Quantum Safe Network Acquisitions Standards Interoperability and Margin Risk

A Commercial Diligence and Valuation Framework for Network Security Products Protocol Evidence Deployment Economics and Acquisition Integration

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Quantum-safe networking is moving from algorithm selection into protocol engineering and production deployment. NIST's final post-quantum standards provide the cryptographic foundation, while IETF publications now define hybrid key exchange for major network protocols. This progress creates acquisition interest in vendors that sell secure gateways, virtual private networks, secure access products, network appliances, protocol libraries, certificate infrastructure and network deployment tooling. Standards availability does not establish that a target's product will interoperate across customer estates, perform within service limits or produce attractive margins after deployment effort.

This paper develops a commercial diligence and valuation framework for quantum-safe network acquisitions. It tests whether a target can convert standards support into deployable products across TLS, SSH, IPsec, identity, software update and device-management workflows. The framework examines protocol version control, hybrid-mode design, client and server compatibility, middlebox behaviour, handshake size, latency, throughput, memory, fragmentation, firmware support, cryptographic-module boundaries, customer acceptance and rollback. It then connects this technical evidence to installed-base conversion, revenue cohorts, direct support cost, channel economics, warranty exposure and transaction value.

The paper separates laboratory compatibility from production acceptance. A buyer should trace representative customer cohorts from qualified device and protocol inventory through test, interoperability approval, change window, production cutover, renewal and cash collection. Claims matrices should identify the precise algorithm, protocol, implementation, product version, hardware boundary and validation status behind every commercial statement. A product can implement ML-KEM correctly and still fail as an acquisition proposition when certificate chains, packet sizes, network paths, hardware acceleration, partner products or customer operating procedures are not ready.

A wholly hypothetical case illustrates the method. The central case has annual revenue of USD 64.00 million, direct product, delivery and support cost of USD 37.00 million, and contribution before central overhead of USD 27.00 million. An integration-heavy case produces USD 30.00 million of revenue and USD 5.00 million of contribution. A scaled network-platform case produces USD 138.00 million of revenue and USD 72.00 million of contribution. A separate probability-weighted valuation illustration produces USD 466.00 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 depends on tested interoperability, controllable deployment economics and a credible path through the installed base. The strongest evidence is versioned protocol support, reproducible multi-vendor testing, customer production acceptance, measured performance, maintainable firmware, renewals, controlled support obligations and collected cash. Transaction

structure should reserve part of the consideration for accepted deployments, recurring revenue quality, contribution margin, installed-base conversion and retention of critical engineering capability.

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

Keywords: quantum-safe networks, post-quantum cryptography, network security M&A, TLS, SSH, IPsec, interoperability, crypto agility, deployment economics, technology valuation

Introduction

Networks carry identity, administration, transactions, software updates and confidential data across long-lived infrastructure. Quantum computers capable of breaking widely used public-key cryptography do not yet exist at the required scale, and the timing remains uncertain. Organisations still need to act because sensitive traffic can be captured for later decryption and because network estates contain thousands of clients, servers, gateways, appliances, certificates, libraries and embedded devices that cannot change simultaneously.

NIST published FIPS 203 for ML-KEM, FIPS 204 for ML-DSA and FIPS 205 for SLH-DSA in August 2024 [1-4]. Its transition guidance identifies 2035 as the end point for removing quantum-vulnerable algorithms from NIST standards, with high-risk systems moving earlier [5]. The UK National Cyber Security Centre recommends discovery and initial planning by 2028, highest-priority network deployment by 2031 and completion by 2035 [6]. The European Union roadmap asks Member States to begin transition by the end of 2026 and address high-risk use cases no later than 2030 [7,8].

Protocol engineering is becoming more concrete. IETF publications define terminology for hybrid schemes, hybrid key exchange in TLS 1.3, engineering guidance and post-quantum or traditional hybrid methods for SSH [12-15,33]. NIST's network deployment programme treats interoperability and benchmarking as a dedicated workstream [16,24]. These developments make product roadmaps easier to test. They also expose the difference between an algorithm demonstration and a network product that customers can deploy, operate and support.

