Finance the Quantum-Safe Network: Telecom Investment Before Migration Deadlines

A capital-allocation framework for funding post-quantum migration across operator networks

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Telecommunications operators face a large cryptographic change programme whose cost, timing and commercial return do not fit neatly inside a normal network-refresh cycle. Post-quantum cryptography standards now provide an implementable destination. Migration still requires discovery across software, firmware, network equipment, identity, signalling, operations, suppliers and customer products. The United Kingdom's National Cyber Security Centre asks organisations to complete discovery and an initial plan by 2028, migrate the highest-priority services by 2031 and complete migration by 2035. NIST has published the first principal post-quantum standards and describes 2035 as the point by which quantum-vulnerable algorithms are to be deprecated and removed from its standards, with higher-risk systems moving earlier. These dates turn cryptographic readiness into an investment, procurement and execution problem.

This paper develops the Quantum-Safe Network Financing Framework for telecom boards, chief financial officers, chief technology officers, lenders, infrastructure investors and strategic partners. It translates a security migration into financeable work packages. The framework begins with a cryptographic asset register and a service-criticality map. It then separates mandatory remediation from growth-enabling modernisation, assigns migration waves to the underlying asset lifecycle, identifies supplier and interoperability dependencies, and links capital release to verifiable technical and commercial milestones. Four tables and three figures provide a repeatable method for defining the investment perimeter, allocating capital, selecting financing instruments and governing delivery.

The paper argues that anchor operators can improve bankability by aggregating demand, publishing interface requirements, creating reference architectures and committing to staged acceptance volumes. Financing should follow controlled migration cells rather than one undifferentiated transformation budget. Long-lived network equipment, roots of trust and regulated services deserve early funding because replacement lead times can exceed ordinary budgeting horizons. Software and protocol changes can be staged through crypto-agile platforms where rollback, telemetry and interoperability are demonstrable. Vendor finance, sustainability-linked facilities, asset-backed structures and strategic co-investment can support defined components, while core security obligations remain governed by the operator.

A wholly hypothetical operator case demonstrates the method. Every amount, timetable, customer characteristic, probability and financing outcome in the case is an illustrative management assumption. The analysis shows how a board can reconcile deadline risk, service continuity, supplier readiness and investment capacity. The central conclusion is that post-quantum migration becomes financeable when the operator defines a bounded asset perimeter, measurable acceptance tests,

accountable cost ownership and a credible route from early anchor demand to repeatable deployment.

JEL Classification: G31, G32, L51, L96, O32, O33

Keywords: post-quantum cryptography, telecom investment, network modernisation, crypto-agility, capital allocation, infrastructure finance, migration deadlines, cybersecurity, technology financing

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE BOARD DECISION

The board decision concerns the timing, perimeter and funding of a network-wide cryptographic migration. It must establish which services require early action, which assets can move through normal refresh, which supplier dependencies need intervention and which expenditure creates reusable capability. A broad instruction to become quantum safe does not provide a capital plan. The investment case needs a dated sequence of assets, service outcomes and acceptance conditions.

The operator should begin with four questions. Which information and control functions need protection for the longest period? Which network components use public-key cryptography or depend on certificates, signatures and key exchange? Which dependencies have replacement lead times that approach policy milestones? Which customer or regulatory commitments can support an accelerated programme? These questions align security risk with asset management and funding capacity.

The decision paper should distinguish obligation, resilience and opportunity. Obligation covers the migration needed to maintain compliant and supportable services. Resilience covers crypto-agility, inventory, testing, telemetry and operating controls that reduce future change cost. Opportunity covers managed quantum-safe services, premium enterprise connectivity and public-sector demand. Each category requires its own evidence and return logic.

