acceptance, invoice, collection, direct cost, contribution, partner exposure, security events and renewal. Aggregate pipeline figures should be supported by the underlying programme records. The dashboard should show where management judgment or customer confirmation remains outstanding.

Product governance should maintain one approved claims register. Every statement about post-quantum capability should identify the product and release, algorithm, protocol, operating mode, cryptographic boundary, validation status, test environment and known limitations. Product, sales, legal and security teams should approve material changes. Customer-facing documentation should be revised when standards, implementations or dependencies change.

Country expansion requires a separate capital gate. Management should present the named authority, target customers, permission path, delivery model, partner terms, twelve-month cost, downside case and stop criteria. The board should approve funding in stages. Early expenditure can validate the market and product fit. Larger commitments should follow signed scope, accepted delivery evidence and a credible contribution path.

The operating scorecard should include inventory coverage, time to classify dependencies, percentage of migrations using an approved reusable pattern, test pass rate, defects escaping into production, time to acceptance, engineering hours per accepted asset, partner quality, security response, cash collection and renewal. These measures connect technical control to commercial performance. They also reveal whether growth is increasing reuse or creating a collection of bespoke national projects.

Independent assurance can strengthen confidence where evidence is safety-critical or highly specialised. Qualified cryptographers, security assessors, legal advisers and local regulatory counsel should examine matters within their competence. Their work should be scoped to specific systems, claims and jurisdictions. A transaction team should preserve the distinction between independent validation, management representation and public-source context.

Regional scale is achieved through disciplined repetition. The platform learns from one accepted deployment, converts the learning into controlled product and operating assets, and then qualifies those assets within the next country's requirements. Governance should reward that learning cycle. It should stop expansion when permissions, customers, product evidence, delivery capacity or contribution do not support further capital.

Frequently asked questions

Does a national post quantum policy create vendor revenue

It creates direction and can create procurement demand. Vendor revenue requires a funded buyer, defined scope, contract, accepted delivery, invoice and collection. The diligence file should preserve each step.

Is the GCC one post quantum security market

The region has shared cybersecurity direction and cooperation. Procurement, regulation, accreditation, data rules, customer institutions and partner structures remain national. Each country requires a separate entry case.

What is the strongest evidence of sovereign demand

A production contract with an accountable public or regulated customer, signed acceptance, collected cash and renewal provides stronger commercial evidence than policy, sponsorship, a memorandum or an unpaid pilot.

How should an acquirer value national sponsorship

Value should follow the capability and access that sponsorship demonstrably creates. Future revenue should remain contingent until funded procurement and customer acceptance are evidenced.

What makes a platform regionally repeatable

The platform needs a reusable technical core, configurable national controls, controlled partners, accepted product releases, country permissions, sufficient delivery capacity and improving contribution across customer cohorts.

Why is local presence insufficient for sovereign control

Sovereign control can require source, build, key, data, release, incident, recovery and continuity authority. An office or reseller may provide none of those technical and legal rights.

What transaction structure suits uncertain regional scale

Base consideration can reflect verified current capability and cash flows. Deferred consideration can depend on accredited products, accepted deployments, contribution, collections, renewals and named country-entry milestones.

What should happen during the first hundred days

The buyer should first protect national controls and customer continuity, then reconcile product and economic evidence, stabilise partner and delivery governance, and finally approve country expansion through explicit scale gates.

Appendix A. Sovereign demand evidence register

For every material programme, record the public purpose, policy source, programme owner, contracting entity, procurement route, approved budget, signed scope, security boundary, acceptance authority, delivery status, invoice, collection and renewal. Attach dated evidence and identify the person responsible for updating it.

Classify each item as policy signal, sponsored activity, funded qualification, production deployment or recurring operation. Keep grants, research collaborations, frameworks and commercial contracts separate. Reconcile the register to the CRM, contract ledger, invoices and bank receipts.

