Crypto-Agility Platforms Valuation through Enterprise Migration Economics

A Commercial Diligence Framework for Recurring Revenue Integration Depth Switching Costs and Evidence-Linked M&A Pricing

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Cryptographic transitions are becoming an enterprise operating requirement. The United States National Institute of Standards and Technology published the first three principal post-quantum standards in August 2024 and subsequently expanded guidance on migration and crypto agility. The United Kingdom National Cyber Security Centre recommends discovery and initial planning by 2028, priority migration by 2031 and broad completion by 2035. United States and European policy similarly directs inventories, roadmaps and phased transition. These developments create a long-duration need to discover cryptographic dependencies, change algorithms and protocols, coordinate suppliers, test interoperability and maintain evidence. They do not establish the value of any specific crypto-agility platform.

This paper develops a commercial diligence and valuation framework for crypto-agility platforms. Such platforms may identify cryptographic use, maintain inventories, define policy, orchestrate key and certificate changes, expose dependencies, automate remediation, test target configurations and generate assurance evidence. Their economic value depends on the enterprise work they remove, the risks they reduce and the recurring control they retain after an initial migration. The framework therefore connects platform value to six customer outcomes: inventory completeness, prioritisation speed, migration labour avoided, production change reliability, continuing policy enforcement and audit evidence.

The analysis separates subscription labels from recurring economics. It examines contract structure, cohort progression, implementation intensity, cloud and hardware dependencies, partner delivery, customer concentration, renewal, expansion, support obligations, capitalised development, validation claims and product rights. Integration depth is tested through deployed connectors, governed systems, active policies, production changes and accountable users. Switching costs are tested through exportability, retraining, workflow redesign, replacement risk and the customer's own operating dependency. Lock-in created by poor portability is treated as a liability rather than defensibility.

A wholly hypothetical operating case illustrates the framework. The central case assumes annual revenue of USD 44.00 million and direct product, implementation and support cost of USD 22.00 million, producing USD 22.00 million of contribution before central overhead. A services-heavy case assumes USD 20.00 million of revenue and USD 4.00 million of contribution. A scaled control-platform case assumes USD 96.00 million of revenue and USD 56.00 million of contribution. A probability-weighted valuation illustration produces USD 337.00 million. These figures are management assumptions for demonstrating the method; they are not observed market data, forecasts or valuation conclusions.

The paper concludes that a premium should follow evidence of embedded and expanding control. Strong evidence includes reconciled inventories, customer-authorised integrations, measurable migration savings, accepted production changes, durable policy workflows, high-quality subscription contracts, low support burden, controlled dependencies, retained technical capability and collected cash. Policy deadlines can support market timing. Valuation should still be tied to customer-level outcomes. Deferred

consideration can bridge uncertainty where future value depends on production adoption, expansion, contribution and retention.

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

Keywords: crypto agility, post-quantum cryptography, cybersecurity M&A, enterprise migration, recurring revenue, switching costs, integration depth, software valuation, commercial diligence, technology acquisition

Introduction

Enterprise cryptography is distributed across applications, cloud services, identity systems, certificates, keys, protocols, source code, hardware, firmware, operational technology and suppliers. A change in an algorithm can therefore become a portfolio-wide technology programme. The transition to post-quantum cryptography makes this complexity visible, while the underlying need extends beyond one transition. Organisations must also respond to algorithm weaknesses, certificate-policy changes, protocol deprecation, key-management incidents and new regulatory expectations.

NIST describes crypto agility as the capability to replace or adapt cryptographic algorithms and protocols while preserving system operations [1,2]. Its finalised post-quantum standards include ML-KEM, ML-DSA and SLH-DSA [3-5]. NIST transition guidance and the NCCoE migration programme emphasise discovery, inventory, interoperability and planning [6,7]. NCSC guidance describes migration as a multi-year technology change and recommends solutions that can support alternative algorithm suites [8]. CISA and its partner agencies similarly call for quantum-readiness roadmaps and cryptographic inventories [9,10].

These requirements create a plausible category for crypto-agility platforms. The category can include products for cryptographic discovery, inventory, policy, orchestration, testing, remediation workflow and assurance. Product boundaries vary. A buyer must establish what the target actually controls, which customer work it removes, what remains dependent on specialists and vendors, and how revenue behaves after the first inventory or migration.

This paper is written for strategic buyers, private equity investors, cybersecurity platforms and investment committees evaluating crypto-agility businesses. It addresses commercial, operating and transaction questions. Technical validation, legal analysis, security assurance, accounting and tax require qualified specialists and transaction-specific evidence.

1 Define the product through the customer control loop

A platform should be defined through the customer control loop it supports. Discovery finds cryptographic objects and dependencies. Classification links them to systems, data, owners and risk. Policy states which algorithms, key lengths, protocols and expiry dates are permitted. Planning assigns remediation, sequence, budget and accountability. Orchestration changes selected components. Testing evaluates interoperability and performance. Monitoring detects drift and produces evidence.

The acquirer should identify which parts of this loop the target performs directly. A scanner that exports a static report is different from a system of record refreshed continuously. A workflow tool that assigns remediation is different from a product that changes keys, certificates or libraries. A policy engine may be valuable without executing migration, provided it remains embedded in governance and creates recurring customer use.

The product definition should specify the unit of control. Units can include applications, hosts, services, endpoints, certificates, keys, repositories, protocols, devices, cloud accounts or governed business services. Pricing and usage should reconcile to that unit. If contracts use a convenient metric that does not track customer value, expansion assumptions require extra scrutiny.

Product claims should also define boundaries. The platform may rely on agents, APIs, source access, traffic visibility, configuration databases, certificate authorities, hardware-security modules, cloud providers and customer engineering. The buyer should map each dependency to coverage, implementation effort and commercial risk. A broad control-loop claim supported by narrow visibility should not receive a platform premium.

