Hardware-Security Module M&A after Post-Quantum Standards

A Commercial Diligence and Valuation Framework for Firmware Readiness Certification Perimeters Installed-Base Migration and Upgrade Economics

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Post-quantum cryptography has moved from research planning into standards-led implementation. The United States National Institute of Standards and Technology published FIPS 203, FIPS 204 and FIPS 205 in August 2024. The United Kingdom National Cyber Security Centre recommends discovery and initial planning by 2028, priority migration by 2031 and broad completion by 2035. Hardware-security modules sit inside many trust architectures that protect keys, payment systems, identities, code signing, public-key infrastructure, cloud services and regulated workloads. Their strategic value after the new standards depends on the upgrade path from installed hardware to validated and interoperable post-quantum operation.

This paper develops a commercial diligence and valuation framework for acquisitions of HSM vendors and HSM-centred platforms. It tests five connected questions. First, which deployed products can support approved post-quantum algorithms through controlled firmware and which require hardware replacement? Second, which certifications and customer approvals must be renewed after a cryptographic change? Third, can the installed base be segmented into executable upgrade cohorts with named owners, maintenance rights and migration windows? Fourth, does migration create recurring product and service economics after engineering, validation and support cost? Fifth, can the buyer preserve trusted manufacturing, key-management continuity, customer confidence and regulatory acceptance through integration?

The framework separates standards-driven market need from vendor-specific evidence. It maps the product estate by module, firmware, certification, interface, deployment environment and end-of-support date. It then connects customer cohorts to upgrade eligibility, migration acceptance, renewal, replacement and collected cash. Diligence covers FIPS 140-3 and sector-specific certification, PKCS #11 and other interfaces, algorithm validation, tamper-response design, manufacturing controls, key backup and transfer, cloud tenancy, secure boot, intellectual-property rights, supply-chain dependency, customer concentration and specialist retention.

A wholly hypothetical case illustrates the method. The central case has annual revenue of USD 58.00 million, direct product, validation, migration and support cost of USD 31.00 million, and contribution before central overhead of USD 27.00 million. A services-heavy case produces USD 28.00 million of revenue and USD 7.00 million of contribution. A scaled platform case produces USD 120.00 million of revenue and USD 68.00 million of contribution. A separate probability-weighted valuation illustration produces USD 418.00 million. These figures are management assumptions used to demonstrate the framework; they are not observed market data, forecasts or valuation conclusions.

The analysis concludes that acquisition value should follow demonstrated upgrade control. Strong evidence includes an authoritative installed-base register, firmware eligibility, current validation, interoperable interfaces, accepted customer migrations, contracted support, controlled manufacturing,

documented key portability, repeatable engineering, renewal or replacement orders, and collected cash. Policy deadlines support market timing. Customer-level evidence determines value. Deferred consideration can bridge uncertainty where the premium depends on new certificates, production migration, cohort conversion, contribution and retention of critical capability.

JEL Classification: G24, G34, L63, L86, M15, O31, O33

Keywords: hardware-security modules, post-quantum cryptography, cybersecurity M&A, FIPS 140-3, firmware, certification, installed base, cryptographic migration, commercial diligence, technology valuation

Introduction

Hardware-security modules are specialised cryptographic systems designed to protect sensitive keys and execute controlled cryptographic operations. They can be deployed as appliances, payment modules, cloud services, network-attached systems, embedded devices or roots of trust. Their value comes from a combined boundary: protected key material, authenticated interfaces, controlled firmware, tamper response, operational procedures and independent validation. A post-quantum algorithm added to software can change several parts of that boundary at once.

NIST published FIPS 203 for ML-KEM, FIPS 204 for ML-DSA and FIPS 205 for SLH-DSA in August 2024 [1-4]. Its module programme applies FIPS 140-3 requirements through the Cryptographic Module Validation Program [30,19]. The UK National Cyber Security Centre recommends that large organisations complete discovery and initial planning by 2028, complete the highest-priority migrations by 2031 and finish broad migration by 2035 [6]. The timetable explicitly recognises long-lived hardware roots of trust, supply chains, hybrid coexistence and cryptographic agility. These developments create a multi-year need to evaluate HSM firmware, performance, interfaces, certification and replacement.

The commercial opportunity varies by installed estate. Some modules may accept new algorithms through signed firmware. Some may require memory, processor, entropy or interface changes. Some may support post-quantum operations while losing the validation or customer approval on which deployment depends. A cloud HSM may hide physical replacement from the customer while leaving the provider with equivalent engineering and certification obligations. The buyer must therefore trace every revenue claim from a named product and customer cohort to a controlled upgrade or replacement path.

This paper is written for strategic buyers, private equity investors, cybersecurity platforms and investment committees evaluating HSM vendors and related control platforms. It addresses commercial, operating and transaction evidence. Cryptographic validation, certification, legal analysis, export controls, accounting and tax require qualified specialists and transaction-specific work.

1 Define the acquisition thesis through the installed base

The acquisition thesis should identify the customer control point the target owns. An enterprise may need to retain existing keys while moving applications to post-quantum algorithms. A payment operator may require a sector-approved module and controlled key ceremony. A cloud provider may need tenant isolation, measured performance and automated fleet replacement. A manufacturer may depend on an embedded root of trust whose hardware cannot be changed after deployment. The acquirer should map each use case to the module, interface, validation boundary, customer acceptance test and revenue stream.

Each decision has a different buyer, budget, procurement route, delivery cycle and acceptance test. An inventory engagement can be purchased from a consulting budget. Product remediation may sit within engineering roadmaps. Hardware replacement can require capital expenditure and long procurement lead times. Managed certificate or key-management services may enter recurring operating budgets. The acquirer should identify which budget pays and which executive can release it.

The thesis should state the target's role in the trust chain. A general-purpose HSM can protect keys for public-key infrastructure, databases, code signing and identity. A payment HSM can support PIN, card and network operations under a specialised approval regime. A cloud HSM can expose controlled functions through a service boundary. An embedded module can anchor secure boot or device identity. Management software can coordinate policy, backup, high availability and estate operations. Revenue quality and replacement risk differ across these roles.

The board should approve a testable statement: the target can convert a defined customer obligation into a specified accepted outcome at a measured contribution and within an evidenced delivery capacity. Diligence should reject broad claims that post-quantum migration alone guarantees demand.