Appendix B. Country entry dossier

Prepare a dossier for each GCC country covering cyber and cryptographic authorities, regulated sectors, data classification, hosting, product approval, supplier registration, local-content requirements, government procurement, national partners, tax, currency, dispute terms and payment practice. Identify facts that require local legal or regulatory advice.

Add a customer-level market map, named procurement routes, delivery resources, partner alternatives, twelve-month cost, contribution case and stop criteria. Update the dossier before every material commitment.

Appendix C. Product control test

Select one production release and reproduce it from controlled source in an approved environment. Verify dependencies, compilers, build instructions, artefact hashes, signing, deployment, monitoring, rollback and recovery. Confirm that the people and permissions needed for continuity are available in the required jurisdiction.

Repeat the test for a cryptographic update. Measure elapsed time, specialist hours, defects, service interruption and customer approval. Record every manual dependency and unresolved supplier constraint.

Appendix D. Revenue cohort file

For each customer, maintain the date and value of paid discovery, architecture, qualification, production deployment, managed assurance and renewal. Record direct labour, partner cost, hardware, cloud, laboratory, accreditation, warranty, receivables and cash collection.

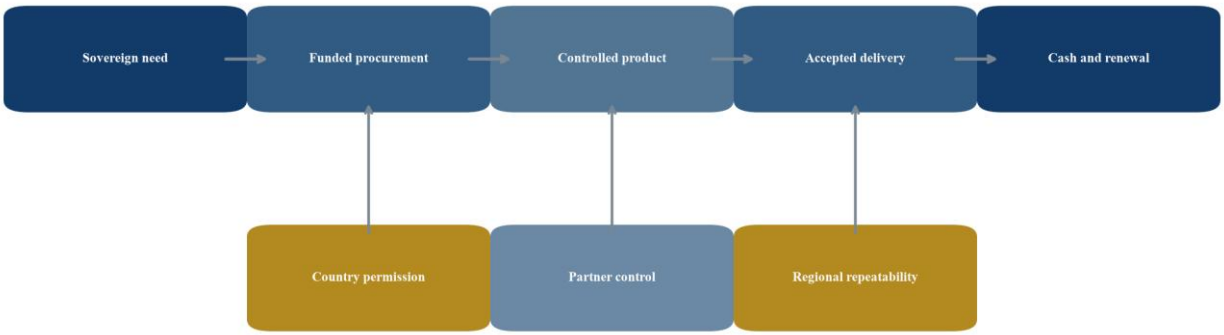
Calculate conversion, duration and contribution by country, sector and product release. Investigate cohorts that stall after a sponsored pilot or require repeated custom engineering.

Appendix E. Transaction evidence room

The evidence room should include policies cited by management, customer contracts, procurement records, acceptance certificates, invoices, collections, partner agreements, product architecture, source and build evidence, software bills of materials, validation records, test matrices, security claims, incident history, staffing, rights, insurance and financial reconciliations.