2 Convert migration policy into enterprise economics

Official timelines support budget conversations, yet the customer's economic decision depends on its estate. NCSC expects large organisations to complete discovery and initial planning by 2028, priority migration by 2031 and broad migration by 2035 [8]. The European coordinated roadmap calls for transition planning and prioritisation across Member States [11,12]. United States federal guidance requires inventories and migration planning [13,14]. National-security guidance creates earlier product requirements in selected environments [15,16].

The platform's value proposition should be expressed through enterprise resources. Discovery can reduce manual interviews, code reviews and spreadsheet reconciliation. Dependency mapping can prevent rework caused by changing a downstream component too early. Policy automation can reduce exceptions and review effort. Orchestration can compress implementation time. Continuous monitoring can detect new vulnerable use after a point-in-time assessment.

Management should support each benefit with customer evidence. The useful records include baseline staff hours, elapsed time, systems covered, exceptions found, changes completed, incidents avoided, audit evidence produced and renewal decisions. Claimed risk reduction should identify the risk owner and the accepted control outcome. Generic statements about future quantum computers cannot establish savings for a particular customer.

The acquirer can translate customer economics into willingness to pay. A platform that removes USD 3.00 million of annual manual effort, protects a critical migration deadline and provides continuing control may support a durable subscription. A tool that produces an initial list and then becomes idle may support a project fee. The valuation model should use the latter economic pattern even when the contract is labelled subscription.

3 Test inventory coverage and data quality

Inventory is the foundation of a crypto-agility platform. The inventory should identify cryptographic algorithms, libraries, certificates, keys, protocols and hardware within a defined scope. It should link each item to a system, owner, business service, data classification, supplier, lifecycle and remediation status. CISA's automated discovery strategy recognises that tools can improve visibility while manual work may remain necessary across heterogeneous estates [9].

The buyer should test coverage against a controlled environment with a known ground truth. The environment should include source code, binaries, network traffic, cloud services, certificates, containers, endpoints, appliances and representative legacy components. Results should report true positives, false positives, false negatives, duplicates, stale objects and unmatched assets. A large object count can indicate visibility or noise. Reconciliation determines which interpretation is correct.

Data lineage is equally important. Each record should show when and how it was discovered, the collector version, supporting evidence, confidence, ownership and changes over time. Customer corrections should improve the maintained record without destroying the original evidence. Role-based access and isolation are essential because the inventory can expose sensitive architecture.

The acquisition team should inspect inventory refresh behaviour. Active connectors should continue to collect data. Failed connectors should generate alerts. Newly deployed software should enter the

inventory. Retired assets should close through controlled rules. If the inventory depends on recurring manual services, direct labour belongs in the unit economics. The product premium should reflect proven automation rather than a data set maintained by hidden consulting effort.

4 Measure integration depth with production evidence

Integration depth is often described through connector counts. The stronger measure is production use. A connector listed in marketing material may be unavailable, unmaintained, limited to read-only data or deployed by no customers. The buyer should verify installed connectors, active data flows, governed objects, workflow actions and accepted production changes by customer cohort.

Depth has several layers. Technical depth reflects authenticated access, coverage and reliability. Workflow depth reflects assignments, approvals, exceptions and reporting. Organisational depth reflects participating teams, business units and executive governance. Economic depth reflects the share of customer work and risk routed through the platform. Replacement becomes harder as these layers deepen, although portability and customer trust remain important.

The diligence data room should include connector architecture, permission models, API limits, release history, error rates, support tickets, customer configurations and change logs. A representative sample should trace a cryptographic finding from detection through ownership, policy decision, remediation, test and closure. Evidence should identify which steps were automated and which required target or customer personnel.

Integration depth also creates obligations. Vendor API changes can break connectors. Customer security teams can restrict permissions. On-premises and operational environments can require long support periods. The valuation model should include maintenance effort, certification, backward compatibility and customer-specific extensions. Deep integration supports value when the platform maintains it efficiently and securely.

5 Separate recurring revenue from recurring control

Recurring revenue is a contract outcome. Recurring control is a customer operating outcome. The two should be reconciled. A prepaid multi-year agreement can produce recurring revenue while the product becomes inactive. A heavily used platform can renew annually with a short cancellation right. The acquirer needs contract evidence and usage evidence.

Contracts should be classified by licence, hosted subscription, managed service, professional service, implementation, support and consumption. IFRS 15 requires entities to identify contracts, performance obligations, transaction price and the timing of transfer [17]. Transaction diligence should not replace formal accounting work, but the framework helps identify where reported recurring revenue includes implementation or stand-ready obligations.

Cohort reporting should show opening recurring revenue, new bookings, expansion, contraction, churn and price changes. It should also show active connectors, covered systems, policies, users, workflows, changes and support effort. Revenue retention without product activity can reflect contractual inertia. Activity without expansion can indicate weak pricing or an incomplete commercial model.

Renewal evidence should include customer rationale. Customers may renew because the inventory remains current, because policy and assurance are embedded, because a migration continues, or because replacement is difficult. The first three can support durable value. Renewal driven by short-term switching friction requires closer examination. The acquirer should model retention after a major migration milestone, when the customer's initial urgency may decline.

6 Build cohort economics around migration stages

The customer journey can begin with paid discovery, move to prioritisation and planning, expand into implementation, and settle into continuing control. Cohorts should be measured from the first paid engagement. Free proofs of concept should be analysed separately because conversion and delivery economics differ.

For each cohort, the buyer should calculate time to initial deployment, implementation hours, contracted annual value, product gross margin, services contribution, expansion, renewal, collection and support. It should also record the migration stage reached. A cohort that renews discovery licences without completing production actions may have different value from one that uses the platform across successive algorithm transitions and governance cycles.