This paper is written for corporate buyers, private equity investors, network-security platforms and investment committees evaluating quantum-safe networking targets. It focuses on the evidence that supports commercial value: protocol conformance, multi-vendor interoperability, performance, installed-base reach, customer acceptance, contribution margin, dependency control and integration readiness. Technical validation, legal analysis and security assurance require qualified specialists and transaction-specific evidence.

1 Define the acquisition thesis as a network deployment decision

The acquisition thesis should identify the network decision the target enables. A customer may need quantum-safe remote access, data-centre transport, site-to-site connectivity, device administration, service-to-service encryption, certificate issuance or code-signing continuity. Each use case has a different protocol path, installed base, performance envelope, procurement owner and acceptance test. A target that succeeds in one environment may fail in another.

The thesis should name the controlled product boundary. A gateway can terminate new cryptography while internal systems remain unchanged. A client library can protect application sessions while leaving device-management traffic exposed. A secure access product can depend on operating-system clients, browsers, identity providers and cloud points of presence. An appliance can depend on accelerator support and firmware that the target does not own. Diligence should map these boundaries before assigning strategic value.

The board should approve a testable statement: the target can convert a defined customer obligation into an interoperable and accepted network outcome, at a measured contribution, across an evidenced installed

base. The statement should identify protocol versions, customer segments, product releases, third-party dependencies and the change path. A broad claim that a product is quantum-safe provides insufficient precision for underwriting.

The customer decision also determines the economic model. A software upgrade may protect existing recurring revenue. A new gateway may create appliance revenue and maintenance. A managed network service may create continuing revenue with continuing delivery cost. A migration assessment may lead to a project without durable product adoption. Acquisition value should follow the outcome that customers buy and keep.

2 Translate standards progress into customer-level demand

Official standards and migration dates are demand signals. They do not create customer orders. Commercial diligence should map each material customer to its data-lifetime risk, applicable authority, product estate, procurement cycle, network refresh schedule and named programme owner. The record should show whether the customer has approved discovery, laboratory testing, a production pilot, fleet deployment or continuing operation.

Network demand often follows installed-base events. Customers may wait for a supported operating-system release, compatible network appliance, validated cryptographic module, approved certificate chain or vendor maintenance window. A target can have strong technical capability while revenue slips because another supplier controls the critical dependency. The buyer should therefore reconcile pipeline dates to external release dates and customer change calendars.

The evidence hierarchy should move from interest to cash. Conference participation, requests for information and unpaid demonstrations indicate awareness. A funded lab test indicates willingness to evaluate. A signed deployment order identifies scope and commercial commitment. Production acceptance, invoice, collection and renewal establish stronger evidence. The target should provide cohort data that preserves this sequence.

Long-lived data and critical communications can accelerate demand. Regulated and national-security customers can also impose deeper qualification, procurement and assurance. The diligence model should capture the earlier need and the slower route to revenue. Management should support each material demand claim with contracts, purchase orders, acceptance records, invoices, collections and authorised customer references.

3 Build the network cryptography and protocol inventory

A deployable plan begins with the flows that need protection. The inventory should cover external and internal TLS, SSH administration, VPN and IPsec tunnels, certificate and identity services, software signing, device enrolment, routing-control channels, APIs, service meshes, load balancers, proxies, wireless infrastructure and supplier-managed links. It should identify client, server, middlebox, appliance, library, firmware and cryptographic-module versions for each material path.

Asset counts alone are insufficient. A buyer needs a flow map linking business service, data sensitivity, endpoint ownership, protocol negotiation, certificate chain, network path, latency requirement, device lifecycle, supplier and remediation owner. The record should identify whether the target controls both endpoints, only a gateway, or neither. It should also identify where encrypted traffic is inspected, accelerated, logged or terminated.

CISA and NIST describe automated discovery as useful while recognising coverage limits [10,11,16,24]. Diligence should test a representative environment with known ground truth. The target should find vulnerable algorithms and protocol configurations, reconcile them to assets and flows, and produce an

actionable change register. False negatives can leave exposure. False positives can create costly and unnecessary projects.

The maintained output is a versioned decision register. It states the current protocol and algorithm, target mode, required product release, dependency, test evidence, performance threshold, rollback route, owner and change window. A target that can keep this register current has a stronger commercial position than one that produces a static scan.