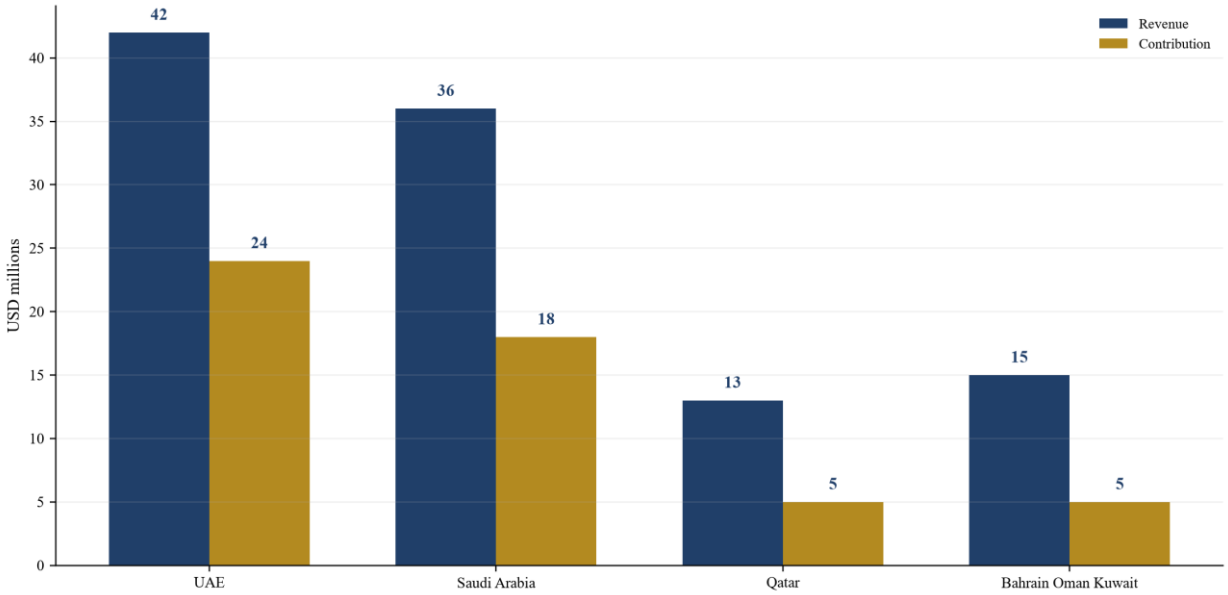
Every investment-committee claim should link to a dated source and accountable owner. Management assumptions should remain visibly separate from observed results.

Figure 1 GCC post quantum security platform diligence architecture



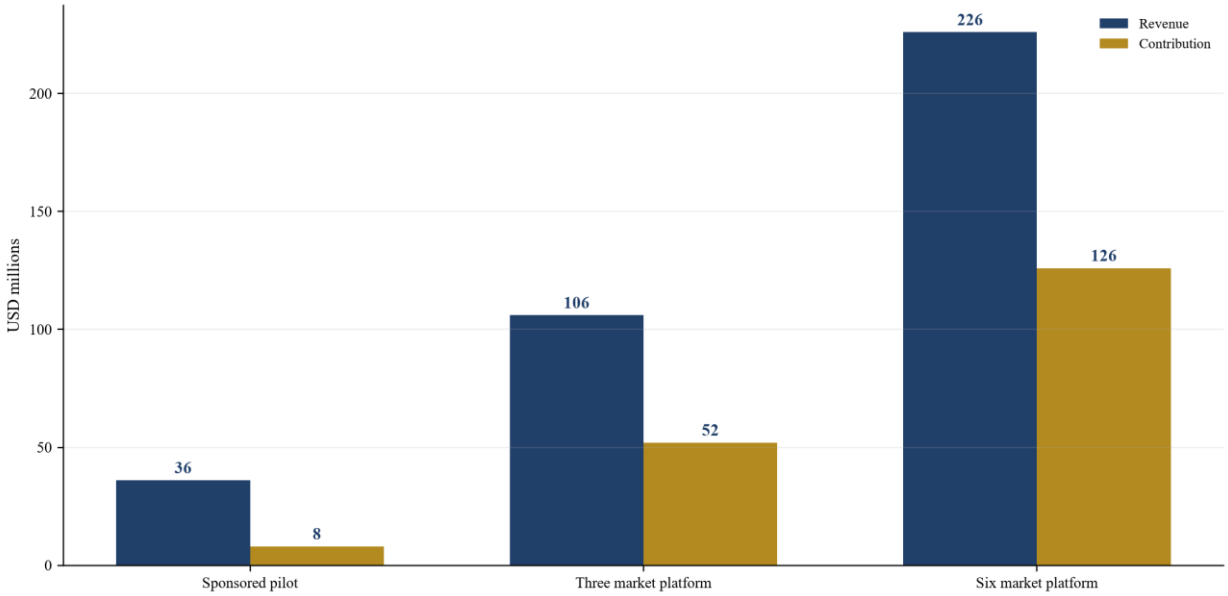
Proposed framework; each conclusion requires country customer product and financial evidence.