The hypothetical cohort in Figure 2 begins with 100 paid discovery customers. Seventy-two reach governed inventory, fifty-four adopt policy workflows, thirty-eight execute production migration and thirty-one retain continuing control. These rates are management assumptions for demonstrating the framework. Actual valuation should use verified customer records.

Sales efficiency should reflect the long decision cycle of regulated and critical environments. Partner-originated customers may reduce acquisition cost but introduce revenue share and account control risk. Expansion can come from new business units, systems, geographies, control modules or transaction volume. The buyer should identify whether expansion follows repeatable product adoption or additional consulting projects.

7 Quantify migration labour avoided

A credible platform can reduce labour in discovery, reconciliation, prioritisation, change preparation, testing and evidence. The value model should calculate avoided work by activity rather than use an unsupported percentage. The baseline should state team, rate, volume, frequency and error rework. Platform cost should include implementation, licences, customer effort, support and remaining manual work.

The hypothetical value bridge assumes 42,000 annual hours of baseline migration and control work. Automated discovery, workflow and reporting remove 13,000 hours; orchestration and reusable testing remove another 7,000 hours. At an assumed blended loaded cost of USD 120 per hour, gross labour avoided is USD 2.40 million. Platform subscription, implementation and residual operating cost total USD 1.35 million, producing USD 1.05 million of annual net labour benefit before risk effects. These are management assumptions.

Risk benefits should remain separate. A failed certificate rotation, protocol change or firmware update can create operational loss, but expected-loss estimates require event probability, exposure and mitigation evidence. Diligence should avoid combining speculative incident avoidance with observed labour savings.

The acquirer should test whether customer savings persist. Initial discovery can create one-time benefit. Continuous inventory, policy monitoring and repeated change programmes can create recurring benefit. The product should show which workload repeats and how the platform participates. A one-time migration tool should be valued on project demand and replacement cycles rather than perpetual recurrence.

8 Assess switching costs and portability

Switching costs arise when replacement requires data migration, connector rebuilds, workflow redesign, policy recreation, retraining, revalidation and operational risk. They can support retention when they reflect genuine embedded value. They can damage trust when the customer cannot export its own inventory or evidence.

The buyer should request export demonstrations for inventory, history, policies, exceptions, evidence and configurations. It should inspect documented APIs, standard formats, data ownership, termination assistance and deletion procedures. Software bills of materials and component transparency can also support portability and dependency control [18,19]. A target that relies on undocumented formats may create short-term lock-in and long-term commercial risk.

Switching-cost analysis should distinguish replacement friction from customer dependence. Friction is the work needed to move. Dependence is the operating consequence of losing the platform. A platform that continuously governs certificate and key policy can create material dependence. A reporting dashboard used quarterly may be easier to replace.

The valuation model should use observed churn, renewal and replacement evidence. Management interviews can explain why customers stayed. Customer interviews should confirm it. Contractual auto-renewal or early termination penalties should not be presented as product defensibility. Sustainable retention comes from continued value, trusted control and reasonable portability.

9 Test product architecture for future transitions

Crypto agility requires more than implementing current post-quantum algorithms. The platform should separate cryptographic policy from application code, identify algorithm use, support controlled configuration, retain evidence and adapt when standards or implementations change. NIST's crypto-agility work addresses algorithm identifiers, interoperability, transition notices, hybrid approaches, keys and protocol complexity [1,2].

Architecture diligence should inspect the policy model, connector framework, data schema, rules engine, orchestration boundaries, test harness, versioning and rollback. Algorithm and protocol identifiers should be explicit. Customer exceptions should be governed. New standards should enter through controlled configuration and tested code rather than extensive customer-specific rewrites.

Hybrid cryptography adds complexity. IETF terminology and protocol work describe combinations of traditional and post-quantum methods [20-23]. The platform should distinguish supported standards, drafts and proprietary implementations. It should identify where hybrid support is needed, how downgrade is prevented, and how compatibility is tested.

Future readiness also depends on validation and supplier roadmaps. Hardware-security modules, certificate authorities, cloud services, network products, browsers and device manufacturers determine what can be deployed. A platform that exposes these dependencies can support planning. A platform that claims to control them should provide contractual and technical evidence.

10 Diligence validation security and trust

A crypto-agility platform can become a sensitive control plane. It may hold inventories, credentials, keys, policies, architecture and change permissions. The buyer should treat platform security as part of the product, not a corporate overhead item. Architecture, access, logging, segregation, secure development, vulnerability management and incident response require review.

Algorithm implementation claims should specify the boundary. NIST's Cryptographic Algorithm Validation Program and Cryptographic Module Validation Program provide formal validation routes [24,25]. A platform can orchestrate validated modules without itself being a validated cryptographic module. Marketing and customer contracts should represent this accurately.

The diligence team should review independent tests, penetration reports, certifications, vulnerability disclosures, software supply chain, secrets handling and customer isolation. It should trace critical findings to remediation. Open-source and commercial dependencies should have owners, supported

versions and patch processes. NCSC secure development and supply-chain guidance provide useful control principles [26,27].

Trust also has a human dimension. Customers may depend on named experts to approve architecture or resolve failures. The buyer should identify these roles, succession, documentation, customer restrictions and retention risk. A trusted platform without transferable capability can lose value after acquisition.

11 Reconcile product and services economics

Professional services can accelerate adoption, provide domain expertise and create customer evidence. They can also obscure product limitations. The buyer should allocate implementation, custom integration, data cleansing, policy design, testing and support effort to the relevant customer and product line.

The central hypothetical case assumes USD 44.00 million of annual revenue. Subscription and usage revenue is USD 28.00 million, managed control is USD 8.00 million, and implementation and advisory work is USD 8.00 million. Direct product infrastructure, implementation and support cost totals USD 22.00 million, leaving USD 22.00 million of contribution before central overhead. These figures are management assumptions.