4 Prove interoperability across the customer stack

Interoperability is the central acquisition test. A laboratory endpoint pair can complete a hybrid handshake while the production path fails because a proxy rejects the message size, an appliance lacks the required extension, a certificate chain exceeds limits, packet fragmentation changes behaviour or a client silently negotiates a weaker mode. Diligence should reproduce the path that customers operate.

The test matrix should specify protocol, RFC or draft version, algorithm combination, client, server, library, operating system, appliance, cloud service, certificate authority, hardware accelerator and configuration. It should test negotiation success, downgrade behaviour, authentication, session resumption, failure modes, observability and rollback. The buyer should distinguish a vendor's own implementation from third-party components included in a demonstration.

Hybrid modes require particular precision. IETF terminology distinguishes combined traditional and post-quantum mechanisms, and protocol publications define specific combinations [12-15,33]. A target should identify the exact construction, encoding, identifiers and release supported. A proprietary combination may solve a customer problem, yet it can create lock-in, rework or standards risk.

Strong evidence includes repeatable automated tests, independent implementations, customer-representative networks, defect histories, regression coverage and production acceptance. A compatibility table based on marketing claims has limited value. The acquirer should value breadth only where the target can maintain it across releases and provide support within contracted service levels.

5 Measure performance and operational fit

Post-quantum and hybrid mechanisms can change key, ciphertext and signature sizes as well as computation, memory and bandwidth requirements. The commercial effect depends on protocol, implementation, hardware, session pattern and network path. A median laboratory benchmark cannot establish customer experience across constrained devices, high-latency links, packet loss, large certificate chains or high connection rates.

Diligence should test handshake latency, throughput, CPU, memory, connection rate, packet size, fragmentation, retransmission, power and failover under representative load. It should separate initial handshake cost from steady-state traffic and session resumption. Results should identify test hardware, software, compiler, configuration, protocol version and statistical distribution. Capacity planning should translate those results into appliances, cloud instances and support obligations.

Operational fit includes monitoring and incident response. Customers need to know which algorithm and mode negotiated, where fallback occurred, which certificates or keys are expiring, and whether an update changed performance. Logs must provide evidence without exposing secrets. Support teams need runbooks for interoperability failures, emergency rollback and customer communication.

The acquisition model should price hardware refresh, cloud cost, engineering support and customer disruption. A product that maintains list price while doubling infrastructure consumption can compress gross margin. A product that requires senior engineers for every cutover can create services economics inside a software multiple. The buyer should calculate contribution after the resources needed to meet the promised network outcome.

6 Measure implementation capacity from named resources

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, network and application engineers, network platform 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. Inventory connectors, prioritisation rules, code transformation, test harnesses and reporting 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 product and deployment economics

Gross margin should include every resource required to deliver the network promise. Direct cost can include appliance hardware, cryptographic accelerators, cloud points of presence, bandwidth, third-party licences, partner fees, qualification laboratories, customer engineering, technical support, warranty, returns, vulnerability response and unbilled pre-sales testing. Classification outside cost of sales does not remove economic dependence.

The central hypothetical case assumes USD 64.00 million of revenue. Network software subscriptions contribute USD 31.00 million of revenue and USD 20.00 million of contribution. Appliances and edge products contribute USD 17.00 million and USD 4.00 million. Maintenance and support contribute USD 10.00 million and USD 3.00 million. Migration and assurance services contribute USD 6.00 million and no contribution after direct effort. Total direct cost is USD 37.00 million, leaving USD 27.00 million before central overhead. These values are management assumptions.

The integration-heavy case assumes USD 30.00 million of revenue and USD 5.00 million of contribution because custom compatibility work, hardware variants and senior support consume margin. The scaled network-platform case assumes USD 138.00 million of revenue and USD 72.00 million of contribution after repeatable protocol support, automated testing, channel enablement and greater installed-base conversion. Neither case is a forecast.

The buyer should inspect margin by product version, customer cohort and deployment stage. A release may appear profitable while unresolved defects and support are carried centrally. Appliance revenue can create working-capital and warranty exposure. Services can accelerate product adoption when tightly bounded. Each cohort should reconcile order, delivery, acceptance, invoice, collection, direct cost and renewal.