Table 1. The quantum-safe network investment perimeter

Investment layer	Primary question	Evidence required	Financing implication
Cryptographic discovery	Where are vulnerable algorithms, keys, certificates and dependencies used?	Complete inventory, ownership, service mapping and data-lifetime assessment	Fund centrally because discovery enables every later work package
Network and platform migration	Which hardware, software and protocols need replacement or upgrade?	Vendor roadmaps, test results, lifecycle dates, interoperability and rollback	Match capital tenor to asset life and migration wave
Customer products	Which services require contract, device or application change?	Customer cohorts, product architecture, consent, acceptance and revenue exposure	Use anchor demand and staged volumes to support incremental investment
Operations and assurance	Can the migrated estate be monitored, governed and recovered?	Telemetry, incident process, certificate lifecycle, conformance and audit evidence	Treat as enduring operating capability, not a one-time project cost
Ecosystem coordination	Are suppliers and interconnect partners ready on compatible dates?	Interface baseline, dependency register, procurement commitments and joint tests	Use shared testbeds, framework agreements and milestone-linked commitments

Each layer should have a named owner, asset inventory, acceptance test, target wave and funding source.

2. CONVERT STANDARDS INTO AN INVESTMENT CLOCK

NIST approved FIPS 203, FIPS 204 and FIPS 205 in August 2024. These standards cover a key-encapsulation mechanism and two digital-signature methods designed to resist attacks by future quantum computers. Their publication supplies a practical basis for product roadmaps, protocol work, procurement specifications and validation. The standards do not complete the migration. Operators must still identify where cryptography is embedded and how changed algorithms affect performance, interoperability and operations.

The NCSC's migration milestones create a useful planning clock. By 2028, organisations should complete discovery, define goals and build an initial migration plan. By 2031, they should complete the highest-priority activities and refine the route to completion. By 2035, they should complete migration across systems, services and products. The NCSC states that discovery and planning can take two to three years for large organisations, followed by a similar period for early migration.

Capital planning should work backwards from these milestones. Network equipment ordered today can remain deployed into the 2030s. Software incorporated into customer premises equipment can be difficult to replace after shipment. Certificates and signatures can protect long-lived firmware, identities and records. The investment clock therefore begins with the procurement and design decisions that create future lock-in.

3. TREAT THE PROGRAMME AS INFRASTRUCTURE MODERNISATION

Post-quantum migration affects network infrastructure, digital platforms and operating procedures. Telecom assets span radio access, transport, core, cloud, data centres, satellites, subsea systems, operational support, billing, identity and customer devices. Cryptography

appears in management planes, signalling, authentication, software signing, virtualisation, APIs and enterprise products. A migration programme must coordinate these systems without disrupting service.

Infrastructure-finance discipline improves the programme. The operator should define assets, useful lives, construction or implementation risk, counterparties, completion tests, operating obligations and sources of repayment. Some expenditure extends asset life or enables a new service. Some prevents stranded equipment or service withdrawal. Some represents ongoing security operations. Classification affects governance and financing.

The programme should be divided into migration cells. A cell combines a bounded service, asset cohort, vendor set, interface baseline, test environment, deployment wave and acceptance authority. Capital can be committed to a cell when its dependencies and completion tests are understood. This approach creates evidence for the next wave and limits the financial effect of technical delay.

4. BUILD A CRYPTOGRAPHIC ASSET REGISTER

A cryptographic asset register records algorithms, protocols, keys, certificates, libraries, hardware modules, signing processes, trust anchors and external services. It should connect each item to a business service, system owner, data type, supplier, deployment location and lifecycle date. Automated discovery can assist, but source-code, configuration, hardware and third-party reviews remain necessary.

The register should identify confidentiality and authenticity horizons. Information that must remain confidential for many years can face harvest-now-decrypt-later exposure. Firmware and software signatures may need to remain trustworthy for the full operating life of equipment. Root certificates can support large populations of devices. These horizons help rank investment before exact quantum-computer timing is known.

Financing depends on the register's quality. A lender or investment committee cannot assess completion risk when the asset base is unknown. The discovery workstream should therefore be a funded phase with measurable coverage, exception treatment and management attestation. Its output becomes the quantity survey for the migration programme.