The services-heavy case assumes USD 20.00 million of revenue and USD 4.00 million of contribution because implementation is bespoke and senior specialists remain heavily involved. The scaled control-platform case assumes USD 96.00 million of revenue and USD 56.00 million of contribution because reusable connectors, partner delivery and recurring policy workflows improve throughput. These scenarios are illustrative.

Management should reconcile labour classifications to payroll, time records, project plans and support tickets. Product engineering used repeatedly for customer delivery belongs in the economic cost of that revenue. Capitalised development should be reviewed separately from operating contribution. IAS 38 distinguishes research expenditure from development expenditure that meets specified recognition criteria [28]. Formal accounting conclusions require transaction-specific work.

12 Evaluate intellectual property and dependency rights

The target's assets may include source code, detection signatures, connector frameworks, policy taxonomies, test data, migration methods, customer configurations and operational know-how. The buyer should establish ownership through employee and contractor assignments, acquisition records, licences and customer terms. Rights should be linked to the revenue and control loop they support.

Open-source components should be identified through a current software bill of materials, licence scan and release process. Relevant obligations can include attribution, notice, source availability, redistribution or patent terms. The acquirer should test whether the target can distribute its product as currently sold and whether remediation changes architecture or economics.

Customer agreements may assign bespoke deliverables, restrict reuse or require isolated work. Data rights may constrain the use of inventories and telemetry for product improvement. Connector access can depend on third-party APIs and partner agreements. The dependency register should identify termination rights, pricing, support periods, change control and replacement routes.

Patents can support differentiation but do not prove product adoption or freedom to operate. Trade secrets require actual confidentiality controls. The most defensible asset may be the accumulated mapping between cryptographic evidence, enterprise systems, policy and accepted remediation. The buyer should verify that this knowledge is captured in the platform and documentation rather than residing only with a few employees.

13 Model revenue quality and concentration

Revenue quality should be assessed by customer, contract, product, geography, sector and migration stage. Government and critical-infrastructure customers can provide credible demand and long relationships while creating concentration, procurement and security constraints. Channel partners can expand reach while weakening direct customer ownership.

The buyer should reconcile bookings, contracted annual value, recognised revenue, invoices, collections and remaining performance obligations. IFRS 15's performance-obligation framework is relevant to understanding when promised goods and services transfer [17]. The diligence model should identify variable consideration, termination rights, acceptance, service credits, free periods and customer funding dependencies.

Concentration should include delivery concentration. One customer may fund a connector or product module used broadly. Losing that customer can reduce revenue and leave maintenance cost. A small number of partners may control access to regulated accounts. A cloud or hardware provider can affect many customer deployments.

Quality improves when revenue is diversified, contracts are clear, product activity is high, collections are timely, expansion is repeatable and support burden is controlled. A high reported growth rate driven by one implementation programme should not be valued as diversified recurring expansion. The buyer should create a bridge from reported revenue to evidence-qualified recurring revenue.

14 Use valuation evidence states

Valuation should reflect the evidence state reached by the target. The first state is technical capability: working code, specialist staff and demonstrations. The second is deployed control: reconciled customer inventories, active integrations and accepted workflows. The third is recurring economics: contracted subscriptions, production usage, renewal, expansion and contribution. The fourth is scaled platform: diversified customers, partner leverage, efficient support and retained product control.

The hypothetical valuation illustration assigns enterprise values of USD 70.00 million, USD 190.00 million, USD 430.00 million and USD 850.00 million to those four states. Illustrative probabilities of 20%, 35%, 30% and 15% produce a probability-weighted value of USD 337.00 million. These values and probabilities are management assumptions. They are not a valuation conclusion or market evidence.

The purpose of the model is to expose dependencies. A buyer can replace the assumptions with transaction evidence and reconcile enterprise value to cash, debt, working capital, tax and other adjustments. Discounted cash flow, comparable-company analysis and precedent transactions can provide additional perspectives, subject to data quality and comparability.

The evidence-state approach can inform transaction structure. Base consideration can reflect deployed and recurring value. Deferred consideration can depend on production adoption, qualified recurring revenue, contribution, customer retention and key capability retention. Milestones should be measurable, auditable and resistant to post-close allocation disputes.

15 Design commercial diligence tests

Commercial diligence should begin with a reconciled customer population. The team should select cohorts by value, stage, sector, product and renewal date. Each sampled customer should be traced through initial problem, procurement, deployment, activity, outcome, invoice, collection and renewal.

Customer interviews should test the problem solved, alternatives considered, implementation effort, product dependence, quantified benefit, remaining migration plan, renewal rationale and replacement

feasibility. Questions should avoid revealing protected architecture. Responses should be reconciled to contracts, usage and support evidence.

Product tests should use known cryptographic artefacts and production-like constraints. The target should demonstrate discovery, classification, policy, assignment, remediation evidence and export. The team should measure coverage, error, time, permissions and manual intervention. Claims about automation should be separated from analyst work performed behind the interface.

The buyer should also test the negative case. It should identify customers with low activity, stalled implementations, unsupported connectors, disputed invoices, non-renewal or heavy services. These records often reveal product and commercial boundaries more clearly than showcase deployments.

16 Structure integration around customer control

Integration can damage value if the acquirer changes access, architecture, branding, support or independence before understanding customer constraints. The first priority is continuity of people, systems, credentials, service levels, project milestones and customer communication.

The first hundred days should reconcile the product roadmap, signed commitments, delivery capacity, security controls, support queue and financial reporting. Customer-specific restrictions should be mapped before consolidating infrastructure or data. Key employees should understand roles, incentives and decision rights.

Commercial integration should preserve the target's evidence while opening distribution. Cross-selling should follow validated use cases and delivery capacity. Bundling can simplify procurement, but it can also obscure price and create support obligations. The combined company should define a common control model and a disciplined connector roadmap.