2 Translate standards and timelines into HSM demand

Official migration dates are market signals. They are not vendor orders. The commercial diligence team should map every material customer to the applicable authority, sector rule, data-lifetime risk, internal policy and procurement milestone. It should identify the named programme owner, approved budget, current phase, contracted deliverable and expected production decision.

The demand map should distinguish awareness, assessment, funded discovery, architecture, pilot, production migration and ongoing operation. A customer presentation is not a qualified opportunity. A free assessment is not paid demand. A paid pilot proves limited willingness to spend but may not establish production scope. A signed multi-year statement of work with accepted milestones provides stronger evidence. Invoices and collections remain the clearest evidence that the customer has converted concern into spending.

Long-lived sensitive data creates earlier urgency. OMB guidance prioritises high-value and high-impact systems [9]. NCSC guidance asks organisations to prioritise sensitive data, critical communications, infrastructure and long-lived hardware [6]. A target serving those environments may face stronger customer need, deeper qualification and longer sales cycles. The diligence model should capture both effects.

Management should provide customer evidence without exposing protected security information unnecessarily. Contracts, purchase orders, redacted budgets, acceptance records, invoices, collections and renewal correspondence can support the demand case. Pipeline should be weighted by completed procurement events, not sales judgement alone.

3 Build the authoritative HSM estate register

HSM migration begins with an authoritative estate register. The register should identify model, serial or service instance, hardware revision, firmware, validated configuration, interface, algorithm set, deployment environment, owner, support contract, key classes, backup arrangement, high-availability pair, customer application, end-of-support date and post-quantum route. Sales shipment data alone is insufficient because modules can be resold, retired, isolated, virtualised or operated by a service provider.

The buyer should reconcile product telemetry, entitlement systems, maintenance records, support tickets, renewal invoices, channel reports and customer confirmations. Each module should be assigned to one of four paths: firmware eligible, hardware upgrade required, replacement required, or unresolved. The reason should be evidenced through signed firmware capability, processor and memory limits, secure-element design, entropy source, interface compatibility, validation status and customer operating constraints.

A representative customer test should trace hardware to the applications and keys that depend on it. A module can be technically upgradeable while its client library, certificate authority, payment switch, code-signing pipeline or recovery process remains incompatible. The diligence team should sample deployed

estates and trace the complete dependency chain. It should also test whether spare devices, disaster-recovery modules and offline roots are represented.

The valuable output is a maintained migration register. It states which module can move, when approved firmware is available, whether revalidation is required, which customer window applies, how keys and policies are preserved, what rollback exists, and which replacement revenue can be contracted. An installed-base premium should follow a reconciled and actionable register rather than historical shipment volume.

4 Segment the installed base into upgrade cohorts

Installed hardware creates a commercial relationship only where the vendor can identify and serve the operator. Channel sales, unsupported products and perpetual licences can reduce visibility. Customers may defer migration, use third-party middleware, move to cloud services or replace the module with another vendor. The target should demonstrate contractual and operating mechanisms that connect support entitlement to firmware, validation evidence, migration tools and replacement offers.

Revenue should be segmented by module and customer cohort. Cohort reporting should show installed units, supported units, firmware-eligible units, migrations attempted, migrations accepted, replacement orders, maintenance renewal and service expansion. Time between release and customer acceptance matters because a large theoretical upgrade base can convert slowly under regulated change controls.

Contract review should identify firmware rights, upgrade charges, appliance ownership, support periods, validation commitments, key-transfer assistance, spare-device obligations, service credits, acceptance and end-of-life notice. Maintenance revenue may require engineering and certification work that has not yet been funded. A cloud subscription may include future algorithm support while leaving the provider with hardware and revalidation cost.

The acquirer should reconcile claimed annual recurring revenue. Software licences, subscriptions and managed services can recur. A renewable consulting retainer is not equivalent to committed recurring revenue. Project revenue should remain project revenue. Contracted backlog should be reduced for unfunded options, expired work orders, missing customer inputs and delivery beyond available capacity.

5 Verify firmware and production migration competence

An HSM target must change live key-management systems without weakening security, exposing keys, breaking interoperability or interrupting service. The work can include signed firmware, algorithm enablement, client-library changes, certificate and key changes, clustering, backup, secure transfer, hardware replacement, protocol upgrades, validation evidence, testing, rollout and rollback. NCSC guidance emphasises procurement, commissioning, testing, backup, business continuity and rollback [6].

Diligence should inspect completed production migrations rather than demonstrations alone. The evidence pack should identify the system, previous cryptography, target architecture, dependency map, test plan, change approvals, performance results, incidents, rollback route, final acceptance and operating support. Customer references should confirm the target's role and the result, subject to confidentiality.

Hybrid approaches can reduce transition risk when properly designed. IETF guidance defines hybrid schemes that combine traditional and post-quantum components, and later standards specify ML-KEM hybrid key agreement for TLS 1.3 [12-15]. A target should explain where it uses hybrid methods, how components are combined, which protocols are standardised, and how compatibility is tested. Proprietary combinations require careful review.

Production competence also depends on change management. The target needs a signed release pipeline, protected build keys, secure manufacturing, test environments, configuration evidence, controlled remote administration, incident response and customer communication. The buyer should inspect a completed

change from source approval through firmware signing, laboratory testing, certificate update, customer deployment and supported rollback. The acquisition thesis should price the full delivery system.

6 Measure engineering validation and delivery capacity

Demand can exceed supply long before it becomes revenue. Capacity should be built from named employees, contractors, partner resources, product automation and customer dependencies. Roles can include cryptographers, security architects, application engineers, infrastructure specialists, hardware engineers, PKI experts, test engineers, project leaders and assurance personnel.

The diligence team should calculate available hours by skill, utilisation, billability, training, sales support, research, leave and management. It should map each signed project to required skills and calendar windows. A single senior architect may be the approval bottleneck across many teams. A partner network may provide scale but reduce margin and delivery control. Customer engineers may be required for code access, testing and production changes.

Management's capacity model should reconcile to payroll, contractor agreements, partner contracts, project plans and timesheets. The team should test whether new hiring is realistic in the required locations and whether security clearance, customer approval or export restrictions constrain deployment. Staff described as post-quantum specialists should have evidenced work relevant to their claimed roles.