8 Diligence intellectual property and dependency control

The target's value may reside in source code, detection logic, protocol implementations, test suites, knowledge bases, network deployment 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 and network 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 every quantum safe claim against its boundary

Terms such as quantum-safe, quantum-resistant and compliant can refer to different evidence. A library may implement ML-KEM. A protocol stack may support a defined hybrid exchange. A cryptographic module may have algorithm or module validation. A gateway may terminate protected sessions while management, logging, update or certificate workflows remain vulnerable. The target should state the boundary of every claim.

The claims matrix should identify the product and version, algorithm, parameter set, protocol, RFC or draft, operating mode, cryptographic module, validation record, test environment and known limitation. NIST's Cryptographic Algorithm Validation Program and Cryptographic Module Validation Program provide defined forms of validation [18,19]. The buyer should verify status on official records and avoid treating a pending submission as an approval.

Marketing, contracts and product documentation should agree with engineering evidence. A customer-facing statement that a product provides end-to-end quantum-safe security may be misleading when traffic is decrypted at an intermediary or when identity uses a vulnerable signature chain. Diligence should inspect warranties, representations, security questionnaires, tender responses and sales training.

Unsupported claims can create remediation, refund, warranty, regulatory and reputational exposure. The acquisition agreement should identify material claims and allocate responsibility for defects known before closing. Post-close governance should require technical approval of future claims as standards and implementations change.

10 Examine customer concentration and procurement quality

Early quantum-safe network 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 network deployment 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 alliances suppliers and ecosystem position

Post-quantum network deployment 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 professional liability and security risk

Inventory and network deployment 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 network cryptography and protocol 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 talent knowledge and technical 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 valuation around network evidence states

Valuation should follow the target's evidence state. A protocol-capability target has specialists, code and laboratory demonstrations. An interoperable-product target has repeatable multi-vendor testing and qualified releases. A production-network platform has accepted deployments, support operations and observable contribution. A scaled platform has diversified customers, repeatable channel delivery, recurring product economics and controlled support.

A wholly hypothetical probability-weighted illustration assigns enterprise values of USD 85 million, USD 280 million, USD 620 million and USD 1,100 million to those four states. The associated probabilities are 20%, 35%, 30% and 15%. The weighted values are USD 17 million, USD 98 million, USD 186 million and USD 165 million, producing USD 466 million in total. These management assumptions demonstrate the method and do not value a named company.

The buyer should cross-check against installed-base conversion, product gross margin, support intensity, cash conversion, dependency control and required investment. Revenue from custom network integration should not receive a software multiple. Appliance revenue requires working-capital and warranty analysis. A sum-of-the-parts model can separate subscription, hardware, maintenance and project components.

Downside cases should include slower standards adoption, protocol changes, customer change-window delays, performance defects, hardware shortages, partner dependence, validation failure, security incidents and support cost. Value should fall where production evidence or economic control depends on customer and supplier actions that the target cannot direct.

15 Structure consideration around network deployment 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 network

acceptance 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 product and customer continuity

Integration should protect product releases, customer change windows, secure development, support response and engineering authority. The first hundred days should secure repositories, signing systems, build pipelines, laboratories, device inventories, vulnerability handling, customer access and partner relationships. Finance should reconcile product revenue, deferred revenue, inventory, warranty, receivables and direct support cost.

The buyer should map every live customer deployment to product version, network path, scheduled change, responsible engineer, partner dependency, acceptance criterion and rollback. Critical releases require named continuity plans. Commercial teams should avoid expanding claims or bundling the product into new offers before technical and contractual review.

Platform integration can create technical risk. Moving telemetry or customer configurations can require consent. Replacing identity, ticketing, development or monitoring systems during a release can weaken evidence and response. Consolidating appliances or cloud infrastructure can change latency, data location and support obligations. The sequence should follow customer and security constraints.

Post-close metrics should remain visible by cohort: qualified endpoints, tested combinations, production acceptance, defects, support hours, subscription renewal, appliance returns, contribution and cash collection. Integration creates value when the combined business supports more accepted network deployments with stable service and improved unit economics.

17 Use a ninety-day 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 value creation 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 network cryptography and protocol inventory, 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 inventory, certificate lifecycle, continuous discovery, 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

Quantum-safe network acquisitions sit at the junction of cryptographic standards, protocol engineering and installed-base economics. Final algorithms and advancing protocol specifications create a credible product market. Acquisition value depends on whether a target can operate across real customer networks, maintain compatibility and deliver acceptable performance within controlled support cost.