Value-creation measures should include active governed assets, inventory reconciliation, time to deploy, production changes, renewal, expansion, contribution, support burden and partner throughput. Revenue alone can reward low-quality implementation. Technical activity alone can reward unused features. The combined scorecard should connect customer outcomes to cash.

17 Allocate transaction risk explicitly

The purchase agreement and operating plan should address rights, security, revenue, delivery, people and dependencies. Intellectual-property defects may require remediation, specific indemnity or a closing condition. Customer consents and change-of-control clauses should be mapped. Security findings should be prioritised by exposure and customer impact.

Working-capital analysis should consider annual prepayments, deferred revenue, contractor timing, customer acceptance and implementation obligations. Revenue quality should inform price and earn-out definitions. Measures should specify treatment of discounts, bundling, acquired customers, currency, bad debt and buyer decisions.

Retention arrangements should focus on capability required to serve customers and maintain the platform. Restrictive terms require jurisdiction-specific legal advice. A broader operating environment, including autonomy, technical standards, resources and customer access, often determines whether key people remain effective.

Representations cannot replace diligence. A buyer should price the evidence it has, place conditions around remediable gaps and reserve deferred value for outcomes that remain genuinely future-dependent.

18 Investment committee decision framework

The investment committee should receive a one-page evidence map alongside the valuation. The map should state the customer's recurring control problem, the platform boundary, verified integrations, qualified recurring revenue, cohort economics, delivery capacity, switching-cost evidence, rights, security status and principal dependencies.

The committee should distinguish three questions. Is the market need credible? Does this target convert the need into accepted customer outcomes? Can the buyer preserve and scale those outcomes at the proposed price? Official migration policy can support the first question. Customer and operating evidence must answer the second and third.

Approval conditions should identify the evidence that must exist at signing and closing. Post-close milestones should focus on unresolved scale assumptions. The model should include downside cases for slower migration, services intensity, connector maintenance, delayed standards, customer concentration and key-person loss.

The strongest acquisition thesis is specific: the target maintains an enterprise control layer that reduces measured migration work, remains active after initial transition, expands through additional governed systems and produces contribution with controlled risk. A broad claim about inevitable post-quantum spending is insufficient.

The committee should also require a reporting cadence that can survive ownership change. Monthly reporting should reconcile contracted value, recognised revenue, invoices and cash with deployment, product activity, support and delivery effort. Quarterly reporting should show customer cohorts, renewal decisions, connector reliability, security findings, roadmap commitments and capacity. Material exceptions should have accountable owners, approved treatments and closure dates.

The reporting design matters because platform economics can deteriorate before reported revenue changes. A connector can become unreliable while an annual contract remains in force. Support tickets can rise before churn. Senior engineers can absorb implementation work that is recorded within product development. Customer inventories can become stale while licence counts remain constant. The buyer needs operational measures that identify these conditions early.

Board measures should therefore combine financial, customer, product and risk evidence. Financial measures include qualified recurring revenue, contribution, collections and cash conversion. Customer measures include time to deploy, active governed systems, renewal and expansion. Product measures include connector reliability, inventory reconciliation, policy activity and accepted changes. Risk measures include security remediation, dependency exposure, concentration and key capability retention. Definitions should be frozen at closing and changed only through documented governance.

This evidence architecture also supports deferred consideration. If an earn-out depends on recurring revenue, the agreement should specify the related contracts, exclusions, recognition rules, customer credits and buyer allocation decisions. If it depends on production adoption, the agreement should define the governed system, required activity, acceptance evidence and measurement period. Clear definitions reduce disputes and keep management focused on customer outcomes that support value.

Conclusion

Crypto-agility platforms sit at the intersection of standards, cybersecurity operations and enterprise change. Their addressable need can extend across multiple algorithm and protocol transitions. Their valuation depends on verified customer economics.

An acquirer should trace value from inventory coverage to governed decisions, production changes, continuing control, renewal, expansion and cash. It should test integration depth through active evidence,

switching costs through portability and replacement work, and recurring revenue through contracts, usage and contribution. It should allocate hidden services and dependency costs to the economic unit they support.

The proposed framework links valuation to evidence states. Technical capability creates an option. Deployed control creates customer relevance. Recurring economics create durability. A scaled platform creates operating leverage. Transaction price and structure should follow the state demonstrated at diligence and reserve future value for future evidence.

Frequently asked questions

What is a crypto agility platform

It is a product or service layer that helps an organisation discover cryptographic use, define policy, plan and execute changes, test outcomes and maintain evidence as algorithms, protocols and products change. The exact boundary must be verified for each vendor.

Why can post quantum migration support recurring demand

The initial transition spans multiple systems, suppliers and years. Continuing inventory, policy monitoring, certificate and key changes, protocol updates and assurance can remain after the first migration. Recurrence depends on the contracted service and active customer use.

Which metric best shows integration depth

No single metric is sufficient. Active authenticated connectors, reconciled governed assets, policy workflows, production changes, accountable users and recurring customer outcomes should be considered together.

When should implementation revenue be treated as recurring

Implementation is project revenue unless the contract and delivery model establish a continuing obligation. A renewable project or retainer does not automatically have software-like recurring economics.

What creates defensible switching costs

Defensible switching costs arise from embedded workflows, maintained evidence, trusted control, replacement work and operational dependency. Reasonable exportability and customer ownership strengthen trust. Poor portability can create commercial and regulatory risk.

How should a buyer test claimed labour savings

The buyer should establish the customer's baseline activities, hours, rates, volumes and rework, then compare them with post-deployment records. Platform fees, implementation, residual labour and support should be deducted from gross savings.

Which outcomes can support deferred consideration

Production adoption, qualified recurring revenue, renewal, expansion, contribution, efficient deployment, customer retention and retention of critical capability can be measured. Definitions should specify buyer actions, allocations and evidence.