Automation can improve throughput. Fleet-management connectors, compatibility rules, signed firmware pipelines, algorithm test harnesses and certification workflows can reduce manual work. The buyer should measure their effect on hours, accuracy and acceptance. Demonstrated time savings matter. Marketing descriptions do not establish capacity.

7 Analyse upgrade and replacement economics

Gross margin can be overstated when scarce technical labour is classified as research, customer success or central engineering. The transaction model should allocate all delivery-related effort to the customer or product line it supports. It should include contractors, partner fees, cloud testing, laboratories, travel, certifications, warranty, support, incident remediation and unbilled pre-sales work.

The central hypothetical case assumes USD 58.00 million of revenue. Appliance and replacement revenue contributes USD 24.00 million, firmware and management subscriptions contribute USD 15.00 million, maintenance contributes USD 11.00 million, and migration and assurance services contribute USD 8.00 million. Direct product, validation, migration and support cost is USD 31.00 million, leaving USD 27.00 million of contribution before central overhead. These values are management assumptions.

The services-heavy case assumes USD 28.00 million of revenue and USD 7.00 million of contribution because bespoke migrations require senior engineers, laboratory work and customer-specific support. The scaled platform case assumes USD 120.00 million of revenue and USD 68.00 million of contribution after reusable firmware, automated fleet management, partner delivery and recurring support increase throughput. Neither case is a forecast.

The buyer should inspect contribution by cohort. Early regulated customers may carry heavy qualification costs. Later customers should show reuse of connectors, playbooks, test evidence and partner capacity. If every project remains bespoke, margin and scale assumptions should be reduced.

8 Diligence firmware intellectual property and supply-chain control

The target's value may reside in source code, detection logic, protocol implementations, test suites, knowledge bases, migration methods, customer configurations and specialist know-how. The buyer should establish ownership, inventor assignment, contractor terms, patent status, trade-secret controls and third-party obligations. Each component should be linked to the revenue or delivery step it supports.

Open-source software can accelerate development and improve interoperability. It can also create notice, attribution, source-disclosure, patent or redistribution obligations. The buyer should obtain a software bill of materials, licence scan, remediation log and release process. Dependencies on cryptographic libraries require version, maintenance, validation and vulnerability review.

Standards dependencies deserve explicit treatment. NIST can publish revised guidance or additional algorithms. IETF protocols continue to evolve. Hardware-security modules, browsers, cloud services and network products determine which combinations can operate in production. The target should show an architecture that can adopt approved changes without rewriting every customer environment. This capability is commonly described as cryptographic agility [16,17].

Customer-specific work can constrain reuse. Contracts may assign deliverables, prohibit use of data or restrict publication of methods. Security-sensitive customers may require isolated environments and limit remote support. The acquisition model should separate reusable platform assets from customer-owned or restricted material.

9 Test certification perimeters and validation evidence

Terms such as quantum-safe, quantum-resistant and compliant can hide different evidence. A product may implement a standard algorithm in a library. A cryptographic module may have undergone algorithm testing or formal module validation. A complete system may still have vulnerable protocols, certificates, update mechanisms or dependencies. The target should state exactly what has been tested, by whom, against which version and within which boundary.

NIST's Cryptographic Algorithm Validation Program and Cryptographic Module Validation Program provide defined forms of validation [18,19]. Validation status should be checked on official lists. A target awaiting validation should identify the submitted module, laboratory, scope, open issues and expected decision. Customer statements should avoid implying approval that has not been granted.

Performance also matters. Post-quantum keys, signatures and messages can affect bandwidth, memory, latency, hardware and certificate infrastructure. Tests should represent the customer's protocols, devices, networks and traffic. Embedded and operational environments can have long lifecycles and constrained resources. Cloud test results do not establish performance on every edge device.

The acquirer should maintain a claims matrix linking each commercial statement to a standard, test, validation, customer acceptance or limitation. Unsupported claims can create mis-selling, warranty, regulatory and reputational exposure.

10 Examine installed-base concentration and procurement quality

Early post-quantum vendors may depend on a few government, defence, financial-services or technology customers. Concentration can provide strong references and demanding validation. It can also create renewal, budget, security-clearance and change-of-control risk. Revenue analysis should show customer, legal entity, contract, programme, product, geography, gross contribution, receivables and dependency.

Government awards require close reading. A framework place does not guarantee work. An indefinite-delivery vehicle may contain a ceiling rather than committed revenue. A research grant is not customer revenue. A prototype contract may end before production. The diligence team should identify funded task orders, appropriations, options, acceptance and termination rights.

Commercial customers may depend on board-approved cyber programmes, vendor roadmaps and broader infrastructure refresh. A migration project can be delayed when a cloud provider, device manufacturer or core-software vendor has not released compatible products. The target's contract should allocate those dependencies and change risk.

Change of control can require customer consent, security review, supplier onboarding or foreign-investment analysis. The buyer should identify customers and programmes that could be lost or restricted after acquisition and include that exposure in transaction conditions and valuation.

11 Assess interfaces alliances and ecosystem position

HSM migration crosses many product boundaries. A target may rely on cloud platforms, hardware-security modules, certificate authorities, identity vendors, network equipment, browsers, operating systems, systems integrators and specialist laboratories. Alliances can expand distribution and capacity. They can also expose the target to channel conflict and weak bargaining power.

The diligence team should classify each relationship as referral, reseller, implementation partner, technology integration, subcontractor or strategic dependency. It should inspect executed agreements, exclusivity, territory, certification, revenue share, lead ownership, service responsibility, support, data access, intellectual property and termination.

Partner-sourced pipeline should be reconciled to registered opportunities and contracts. A memorandum of understanding should not be valued as distribution. Certification badges should be verified. Joint demonstrations should be separated from customer deployment. The target should identify which partner products are required for its solution and which can be substituted.

The strongest ecosystem position is evidenced by repeatable integration, accepted reference architectures, trained partners, joint customer wins and clear support boundaries. The buyer should test whether the acquisition strengthens that position or causes partners to treat the target as a competitor.

12 Quantify key-custody liability and security risk

Inventory and migration work can affect confidentiality, availability, authentication and software trust. A missed dependency can leave an exposure. A failed cutover can interrupt a critical service. An implementation flaw can create a new vulnerability. Advice may influence regulated or national-security systems. These risks require a specific liability review.