Figure 2 Hypothetical central annual revenue and contribution by GCC market



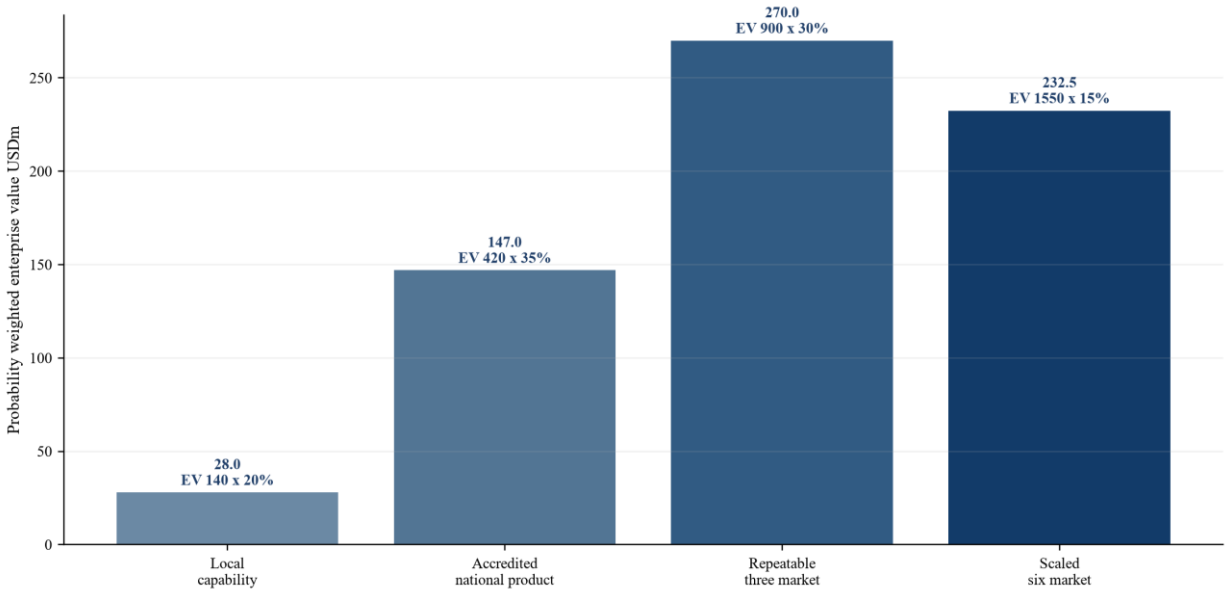
Management assumptions in USD millions; figures are not market observations or forecasts.

Figure 3 Hypothetical annual revenue and contribution by operating case



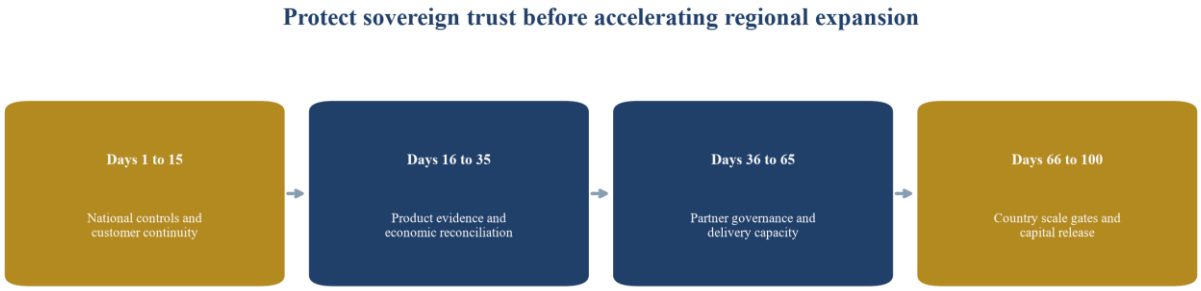
Management assumptions in USD millions; excludes central overhead tax financing and integration.