A buyer should begin with the network path. It should identify endpoints, middleboxes, certificate chains, product versions, hardware boundaries, change windows and owners. The target should demonstrate the exact algorithms and protocol combinations it supports, reproduce multi-vendor interoperability, measure performance and show how customers move from laboratory qualification to production acceptance.

Commercial evidence should follow the same path. Customer cohorts should reconcile qualification, order, deployment, acceptance, invoice, collection and renewal. Product margin should include appliances, cloud cost, partner fees, customer engineering, warranty and support. Claims should remain within verified technical and validation boundaries. Valuation should increase only as evidence moves from capability to interoperable product, accepted production platform and scaled recurring economics.

Transaction structure can connect price to those outcomes. Upfront consideration should reflect owned technology, installed customers, accepted products and current contribution. Deferred value can follow installed-base conversion, recurring revenue quality, production acceptance, support margin and retention of critical engineering capability. A disciplined process allows the buyer to distinguish a valuable network platform from a promising protocol implementation or an integration-heavy services business.

Frequently asked questions

Do final post quantum standards prove customer demand

They establish a technical and policy basis for network deployment. 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 commercial diligence test

The buyer should trace a representative cohort from paid inventory through production network deployment, acceptance, invoice, collection and renewal or expansion. This shows whether the target converts concern into delivered economics.

How should network discovery and compatibility tools be tested

Use a controlled environment with known algorithms, certificates, protocols, libraries, devices and services. Measure coverage, false positives, false negatives, asset reconciliation and whether the output supports accountable remediation.

When can deployment revenue be treated as recurring

Software subscriptions and managed services can recur when contracts and continuing customer value support them. Renewable consulting projects remain project revenue unless the contractual commitment and service characteristics establish a recurring obligation.

What creates a defensible implementation platform

Defensibility can come from owned tooling, accurate inventory methods, accepted architectures, protocol expertise, test assets, partner integrations, customer evidence, secure delivery and accumulated operational 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 network deployments, 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. Network protocol and interoperability diligence fields

The inventory register should record the business service, application, owner, environment, data sensitivity, lifecycle, algorithm, key size, certificate, protocol, library, hardware module, supplier, source of detection, confidence, exposure, target state, dependency, remediation owner, budget, deadline, test requirement and acceptance status. Each record should link to source evidence and retain change history.

The buyer should inspect coverage across source code, binaries, runtime traffic, certificates, keys, devices, cloud and network services, operational technology and third-party products. It should record known blind spots and the manual work needed to close them. A maintained inventory has more value than a one-time scan.

Appendix B. Hypothetical financial model

The central case assumes USD 31.00 million of network software subscription revenue, USD 17.00 million of appliance and edge-product revenue, USD 10.00 million of maintenance and support revenue, and USD 6.00 million of migration and assurance-services revenue. Direct product, delivery and support cost totals USD 37.00 million and contribution totals USD 27.00 million before central overhead.

The integration-heavy case assumes USD 30.00 million of revenue and USD 5.00 million of contribution. The scaled platform case assumes USD 138.00 million of revenue and USD 72.00 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 network deployment work, whether inventory outputs are complete enough to support decisions, whether production network deployments 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.

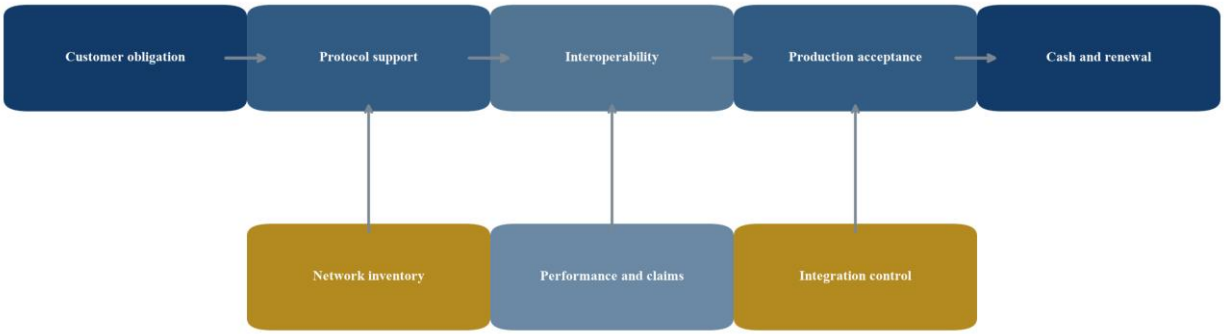
It should identify dependencies outside the target's control. These can include standards, cloud and hardware products, customer engineering, security approvals, protocol maturity and procurement. The transaction should allocate price, capital and timing according to those dependencies.