The data room should include customer warranties, indemnities, liability caps, service credits, professional-services obligations, security schedules, incident terms, insurance, claims and near misses. The buyer should identify commitments that exceed insurance or the target's control. Broad warranties that a system is quantum-safe can be difficult to support when standards, products and threat models evolve.

The target's own security should meet the sensitivity of its work. Diligence should inspect secure development, access control, code signing, secrets management, repositories, privileged administration, endpoint protection, supplier access, vulnerability management, incident response and recovery. Customer cryptographic inventories can reveal high-value architecture and deserve strong protection.

Risk allocation should follow the service boundary. The target can warrant defined methods, personnel and agreed deliverables. Customers and product vendors retain responsibilities for their systems, decisions and supplied information. The buyer should price unresolved exposures and require remediation or specific indemnity where evidence supports it.

13 Protect engineering knowledge and certification authority

Scarce expertise can be the principal asset. The buyer should identify who can design architectures, approve claims, solve failures, maintain tooling, satisfy customers and train others. Organisation charts and job titles provide limited evidence. Project records, code history, design decisions, customer reliance and peer review reveal actual authority.

Key-person analysis should map each critical capability to at least two people, documentation and a succession route. Founder dependence is material when one person owns customer relationships, technical direction and final approval. Contractors can create continuity and intellectual-property risk. Security clearances and nationality restrictions may limit transfer between projects or countries.

Retention should address role, decision authority, compensation, research time, customer continuity and integration design. A large buyer can lose specialist staff through slow approvals or a purely sales-led operating model. The post-close plan should preserve technical review and secure development while integrating finance, legal, sales and support controls.

Knowledge transfer should be observable. Paired project leadership, reviewed documentation, repeat delivery and incident exercises provide stronger evidence than a training schedule. Earn-outs should avoid incentives to accept low-quality work or defer necessary investment.

14 Build a valuation model around upgrade evidence states

Valuation should reflect the target's current evidence state. A capability-stage target has specialists, prototypes and early customer access. A validated-tooling target has repeatable inventory or testing assets and accepted pilots. A contracted-migration target has funded programmes, implementation capacity and observable contribution. A scaled-platform target has diversified customers, partner delivery, recurring software or assurance and stable unit economics.

A wholly hypothetical probability-weighted illustration assigns enterprise values of USD 90.00 million, USD 260.00 million, USD 540.00 million and USD 980.00 million to four evidence states: legacy installed base, validated hybrid platform, contracted upgrade engine and scaled post-quantum platform. The associated probabilities are 20%, 35%, 30% and 15%. The weighted values are USD 18.00 million, USD 91.00 million, USD 162.00 million and USD 147.00 million, producing USD 418.00 million in total. The assumptions demonstrate the method and do not value a named company.

The buyer should cross-check against revenue quality, contribution, cash conversion, product ownership, customer concentration and required investment. A software multiple should not be applied to labour-intensive migration revenue. A services multiple can understate reusable tooling and recurring assurance. Sum-of-the-parts analysis can separate these components.

Downside cases should include procurement delay, slower conversion from assessment, hiring constraints, partner dependence, failed validation, security incident and standards change. Value should fall when evidence requires future investment or customer action that the target does not control.

15 Structure consideration around certification and migration evidence

Transaction structure can bridge uncertainty between strategic market timing and vendor-specific evidence. Upfront consideration should reflect owned assets, retained capability, contracted work and verified economics at closing. Deferred consideration can follow production acceptance, qualified recurring revenue, gross contribution, collections and retention of critical personnel.

An earn-out should use measures the seller can influence and the buyer can verify. Bookings can reward contracts that are poorly priced or beyond capacity. Revenue can reward low-margin subcontracting. EBITDA can be affected by buyer allocations. A balanced mechanism may combine accepted firmware, certification and replacement milestones, recurring software or managed-service revenue, customer retention and contribution before agreed central charges.

Holdbacks or escrow can address specific indemnities, intellectual-property defects, customer consents or validation claims. Reverse conditions may protect the seller if the buyer changes the agreed operating model. Governance during the earn-out should define investment, hiring, pricing, project acceptance and reporting.

The buyer should avoid paying twice for the same expectation. A high strategic premium and a full achievement-based earn-out can duplicate value. The valuation bridge should show which evidence is paid at closing and which future outcome releases additional consideration.

16 Plan integration around trust continuity

Integration should preserve customer trust and technical credibility. The first hundred days should secure people, repositories, customer delivery, partner relationships, incident response and financial control. It should also identify which functions remain separate because of security, accreditation or customer obligations.

The buyer should map all live projects, milestones, access permissions, dependencies, responsible specialists, customer communications and cash commitments. Critical releases and migrations should have named continuity plans. Commercial teams should avoid announcing expanded capability before technical and contractual review.

Tool integration requires care. Moving code, telemetry or customer inventories into the buyer's environment can require consent and security approval. Identity changes can interrupt access. Replacing ticketing or development systems during a critical migration can reduce evidence quality. The integration plan should sequence changes around customer milestones.

Operating metrics should remain visible after close. The buyer should track estate-register accuracy, conversion between stages, accepted HSM upgrades and replacements, specialist utilisation, contribution, incidents, renewals, collections and customer concentration. Integration success is demonstrated when the combined business delivers more accepted work with controlled risk and improved cash generation.

17 Use a ninety-day HSM diligence programme

Days one to thirty should establish the evidence perimeter. The team maps products, services, customers, contracts, revenue, people, tools, intellectual property, dependencies, validations, liabilities and security controls. It selects representative customer files and defines technical tests. Finance reconciles revenue, backlog, receivables and staff cost.

Days thirty-one to sixty should test the operating claims. Technical reviewers run controlled inventory and interoperability tests. Commercial reviewers interview authorised customer and partner references. Operations reconciles signed work to named capacity. Legal reviewers analyse contracts, intellectual property, open-source obligations, data and change-of-control terms. Security reviewers inspect the target's own controls.

Days sixty-one to ninety should convert findings into transaction decisions. The team builds central and downside cases, identifies remediation, prices retained risk, defines conditions, drafts consideration mechanics and finalises the integration plan. The investment committee receives an evidence map that links every material assumption to a source and owner.

The programme can be compressed or extended according to transaction size and access. The sequence matters. Technical promise, commercial demand, delivery capacity and cash economics should be tested together. A finding in one workstream should update the others.