Figure 4 Hypothetical platform valuation by evidence state



Management assumptions in USD millions; the chart is not a valuation conclusion.

Figure 5 First hundred days regional platform sequence



Proposed sequence; timing should follow transaction national and customer constraints.

Table 1 GCC policy and capability signals

Jurisdiction	Public signal	Diligence implication	Evidence still required
UAE	National Encryption Policy and announced post quantum migration activity	Clear basis for discovery migration and national capability programmes	Funded scope acceptance cash and renewal
GCC	Regional Cybersecurity Strategy and cooperation mechanisms	Supports shared direction and information exchange	Country procurement product approval and delivery economics
Saudi Arabia	National Cryptographic Standards and cyber controls	Structured cryptographic and regulated-sector control environment	Specific post quantum programme customer and budget evidence

Jurisdiction	Public signal	Diligence implication	Evidence still required
Qatar	National strategy assurance standard and cryptographic standard	Strong governance basis for critical-system assurance	Procurement ownership qualification and product acceptance
Bahrain Kuwait Oman	National strategies cloud data and capability frameworks	Relevant adjacent conditions for market entry	Country-specific need authority contract and contribution

Official public sources; customer demand and commercial conclusions require separate evidence.

Table 2 Sovereign demand evidence hierarchy

Stage	Evidence	Valuation treatment	Principal risk
Policy signal	Official policy or strategy	Strategic context only	No funded buyer or defined scope
Sponsored activity	National programme laboratory or public collaboration	Capability option	Sponsorship may not convert to procurement
Funded qualification	Contracted inventory test or pilot	Project backlog subject to delivery	Programme may stop after qualification
Production deployment	Signed order and accepted operating release	Operating revenue subject to collection	Acceptance liability and concentration
Recurring operation	Subscription support assurance or renewal	Recurring value for enforceable term	Service cost renewal and policy change

Proposed classification for transaction diligence.

Table 3 National control capability test

Dimension	Diligence test	Strong evidence	Warning signal
Source and build	Reproduce released product in approved environment	Controlled source dependencies build and artefact hashes	Escrow without reproducible build
Keys and releases	Inspect custody signing approval and recovery	Separated authority monitored access and tested recovery	Foreign or individual dependency
Operations	Execute support incident and rollback locally	Approved staff runbooks and exercised authority	Local office without operating control
Data	Trace collection storage access transfer and deletion	Enforced residency classification and audit	Contract promise without technical control
Continuity	Test supplier failure and disengagement	Substitute routes documentation and named owners	Sole supplier or undocumented specialist dependency

Proposed buyer test; requirements vary by customer and jurisdiction.

Table 4 Hypothetical central annual economics by market

Market cohort	Revenue	Direct cost	Contribution
UAE sovereign and critical infrastructure	42.00	18.00	24.00
Saudi national and regulated programmes	36.00	18.00	18.00
Qatar programmes	13.00	8.00	5.00

Market cohort	Revenue	Direct cost	Contribution
Bahrain Oman and Kuwait programmes	15.00	10.00	5.00
Total	106.00	54.00	52.00

Management assumptions in USD millions; excludes central overhead tax financing and integration.

Table 5 Hypothetical operating cases

Case	Revenue	Contribution	Principal condition
Sponsored pilot	36.00	8.00	Bespoke delivery senior engineers and limited reuse
Three market platform	106.00	52.00	Accepted products controlled delivery and country evidence
Six market platform	226.00	126.00	Accredited releases trained partners and recurring assurance

Management assumptions in USD millions; these cases are not forecasts.

Table 6 Hypothetical valuation evidence states

Evidence state	Enterprise value	Probability	Weighted value
Local capability	140.00	20%	28.00
Accredited national product	420.00	35%	147.00
Repeatable three market platform	900.00	30%	270.00
Scaled six market sovereign platform	1,550.00	15%	232.50
Total		100%	677.50

Management assumptions in USD millions; the calculation is not a valuation conclusion.