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.

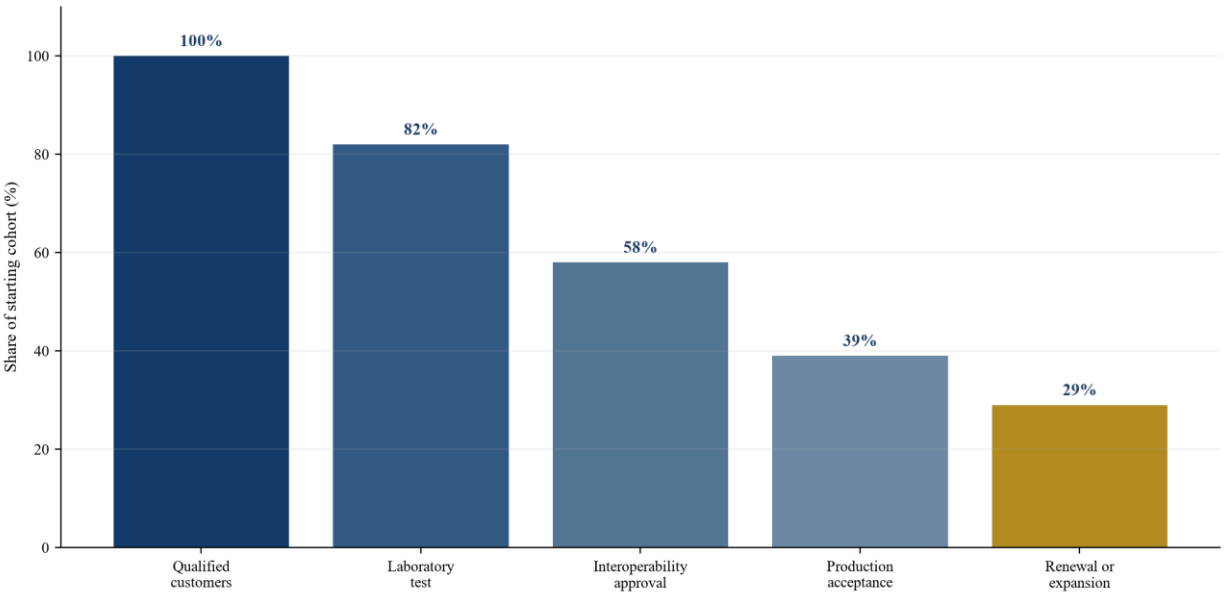
Each level answers a different question. An acquisition premium should be linked to the levels the target has reached and can sustain. Future levels can be addressed through milestones, earn-outs and staged investment.