18 Establish post-close upgrade and platform gates

The first gate protects the existing business. Critical people remain, customer commitments are met, access is controlled and cash reporting is reconciled. The second gate improves evidence quality through a maintained HSM estate register, standard project architecture, resource planning and contribution reporting. The third gate increases throughput through reusable tooling, trained partners and repeatable testing.

The fourth gate builds recurring economics. Suitable functions can move into software subscription, managed fleet management, certificate lifecycle, continuous configuration assurance, assurance or support. The product must provide continuing customer value and should not be described as recurring merely because a project renews. The fifth gate expands distribution through qualified alliances and adjacent customers.

Capital should follow the gates. Research and product investment can precede revenue when the board understands the technical objective and customer path. Hiring should follow qualified backlog and a realistic onboarding period. Acquisition of adjacent capability should wait until the first target's delivery and integration controls are stable.

Value creation should remain connected to collected cash. The board can track contracts, acceptance, invoice, collection, direct cost, contribution and reinvestment by cohort. This discipline prevents a standards-driven market narrative from concealing weak execution.

Conclusion

Post-quantum migration has an official standards base and visible public-sector timelines. The work is extensive because cryptography is embedded in software, hardware, identity, communications, suppliers and operating processes. These conditions support a long implementation market. They also create room for vendors to overstate the commercial meaning of policy announcements, pilots and technical demonstrations.

An acquisition should be underwritten from customer evidence. The target should identify vulnerable cryptography accurately, convert inventories into prioritised plans, secure funded implementation scope, deliver production change safely, and retain enough specialist and partner capacity to meet the backlog. Revenue should be classified by work stage and cohort. Direct cost should include scarce technical effort. Product claims should link to standards, tests and validation boundaries.

The transaction structure should pay for current evidence and reserve further value for accepted migration, durable revenue, contribution and retained capability. Integration should protect technical authority, customer trust, secure environments and partner relationships. A board using this framework can assess whether it is acquiring a credible migration platform, a valuable specialist team, a project backlog or an early option. Each can have value. The price and capital plan should match the evidence.

Frequently asked questions

Do final post quantum standards prove customer demand

They establish a technical and policy basis for migration. Customer demand requires a budget owner, procurement route, funded scope and acceptance plan. Diligence should trace each material opportunity to those records.

What is the most important HSM commercial diligence test

The buyer should trace a representative installed-base cohort from supported device through firmware eligibility, validation, production upgrade or replacement, acceptance, invoice, collection and renewal. This shows whether the target converts a deployed estate into delivered economics.

How should the installed HSM estate be tested

Reconcile shipment, entitlement, telemetry, support, channel and customer records. Sample model, hardware revision, firmware, validation certificate, interface, key classes, backup, high availability, support status and application owner. The output should support a controlled upgrade or replacement decision.

When can HSM migration revenue be treated as recurring

Firmware and management subscriptions, maintenance and managed HSM services can recur when contracts and continuing customer value support them. Hardware replacement and migration projects remain transactional unless the contractual commitment and service characteristics establish a recurring obligation.

What creates a defensible HSM platform

Defensibility can come from controlled firmware, trusted manufacturing, validated configurations, stable interfaces, key-portability methods, fleet management, laboratory assets, partner integrations, customer acceptance and accumulated operating knowledge. Each element requires verification.

How should an acquirer value scarce technical talent

The buyer should map people to revenue, approvals, code, customer trust and failure resolution. Value depends on retention, transferability, documentation, succession and the operating environment required for those people to remain effective.

Which outcomes are suitable for an earn out

Accepted production migrations, qualified recurring revenue, customer retention, delivery contribution, collections and retention of critical capability can be measured. Definitions should limit buyer allocation disputes and avoid rewarding poorly priced bookings.

What should happen in the first hundred days

The buyer should protect people, customer milestones, secure access, partner relationships and financial reporting. Tool and systems integration should follow customer and security constraints. Scale investment should follow verified delivery evidence.

Appendix A. HSM estate-register diligence fields

The estate register should record the business service, application, owner, environment, model, serial or service instance, hardware revision, firmware, validation certificate, approved configuration, algorithms, interfaces, key classes, backup and high-availability relationship, support entitlement, end-of-support date, target state, migration owner, budget, deadline, test requirement and acceptance status. Each record should link to source evidence and retain change history.

The buyer should reconcile shipments, telemetry, maintenance, support, channel and customer records. It should record unknown locations and unsupported devices. A maintained estate register has more value than cumulative shipment history.

Appendix B. Hypothetical financial model

The central case assumes USD 24.00 million of appliance and replacement revenue, USD 15.00 million of firmware and management subscription revenue, USD 11.00 million of maintenance revenue, and USD 8.00 million of migration and assurance services revenue. Direct cost totals USD 31.00 million and contribution totals USD 27.00 million before central overhead.

The services-heavy case assumes USD 28.00 million of revenue and USD 7.00 million of contribution. The scaled platform case assumes USD 120.00 million of revenue and USD 68.00 million of contribution. A real model should add sales capacity, research, product development, central engineering, tax, working capital, capital expenditure, financing and acquisition integration.

Appendix C. Customer evidence file

Each material customer file should include the legal entity, programme owner, applicable obligation, budget source, procurement route, contract, statement of work, work order, change control, acceptance criteria, project plan, dependency register, delivery team, technical evidence, invoice, collection, support commitment, renewal path and authorised reference record.

The file should distinguish customer-provided information, target analysis, accepted deliverables and management expectation. Sensitive inventories and architecture should remain in controlled rooms with role-based access and an audit trail.

Appendix D. Investment committee questions

The committee should ask whether customers have funded migration work, whether inventory outputs are complete enough to support decisions, whether production migrations have been accepted, whether contracted work fits named delivery capacity, whether contribution includes all specialist cost, whether intellectual property is owned, whether claims match validation evidence, and whether critical people will remain.