What should happen during the first hundred days

The acquirer should protect people, access, customer commitments and security controls; reconcile contracts, activity and economics; integrate connectors and governance carefully; and scale only after verified delivery capacity and customer evidence support it.

Appendix A. Customer evidence request

The buyer should request a customer register showing contract start, product, recurring and services value, implementation status, active connectors, governed assets, policy use, production changes, support effort, invoices, collections, renewal, expansion and customer owner. Contract files should include statements of work, amendments, acceptance, service levels, termination, data rights and change-of-control terms.

For a representative sample, the target should provide a trace from discovery evidence to a closed remediation. The trace should show the original artefact, business context, policy decision, responsible owner, technical change, test, approval and continuing monitoring. Customer confirmation should be obtained through an agreed and secure process.

Appendix B. Product and architecture evidence request

The product pack should include architecture, data model, connector catalogue, active deployment counts, permissions, error rates, release history, roadmap, security model, dependency register, software bill of materials, licence scan, vulnerability process and validation claims. The buyer should distinguish product capability from analyst-assisted outputs.

A controlled demonstration should use known cryptographic artefacts across representative environments. It should test discovery, reconciliation, policy, workflow, export, access control and audit history. Results should be retained as transaction evidence.

Appendix C. Operating model and capacity request

The operating pack should reconcile organisation chart, payroll, contractors, partner capacity, project plans, timesheets, support queue, engineering allocation, cloud cost and customer profitability. It should identify key approvals, succession, customer restrictions and hiring requirements.

Capacity should be built from named resources and demonstrated product automation. Forecast hiring and partner leverage should remain separate from current capacity. The model should include connector maintenance, standards updates, security work and customer support.

Appendix D. Valuation bridge

The valuation bridge should begin with reported revenue and reconcile to qualified recurring revenue, project revenue, managed service, variable consideration and non-recurring items. Contribution should include product infrastructure, delivery labour, partner fees, customer success, support and recurring engineering used for customer obligations.

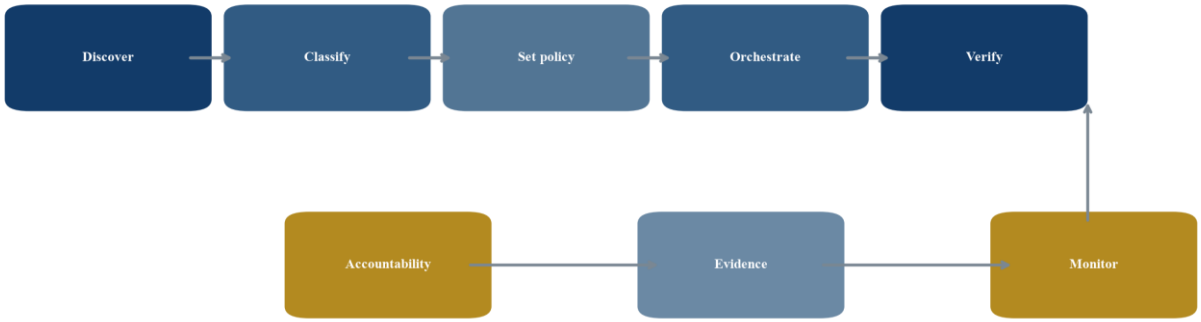
The buyer should model services-heavy, central and scaled cases. Evidence-state probabilities can express uncertainty while retaining a clear view of the assumptions. Enterprise value should then be reconciled to transaction-specific cash, debt, working capital, tax and other adjustments.

Appendix E. Transaction evidence hierarchy

External standards and policy establish direction. Customer strategy and budget establish intent. Signed contracts establish committed scope subject to their terms. Active integrations establish deployment. Accepted production changes establish delivery. Invoices and collections establish commercial conversion. Renewal, expansion and stable contribution establish repeatability.

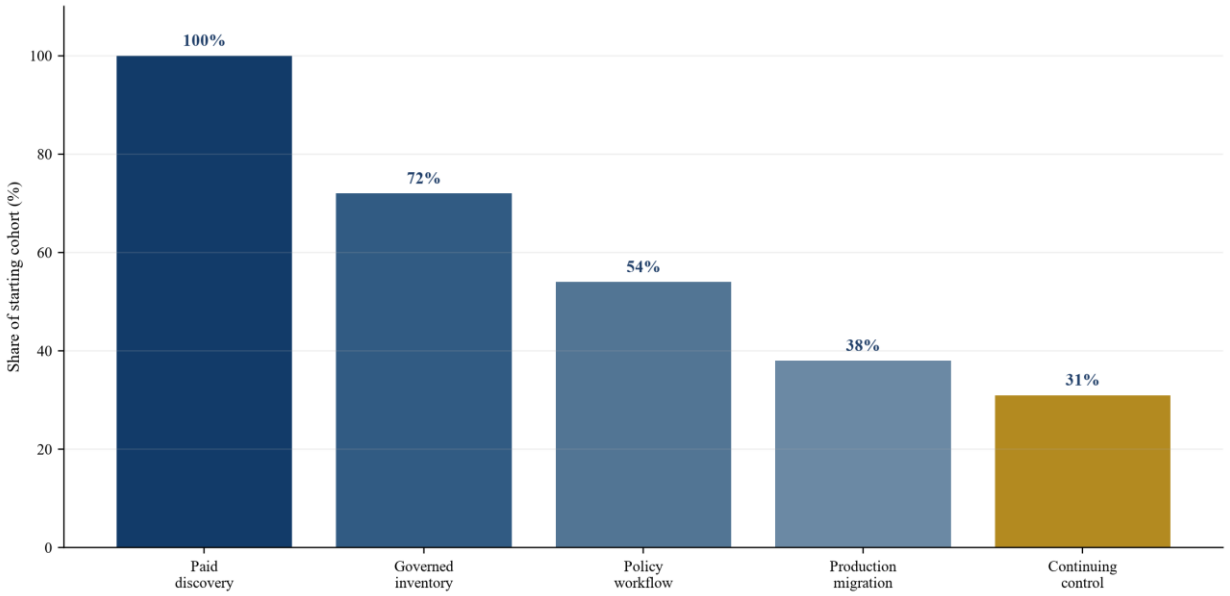
Each level answers a separate question. A premium should reflect the levels already achieved. Deferred consideration can address outcomes that remain future-dependent.