Figure 1 Quantum safe network acquisition diligence architecture



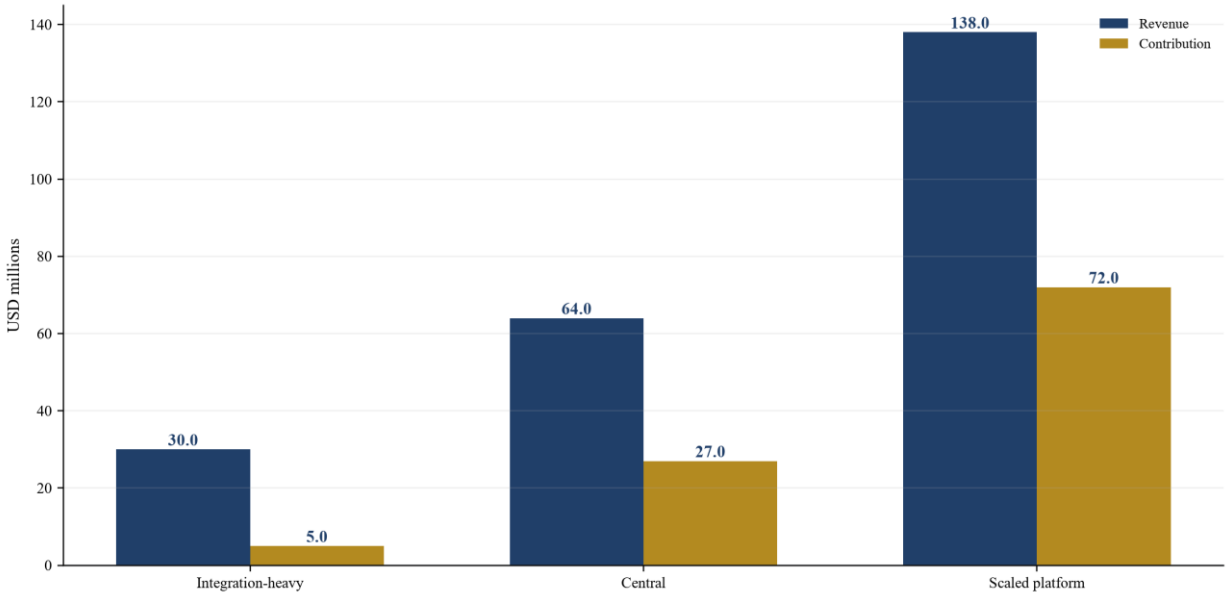
Proposed framework; each conclusion requires target and customer evidence.

Figure 2 Customer deployment revenue cohort



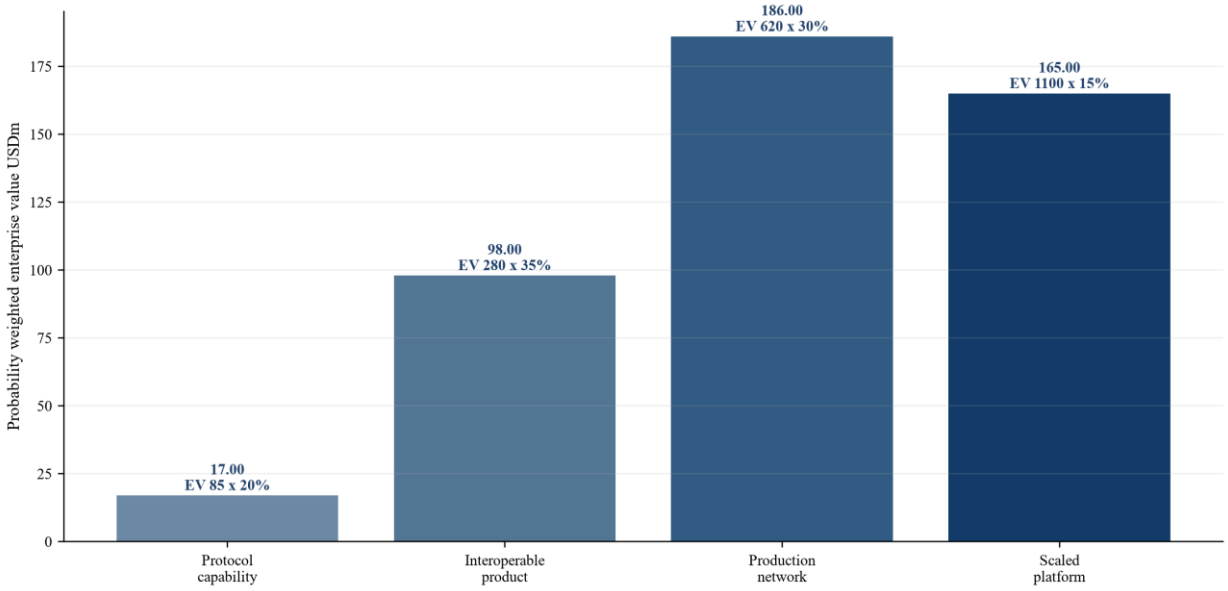
Hypothetical management assumptions; percentages represent cohort progression, not market observations.