5. MAP CRYPTOGRAPHY TO CUSTOMER AND NETWORK SERVICES

An algorithm inventory alone does not show commercial importance. The operator should map cryptographic dependencies to services such as mobile authentication, enterprise VPN, managed security, roaming, interconnect, cloud connectivity, network slicing, IoT management, emergency communications and critical-infrastructure links. The map should identify revenue, contractual service levels, regulated functions and customer switching constraints.

Service mapping prevents low-value components from absorbing attention while a critical dependency remains hidden. A library used in a test environment has a different priority from a root of trust used to sign network firmware. A management interface with privileged access can matter more than its hardware cost suggests. Priority follows the consequence and duration of compromise.

The service map also identifies financing support. Enterprise and public-sector customers may fund premium migration, testing or dedicated assurance. Wholesale partners may share

interconnect work. Consumer products may require operator-funded change because individual willingness to pay is limited. The investment case should state the beneficiary, payment mechanism and evidence.

6. ESTABLISH THE BASELINE COST MODEL

The baseline should include discovery, architecture, laboratories, vendor development, licences, hardware, integration, certification, deployment, customer migration, training, spares, programme management and contingency. It should distinguish capital expenditure from operating expenditure according to applicable accounting policy. It should also record internal labour and opportunity cost.

Cost estimates should be organised by asset cohort and migration cell. Unit costs can then be tested against quantities and deployment rates. The model should identify supplier assumptions, foreign exchange, inflation, lead times and minimum orders. A central contingency can obscure weak estimates; risk allowances should sit beside the dependency that creates them.

The baseline needs a counterfactual. Normal lifecycle replacement may already fund part of the work. Security migration can accelerate replacement, require a more capable platform or change implementation effort. The incremental quantum-safe cost is the difference between the approved lifecycle plan and the migration-compliant plan, including timing and stranded-asset effects.

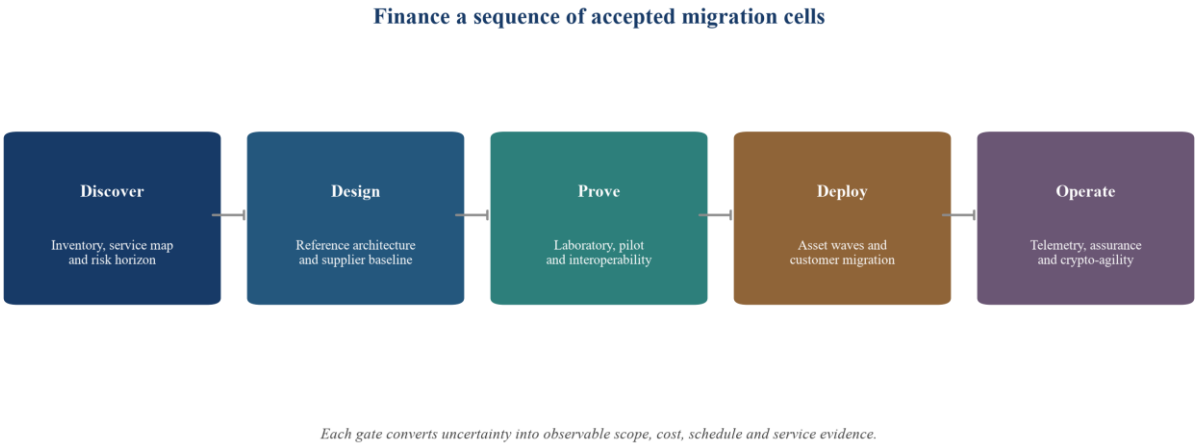


Figure 1. A staged quantum-safe network investment architecture

Capital is released as discovery, interoperability and acceptance evidence improves.

7. ALIGN MIGRATION WITH ASSET LIFECYCLES

Asset age, support status and replacement lead time should shape migration waves. Equipment close to retirement can move through planned refresh if the replacement is quantum-safe capable. Recently deployed assets may need firmware, module or overlay changes. Long-lived specialised equipment may require early redesign because a replacement market does not yet exist.