Figure 1 Crypto agility platform enterprise control loop



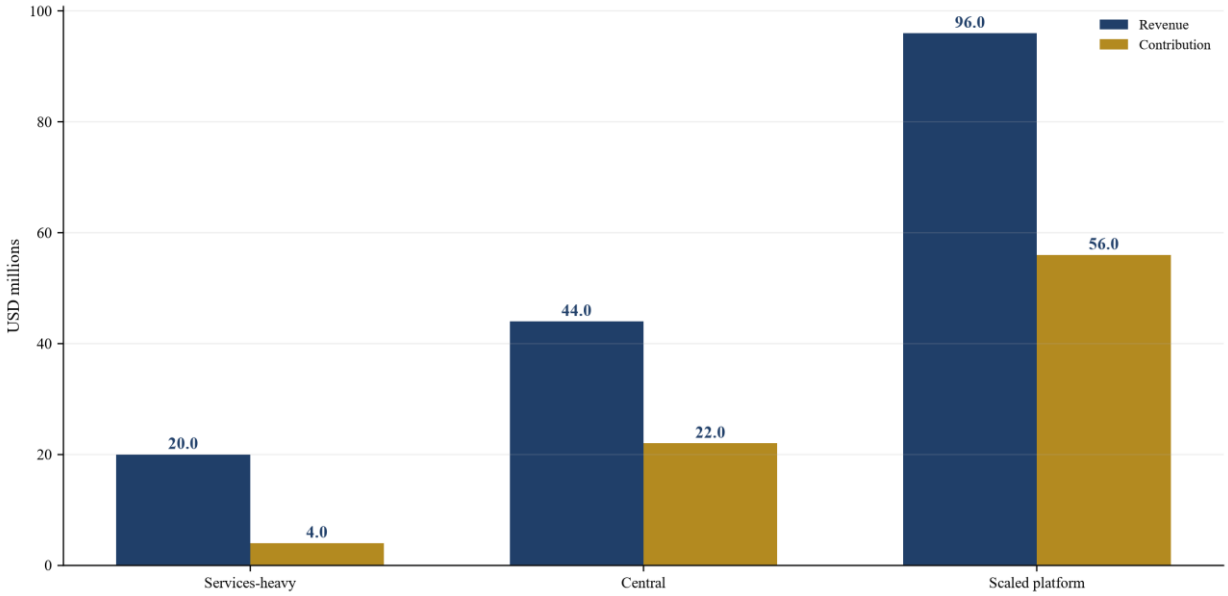
Proposed framework; customer and target evidence is required for every stage.

Figure 2 Hypothetical customer progression from discovery to continuing control



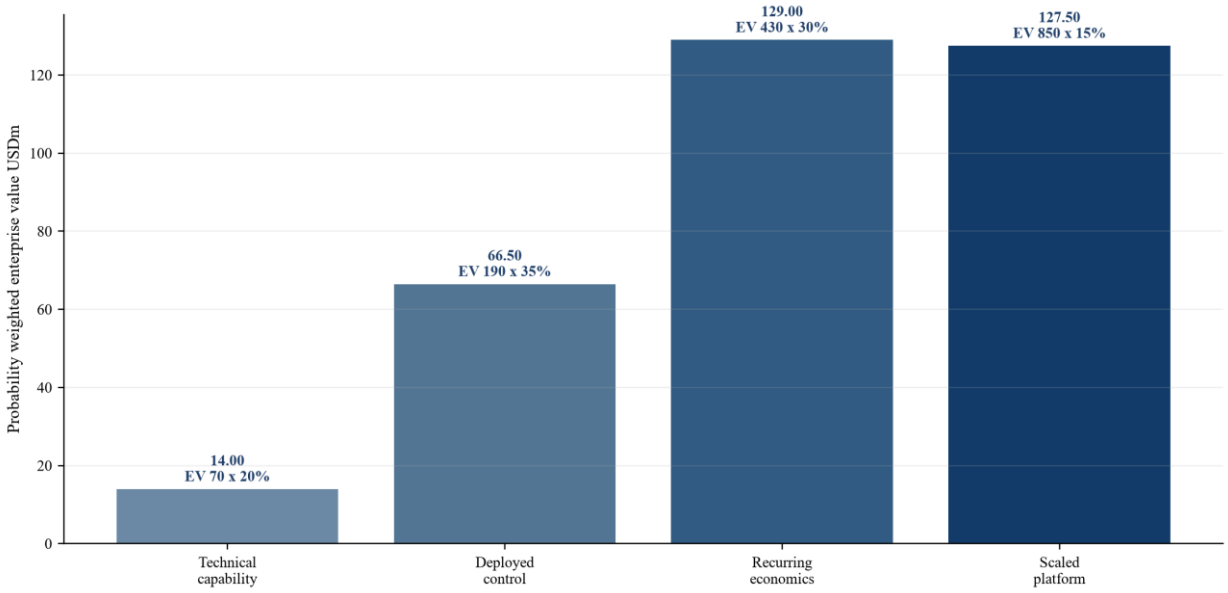
Management assumptions; percentages are illustrative and are not market observations.