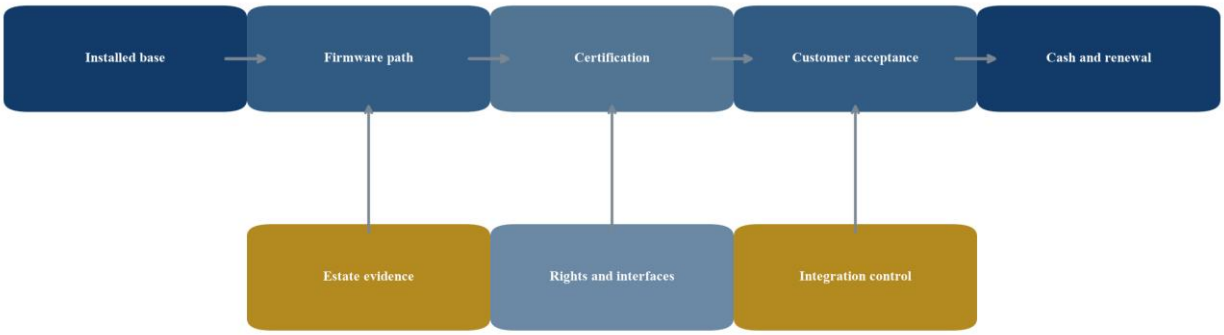
It should identify dependencies outside the target's control. These can include standards, cloud and hardware products, customer engineering, security approvals, protocol maturity and procurement. The transaction should allocate price, capital and timing according to those dependencies.

Appendix E. Transaction evidence hierarchy

The evidence hierarchy begins with policy and standards, which establish external direction. Customer strategy and budget establish organisation-level intent. Signed contracts establish committed scope subject to their terms. Production acceptance establishes delivery. Invoices and collections establish commercial conversion. Renewals, expansion and stable contribution establish repeatability.

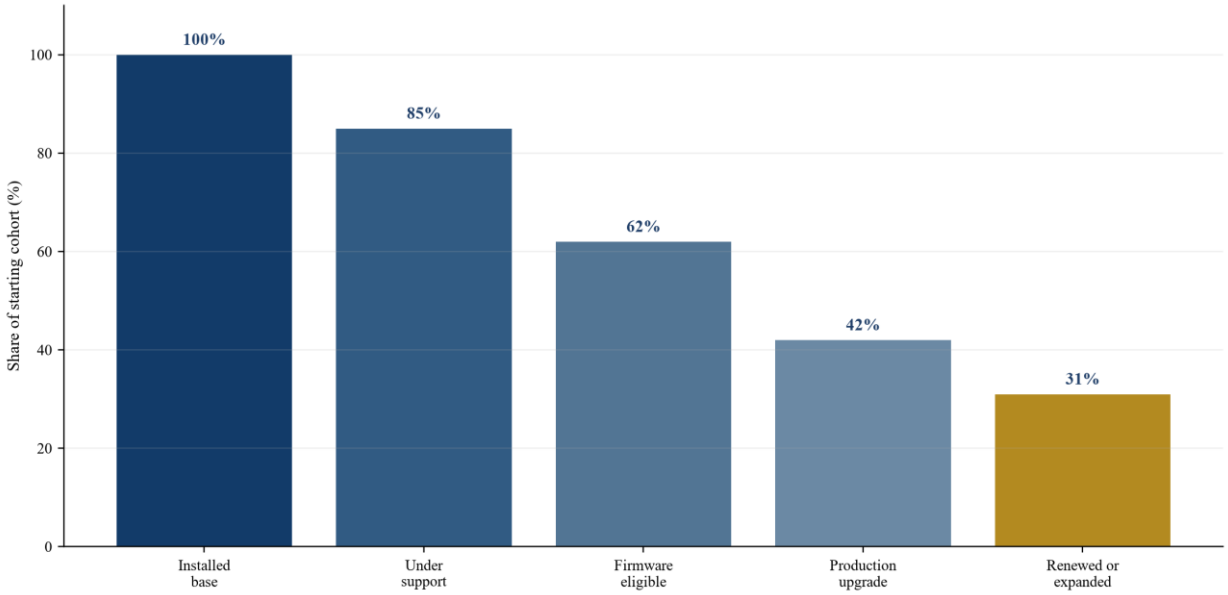
Each level answers a different question. An acquisition premium should be linked to the levels the target has reached and can sustain. Future levels can be addressed through milestones, earn-outs and staged investment.

Figure 1 HSM acquisition diligence architecture



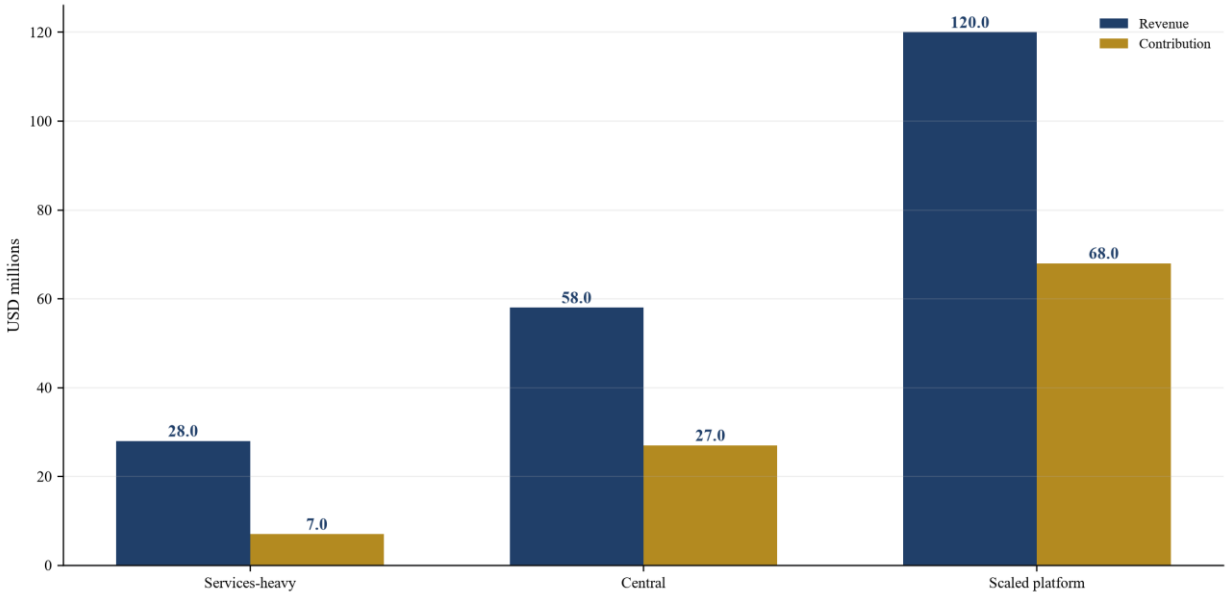
Proposed framework; each conclusion requires target and customer evidence.