Table 7 Acquisition gate and consideration map

Gate	Required evidence	Transaction response	Post close measure
Control	Source build key data and continuity rights	Closing condition or specific protection	Reproducible build and recovery test
Demand	Contract budget acceptance invoice and collection	Base consideration	Cohort conversion and cash
Product	Versioned tests claims and accreditation	Product milestone	Accepted release and defect rate
Economics	Contribution and working capital by programme	Valuation and working capital adjustment	Contribution and collection
Regional scale	Country permission customer and reusable delivery	Deferred consideration	New market acceptance renewal and cash

Proposed transaction framework; legal tax regulatory and national-security terms require qualified advice.

References

[1] National Institute of Standards and Technology. Post-Quantum Cryptography Project. https://csrc.nist.gov/projects/post-quantum-cryptography

[2] National Institute of Standards and Technology. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://csrc.nist.gov/pubs/fips/203/final

[3] National Institute of Standards and Technology. FIPS 204 Module-Lattice-Based Digital Signature Standard. https://csrc.nist.gov/pubs/fips/204/final

[4] National Institute of Standards and Technology. FIPS 205 Stateless Hash-Based Digital Signature Standard. https://csrc.nist.gov/pubs/fips/205/final

[5] National Institute of Standards and Technology. Post-Quantum Cryptography Publications. https://csrc.nist.gov/Projects/post-quantum-cryptography/publications

[6] National Institute of Standards and Technology. Post-Quantum Cryptography. https://www.nist.gov/pqc

[7] National Institute of Standards and Technology. Crypto Agility Project. https://csrc.nist.gov/projects/crypto-agility

[8] National Cybersecurity Center of Excellence. Crypto Agility Considerations for Migrating to Post-Quantum Cryptographic Algorithms. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[9] Internet Engineering Task Force. RFC 9794 Terminology for Post-Quantum Traditional Hybrid Schemes. https://www.rfc-editor.org/rfc/rfc9794.html

[10] Internet Engineering Task Force. RFC 9954 Hybrid Key Exchange in TLS 1.3. https://www.rfc-editor.org/rfc/rfc9954.html

[11] Internet Engineering Task Force. RFC 10024 Hybrid ML-KEM Key Agreement for TLS 1.3. https://www.rfc-editor.org/rfc/rfc10024.html

[12] Internet Engineering Task Force. RFC 10042 Hybrid ML-KEM Key Exchange for SSH. https://www.rfc-editor.org/rfc/rfc10042.html

[13] UAE Cabinet. UAE Cabinet Approves National Cybersecurity Strategy. https://uaecabinet.ae/en/news/uae-cabinet-approves-national-cybersecurity-strategy-api-first-policy

[14] UAE Government. National Encryption Policy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/cyber-activities/National-Encryption-Policy

[15] Emirates News Agency. UAE Announces Approval of National Encryption Policy. https://www.wam.ae/en/article/15w563h-uae-announces-approval-national-encryption-policy

[16] Advanced Technology Research Council. UAE Cyber Security Council Partners with ATRC to Advance National Post-Quantum Security Transition. https://www.atrc.gov.ae/news/uae-cyber-security-council-partners-atrc-advance-national-post-quantum-security-transition

[17] Advanced Technology Research Council. UAE Cybersecurity Council Advances National Readiness for Future Quantum Threats with ATRC QuantumGate. https://atrc.gov.ae/news/uae-cybersecurity-council-advances-national-readiness-future-quantum-threats-atrcs-quantumgate

[18] Dubai Electronic Security Center. New Innovative Projects at GISEC Global 2025. https://desc.gov.ae/news-post/dubai-electronic-security-center-launches-new-innovative-projects-at-gisec-global-2025/

[19] Gulf Cooperation Council Secretariat General. Final Statement of the Forty-Fifth Session of the Supreme Council. https://www.gcc-sg.org/en/MediaCenter/News/Pages/news2024-12-1-3.aspx