Figure 3 Hypothetical annual revenue and contribution by operating case



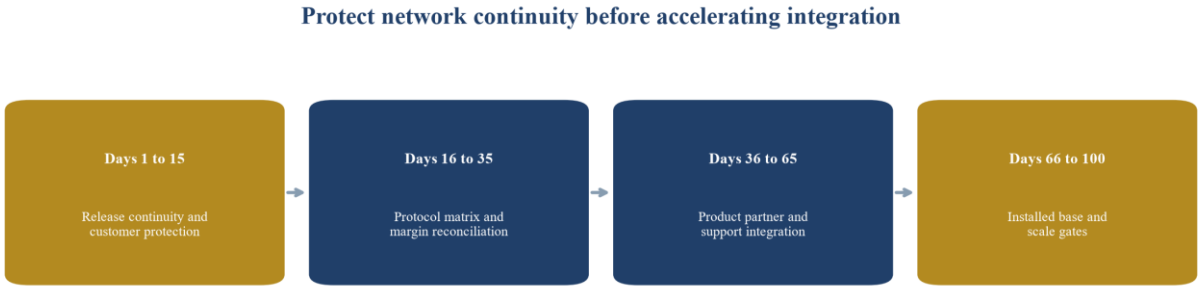
Management assumptions in USD millions; excludes central overhead tax financing and integration.

Figure 4 Hypothetical network acquisition valuation by evidence state



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

Figure 5 First hundred days network product integration 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 network deployment 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 network deployment by 2031 completion by 2035	Near-term assessment demand can precede production network deployment	Cohort conversion and capacity plan
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 Network deployment revenue evidence hierarchy

Stage	Evidence	Revenue treatment	Principal risk
Awareness	Meeting conference or request for information	Exclude from qualified pipeline	Interest has no budget
Funded qualification	Purchase order and accepted protocol test scope	Project revenue	Customer may stop after laboratory work
Interoperability approval	Signed test report across required product stack	Qualified backlog	Supplier and release dependencies
Production network deployment	Signed work order and change approvals	Backlog subject to delivery capacity	Acceptance and liability

Stage	Evidence	Revenue treatment	Principal risk
Managed assurance	Subscription or managed-service contract	Recurring only for enforceable committed period	Service cost and renewal

Proposed classification for transaction diligence.

Table 3 Network inventory and interoperability capability test

Dimension	Diligence test	Strong evidence	Warning signal
Coverage	Compare flow inventory with known network paths	Reconciled endpoints middleboxes and protocols	Asset counts without flow ownership
Interoperability	Reproduce required clients servers and appliances	Versioned multi-vendor test matrix	Single-vendor demonstration
Performance	Test load latency fragmentation memory and failover	Customer-representative distributions and limits	Unqualified median benchmark
Operability	Review telemetry rollback and support workflows	Accepted runbooks and regression tests	Senior engineer dependency
Continuity	Repeat tests after product and protocol updates	Current compatibility history	One-time certification claim

Proposed buyer test for a representative environment.

Table 4 Hypothetical central annual economics

Revenue or cost item	Revenue	Direct cost	Contribution
Network software subscriptions	31.00	11.00	20.00
Appliances and edge products	17.00	13.00	4.00
Maintenance and support	10.00	7.00	3.00
Migration and assurance services	6.00	6.00	0.00
Total	64.00	37.00	27.00

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

Table 5 Hypothetical operating cases

Case	Revenue	Contribution	Principal condition
Integration-heavy	30.00	5.00	Custom compatibility work and senior support intensity
Central	64.00	27.00	Accepted products and controlled deployment
Scaled platform	138.00	72.00	Repeatable product support and diversified installed base

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

Table 6 Hypothetical valuation evidence states

Evidence state	Enterprise value	Probability	Weighted value
Protocol capability	85.00	20%	17.00
Interoperable product	280.00	35%	98.00

Evidence state	Enterprise value	Probability	Weighted value
Production network platform	620.00	30%	186.00
Scaled quantum-safe platform	1,100.00	15%	165.00
Total		100%	466.00

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] Cloud Security Alliance. Quantum-Safe Security Working Group. 2026. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security

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

[30] International Organization for Standardization. ISO IEC 27001 Information Security Management Systems. 2022. https://www.iso.org/standard/27001

[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

[33] Internet Engineering Task Force. RFC 10042 Post-Quantum Traditional Hybrid Key Exchange with ML-KEM for SSH. August 2026. https://datatracker.ietf.org/doc/html/rfc10042

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.