Figure 2 Installed-base upgrade cohort



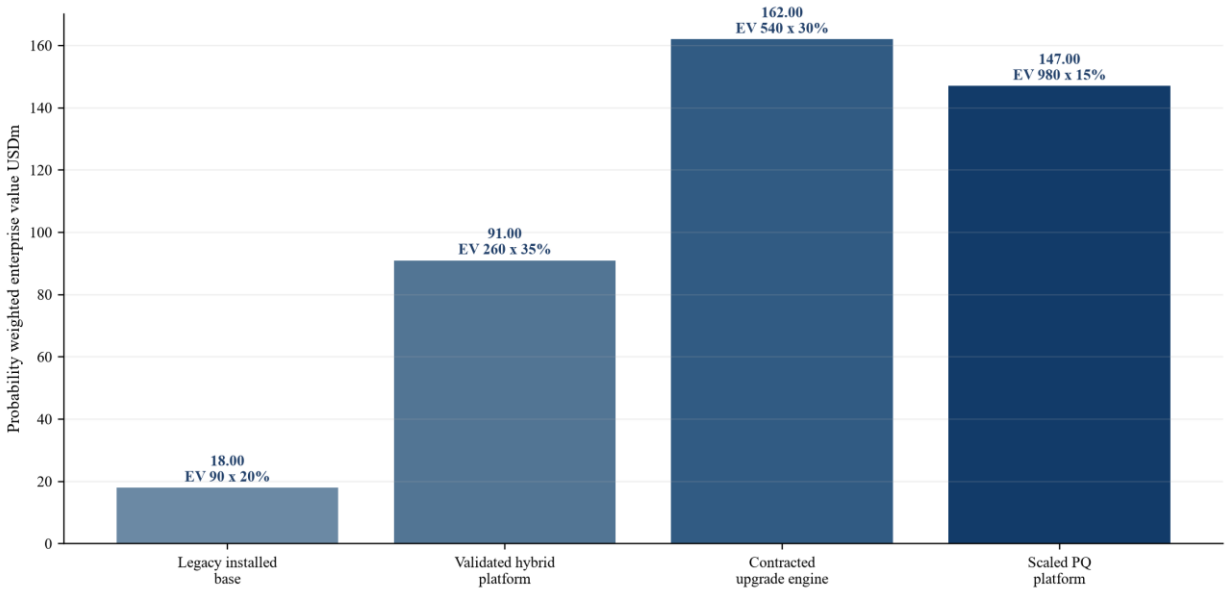
Hypothetical management assumptions; percentages represent cohort progression, not market observations.

Figure 3 Hypothetical annual revenue and contribution by operating case



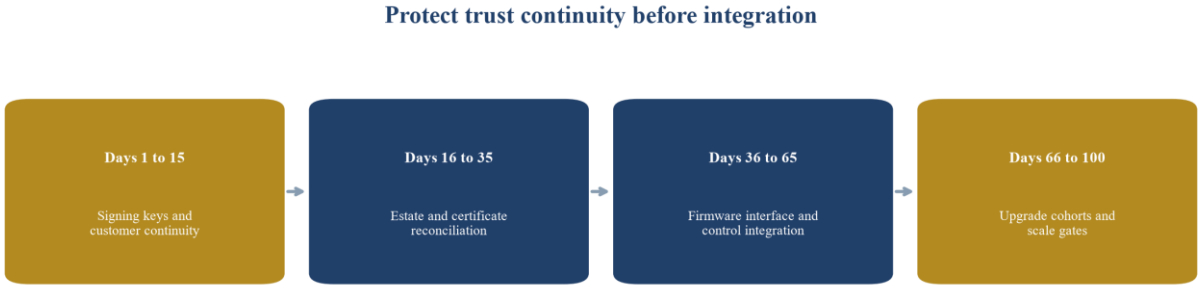
Management assumptions in USD millions; excludes central overhead tax financing and integration.

Figure 4 Hypothetical probability weighted valuation by evidence state



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

Figure 5 First hundred days trust-continuity sequence



Proposed sequence; timing should follow transaction and customer constraints.

Table 1 Policy and standards signals relevant to diligence

Signal	Current evidence	Transaction implication	Required target evidence
NIST principal standards	FIPS 203 204 and 205 final in 2024	Product and migration work can reference final algorithms	Versioned implementation test and claim boundary
United States transition	Inventory duties and 2035 transition direction	Federal and supplier demand can become budgeted work	Funded order procurement route and customer acceptance
United Kingdom timeline	Discovery by 2028 priority migration by 2031 completion by 2035	Near-term assessment demand can precede production migration	Cohort conversion and capacity plan

Signal	Current evidence	Transaction implication	Required target evidence
European Union roadmap	Transition start by end 2026 high-risk use cases by end 2030	Multi-country opportunity with national implementation differences	Jurisdiction and customer-specific plan
Protocol development	Hybrid and post-quantum protocol standards continue to mature	Product compatibility and roadmap dependencies remain	Tested protocol support and upgrade architecture

Official policy and standards evidence; target-specific commercial conclusions require separate verification.

Table 2 Installed-base revenue evidence hierarchy

Stage	Evidence	Revenue treatment	Principal risk
Awareness	Meeting conference or request for information	Exclude from qualified pipeline	Interest has no budget
Estate assessment	Purchase order and accepted module scope	Project revenue	Customer may choose another vendor
Firmware plan	Approved release validation and migration plan	Project revenue	Revalidation and interface dependencies
Production upgrade	Signed work order and change approvals	Backlog subject to engineering capacity	Key continuity acceptance and liability
Managed assurance	Subscription or managed-service contract	Recurring only for enforceable committed period	Service cost and renewal

Proposed classification for transaction diligence.

Table 3 HSM estate-register capability test

Dimension	Diligence test	Strong evidence	Warning signal
Coverage	Reconcile shipment telemetry support and customer records	Module-level ownership and configuration	Shipment counts without deployed location
Accuracy	Sample model firmware and certificate data	Verified configurations and support status	Unsupported installed-base claim
Actionability	Trace module to upgrade replacement and owner	Prioritised maintained migration register	Static asset list
Integration	Review client APIs backup HA and management plane	Versioned interfaces and accepted workflows	Proprietary undocumented dependency
Continuity	Test entitlement firmware and status refresh	Current register with change history	Historical shipment ledger

Proposed buyer test for a representative environment.