Figure 3 Hypothetical annual revenue and contribution by operating case



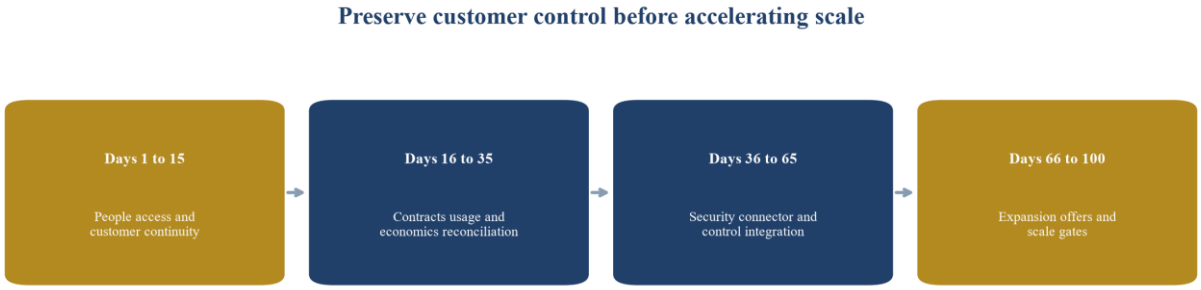
Management assumptions in USD millions; excludes central overhead tax financing and integration.

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 customer-control integration sequence



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

Table 1 Enterprise migration need and valuation evidence

Signal	Enterprise implication	Platform opportunity	Required valuation evidence
NIST post-quantum standards	Product and protocol transition	Inventory policy and migration control	Accepted production use
NCSC 2028 2031 2035 milestones	Multi-year planning and execution	Continuing workflow and evidence	Funded customer roadmap
US federal inventory direction	Recurring discovery and reporting	Maintained system of record	Verified coverage and refresh
EU coordinated roadmap	Cross-border sequencing	Policy and assurance	Customer applicability and budget
Protocol and supplier change	Interoperability dependencies	Dependency mapping and testing	Maintained connectors and evidence

External signals establish direction; target-specific conclusions require separate verification.

Table 2 Recurring revenue evidence hierarchy

Evidence level	Contract evidence	Product evidence	Valuation treatment
Labelled subscription	Invoice and term	Low or unknown activity	Verify before classification
Active deployment	Contracted access	Reconciled integrations and users	Qualified recurring base
Embedded control	Renewal and expansion	Policy workflow and production actions	Durability premium subject to economics
Scaled platform	Diversified cohorts	Efficient support and partner leverage	Platform case subject to retention

Proposed classification for transaction diligence.

Table 3 Integration depth diligence test

Dimension	Measure	Strong evidence	Warning signal
Technical	Active authenticated connectors	Reliable governed data flows	Marketing-only connector count

Dimension	Measure	Strong evidence	Warning signal
Workflow	Assignments approvals and exceptions	Closed evidence-linked actions	Reports exported to spreadsheets
Organisational	Teams and business units	Multiple accountable owners	One champion only
Economic	Work and risk routed through product	Measured savings and renewal	Contractual inertia
Portability	Export and replacement route	Documented formats and APIs	Customer data trapped

Proposed buyer test for representative customer deployments.

Table 4 Hypothetical central annual economics

Revenue or cost item	Revenue	Direct cost	Contribution
Subscription and usage	28.00	9.00	19.00
Managed control	8.00	5.00	3.00
Implementation and advisory	8.00	8.00	0.00
Total	44.00	22.00	22.00

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

Table 5 Hypothetical operating cases

Case	Revenue	Contribution	Principal condition
Services-heavy	20.00	4.00	Bespoke deployment and scarce specialist effort
Central	44.00	22.00	Embedded control with measured implementation
Scaled platform	96.00	56.00	Reusable connectors partner throughput and expansion

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

Table 6 Hypothetical valuation evidence states

Evidence state	Enterprise value	Probability	Weighted value
Technical capability	70.00	20%	14.00
Deployed control	190.00	35%	66.50
Recurring economics	430.00	30%	129.00
Scaled platform	850.00	15%	127.50
Total		100%	337.00

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

Table 7 Acquisition gate and transaction response

Gate	Required evidence	Transaction response	Post-close measure
Rights	Ownership licences and customer permissions	Condition remediation or indemnity	Rights closure
Deployment	Active reconciled customer integrations	Base consideration	Governed assets and uptime

Gate	Required evidence	Transaction response	Post-close measure
Recurrence	Contracts usage renewal and collection	Revenue quality adjustment	Retention and expansion
Economics	Contribution after delivery and support	Valuation adjustment	Contribution and cash conversion
Scale	Reusable connectors partners and capability	Deferred consideration	Efficient deployment and support

Proposed framework; legal tax accounting and security terms require qualified advice.

References

[1] National Institute of Standards and Technology. Crypto Agility Project. 2026. https://csrc.nist.gov/projects/crypto-agility

[2] National Institute of Standards and Technology. CSWP 39 Considerations for Achieving Crypto Agility Strategies and Practices. 2025. https://csrc.nist.gov/pubs/cswp/39/final

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

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

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

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

[7] National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography. 2026. https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

[8] 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

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

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

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

[12] 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

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

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

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

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

[17] IFRS Foundation. IFRS 15 Revenue from Contracts with Customers. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[18] National Telecommunications and Information Administration. Minimum Elements for a Software Bill of Materials. 2021. https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

[19] Cybersecurity and Infrastructure Security Agency. Software Bill of Materials. 2026. https://www.cisa.gov/sbom

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

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

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

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

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

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

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

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

[28] IFRS Foundation. IAS 38 Intangible Assets. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[29] IFRS Foundation. IFRS 3 Business Combinations. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[30] United States Securities and Exchange Commission. Cybersecurity Risk Management Strategy Governance and Incident Disclosure. 2023. https://www.sec.gov/rule-release/33-11216

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

[32] National Institute of Standards and Technology. What Is Post-Quantum Cryptography. 2026. https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography

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.