[20] Gulf Cooperation Council Secretariat General. GCC Cybersecurity Cooperation and Executive Plan. https://www.gcc-sg.org/en/MediaCenter/News/Pages/news-2026-8-27-2.aspx

[21] Gulf Cooperation Council Secretariat General. GCC States in Global Cybersecurity Index 2024. https://www.gcc-sg.org/en/MediaCenter/News/Pages/news2024-11-3-1.aspx

[22] Saudi National Cybersecurity Authority. National Cryptographic Standards. https://nca.gov.sa/en/regulatory-documents/frameworks-and-standard-list/ncs/

[23] Saudi National Cybersecurity Authority. National Cryptographic Standards PDF. https://nca.gov.sa/ncs_en.pdf

[24] Saudi National Cybersecurity Authority. Essential Cybersecurity Controls ECC 2 2024. https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/

[25] Saudi National Cybersecurity Authority. Cloud Cybersecurity Controls CCC 2 2024. https://nca.gov.sa/en/regulatory-documents/controls-list/ccc/

[26] Saudi National Cybersecurity Authority. Data Cybersecurity Controls. https://nca.gov.sa/en/regulatory-documents/controls-list/dcc/

[27] Qatar National Cyber Security Agency. National Cyber Security Strategy 2024 to 2030. https://www.ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20Eng%20OL_0.pdf

[28] Government Communications Office Qatar. National Cyber Security Strategy 2024 to 2030 Launch. https://www.gco.gov.qa/en/media-centre/top-news/the-national-cyber-security-strategy-2024-2030-is-launched/

[29] Qatar National Cyber Security Agency. National Information Assurance Standard Version 2.1. https://assurance.ncsa.gov.qa/sites/default/files/publications/policy/2023/NCSA_CSGA_%20National_Information_Assurance_Standard_En_V2.1_0.pdf

[30] Qatar National Cyber Security Agency. Qatar National Cryptographic Standard Version 1.0. https://qcert.ncsa.gov.qa/sites/default/files/public/documents/qatar_national_cryptographic_standard_-_version_1.0.pdf

[31] Qatar Communications Regulatory Authority. Cloud Policy Framework. https://www.cra.gov.qa/en/press-releases/cra-publishes-the-cloud-policy-framework

[32] Bahrain National Cyber Security Center. National Cyber Security Strategy 2025 to 2028. https://ncsc.gov.bh/en/national-strategy/bahrain-national-cyber-security-strategy-2025-2028.html

[33] Bahrain National Cyber Security Center. National Cyber Security Strategy Executive Summary. https://www.ncsc.gov.bh/assets/images/National_Cyber_Security_Strategy_Summary_2025_2028_1517a02fac.pdf

[34] Bahrain National Cyber Security Center. About the National Cyber Security Center. https://ncsc.gov.bh/en/about/who-are-we.html

[35] Kuwait Communications and Information Technology Regulatory Authority. Cloud Computing Regulatory Framework. https://www.citra.gov.kw/sites/en/LegalReferences/Cloud_computing_regulatory_framework.pdf

[36] Kuwait Communications and Information Technology Regulatory Authority. Data Classification Policy. https://www.citra.gov.kw/sites/en/LegalReferences/Data_Classification.pdf

[37] Oman Information Technology Authority. Cybersecurity Industry Development Program. https://www.ita.gov.om/itaportal/Data/English/DocLibrary/202382133148936/CYBERSECURITY_INDUSTRY_DEVELOPMENT_PROGRAM_En.pdf

[38] Oman Information Technology Authority. Regional Cybersecurity Week 2024 Recommendations. https://www.ita.gov.om/itaportal/Data/English/DocLibrary/202511411419126/REGIONAL-CYBERSECURITY-WEEK-2024-EN.pdf

[39] International Telecommunication Union. Global Cybersecurity Index 2024. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

[40] United States National Security Agency. Post-Quantum Cybersecurity Resources. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

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.