Table 4 Hypothetical central annual economics

Revenue or cost item	Revenue	Direct cost	Contribution
Appliances and replacement	24.00	15.00	9.00
Firmware and management subscriptions	15.00	4.50	10.50
Maintenance	11.00	5.50	5.50
Migration and assurance services	8.00	6.00	2.00

Revenue or cost item	Revenue	Direct cost	Contribution
Total	58.00	31.00	27.00

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

Table 5 Hypothetical operating cases

Case	Revenue	Contribution	Principal condition
Services-heavy	28.00	7.00	Bespoke migration and senior engineering intensity
Central	58.00	27.00	Firmware reuse accepted upgrades and maintenance
Scaled platform	120.00	68.00	Automated fleet control partner delivery and diversified customers

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

Table 6 Hypothetical valuation evidence states

Evidence state	Enterprise value	Probability	Weighted value
Legacy installed base	90.00	20%	18.00
Validated hybrid platform	260.00	35%	91.00
Contracted upgrade engine	540.00	30%	162.00
Scaled PQ platform	980.00	15%	147.00
Total		100%	418.00

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
Rights	Ownership open-source review and customer permissions	Condition or specific indemnity	Remediation closure
Demand	Funded contracts and authorised customer confirmation	Base consideration	Accepted backlog conversion
Capacity	Named resources and partner commitments	Hiring and retention plan	Delivery throughput and utilisation
Economics	Contribution and collection by cohort	Valuation and working-capital adjustment	Contribution and cash conversion
Scale	Reusable tooling renewal and expansion	Deferred consideration	Recurring revenue and customer retention

Proposed transaction framework; legal and tax terms require qualified advice.

References

[1] National Institute of Standards and Technology. Post-Quantum Cryptography Project. 2026. https://csrc.nist.gov/projects/post-quantum-cryptography

[2] National Institute of Standards and Technology. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024. https://csrc.nist.gov/pubs/fips/203/final

[3] National Institute of Standards and Technology. FIPS 204 Module-Lattice-Based Digital Signature Standard. 2024. https://csrc.nist.gov/pubs/fips/204/final

[4] National Institute of Standards and Technology. FIPS 205 Stateless Hash-Based Digital Signature Standard. 2024. https://csrc.nist.gov/pubs/fips/205/final

[5] National Institute of Standards and Technology. NIST IR 8547 Transition to Post-Quantum Cryptography Standards. 2024. https://csrc.nist.gov/pubs/ir/8547/ipd

[6] United Kingdom National Cyber Security Centre. Timelines for Migration to Post-Quantum Cryptography. 20 March 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[7] European Commission. Post-Quantum Cryptography. 2026. https://digital-strategy.ec.europa.eu/en/policies/post-quantum-cryptography

[8] NIS Cooperation Group. Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[9] United States Office of Management and Budget. M-23-02 Migrating to Post-Quantum Cryptography. 18 November 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[10] United States Executive Office of the President. Report on Post-Quantum Cryptography. July 2024. https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[11] Cybersecurity and Infrastructure Security Agency. Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools. 15 August 2024. https://www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf

[12] Internet Engineering Task Force. RFC 9794 Terminology for Post-Quantum Traditional Hybrid Schemes. 2025. https://datatracker.ietf.org/doc/html/rfc9794

[13] Internet Engineering Task Force. RFC 9954 Hybrid Key Exchange in TLS 1.3. July 2026. https://www.ietf.org/ietf-ftp/rfc/rfc9954.html

[14] Internet Engineering Task Force. RFC 9958 Post-Quantum Cryptography for Engineers. 2026. https://datatracker.ietf.org/doc/rfc9958/

[15] Internet Engineering Task Force. RFC 10024 Post-Quantum Traditional Hybrid Key Agreement Mechanisms for TLS 1.3. August 2026. https://www.ietf.org/ietf-ftp/rfc/rfc10024.html

[16] National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography. 2026. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[17] National Institute of Standards and Technology. Considerations for Achieving Crypto Agility. 2026. https://csrc.nist.gov/projects/crypto-agility

[18] National Institute of Standards and Technology. Cryptographic Algorithm Validation Program. 2026. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

[19] National Institute of Standards and Technology. Cryptographic Module Validation Program. 2026. https://csrc.nist.gov/projects/cryptographic-module-validation-program

[20] National Security Agency. Post-Quantum Cybersecurity Resources. 2026. https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

[21] National Security Agency. Commercial National Security Algorithm Suite 2.0 Cybersecurity Advisory. 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSI_CNSA_2.0_ALGORITHMS_.PDF

[22] Committee on National Security Systems. CNSS Policy 15 Use of Public Standards for Secure Information Sharing. 4 March 2025. https://www.cnss.gov/CNSS/openDoc.cfm?N6iRcTz7fR9Kp0LJqFh1fQ==

[23] Cybersecurity and Infrastructure Security Agency. Quantum Readiness Migration to Post-Quantum Cryptography. August 2023. https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf

[24] National Cybersecurity Center of Excellence. NIST SP 1800-38B Migration to Post-Quantum Cryptography Quantum Readiness Cryptographic Discovery. 2023. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

[25] European Commission. Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. 11 April 2024. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

[26] European Union Agency for Cybersecurity. Post-Quantum Cryptography Integrations Study. 2022. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[27] European Union Agency for Cybersecurity. Cryptography Topic. 2026. https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography

[28] OASIS. PKCS 11 Cryptographic Token Interface Current Documents. 2026. https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.2/pkcs11-base-v3.2.html

[29] Payment Card Industry Security Standards Council. Information Supplement Cryptographic Key Blocks. 2019. https://www.pcisecuritystandards.org/document_library/

[30] National Institute of Standards and Technology. FIPS 140-3 Security Requirements for Cryptographic Modules. 2019. https://csrc.nist.gov/pubs/fips/140-3/final

[31] United Kingdom National Cyber Security Centre. Supply Chain Security Guidance. 2026. https://www.ncsc.gov.uk/collection/supply-chain-security

[32] United Kingdom National Cyber Security Centre. Principles for Secure System Development. 2026. https://www.ncsc.gov.uk/collection/developers-collection/principles

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.