The operator should create a lifecycle matrix covering end of sale, end of support, certificate life, software-maintenance term and physical replacement window. It should test whether vendor

roadmaps align with internal deadlines. A promise of future support has limited financing value without a version, date, price, performance envelope and contractual remedy.

Lifecycle alignment can reduce stranded value. It can also create concentration risk when many assets reach a migration window at once. Procurement should reserve manufacturing and engineering capacity before demand peaks. The capital plan should show prepayments, inventory, working capital and storage requirements where supply capacity is constrained.

8. PRIORITISE LONG-LIVED ROOTS OF TRUST

Roots of trust, code-signing systems, certificate authorities, subscriber identity systems and device-manufacturing credentials can remain embedded for long periods. Their compromise can affect entire device populations or software chains. Migration may require secure ceremonies, hardware modules, new enrolment, dual signatures and coordinated field updates.

These assets deserve early design funding even when deployment occurs later. The operator should determine whether current hardware supports new algorithms, whether signature size affects firmware or protocols, and whether old and new trust chains can coexist. Recovery from a failed trust migration can be operationally severe.

The financing model should recognise the asymmetry. A trust-system upgrade may produce limited direct revenue while protecting a large asset and customer base. Its return is continuity and avoided remediation. The board should fund it through core resilience capital and require strong assurance, independent testing and executive ownership.

9. ASSESS NETWORK-EQUIPMENT READINESS

Network equipment includes routers, gateways, radio systems, security appliances, management platforms and customer-premises devices. Post-quantum changes can affect secure boot, firmware signing, management sessions, VPNs and control-plane protocols. The operator should obtain vendor-specific roadmaps rather than rely on product-family statements.

Testing should measure processing load, memory, packet size, handshake latency, certificate handling, failover and mixed-mode operation. Larger keys and signatures can expose assumptions in constrained devices and protocols. A laboratory result should specify hardware, software, configuration, traffic and error conditions.

Procurement should require crypto-agility, algorithm inventory, software-bill-of-material visibility, supported migration paths and vulnerability response. Equipment bought before the migration plan is complete should include contractual upgrade rights. The cost of these rights belongs in the investment case because it protects future optionality.

10. UNDERWRITE SOFTWARE AND PROTOCOL CHANGE

Many migration activities occur in software, firmware and protocols. The apparent absence of physical construction does not remove programme risk. Operators depend on large code estates, open-source libraries, cloud services and vendor release trains. A change in one cryptographic primitive can affect authentication, message size, storage, performance and compatibility.

The operator should maintain a protocol compatibility matrix. It should identify versions that support hybrid or post-quantum mechanisms, the endpoints that must change together and the

consequences of negotiation failure. Rollback should preserve a known security state rather than silently return to a weak algorithm.

Software work can be financed as a reusable platform when it creates inventory, policy, orchestration, telemetry and testing capabilities across services. Bespoke remediation with no reusable component should remain attributed to the affected service. This distinction improves accountability and prevents a platform budget from absorbing unrelated work.

11. BUILD CRYPTO-AGILITY AS AN INVESTABLE CAPABILITY

Crypto-agility is the capacity to identify, change, test and govern cryptographic mechanisms without rebuilding the whole service. It includes abstraction, policy, inventory, automated certificate lifecycle, configurable algorithms, interoperability testing and operational telemetry. It does not mean uncontrolled algorithm switching.

The capability can reduce the cost of future standards changes and vulnerability response. Its value should be demonstrated through cycle time, coverage, rollback, defect rates and supported systems. The operator should avoid a broad platform project whose benefits remain unmeasured.

Investment can be staged. The first release can cover high-priority services and a limited algorithm set. Later releases can extend coverage after the operating model is proven. Milestone funding should depend on completed integrations and exercised change procedures, not feature counts alone.

12. USE HYBRID MIGRATION DELIBERATELY

Hybrid mechanisms combine established and post-quantum methods during transition. They can support compatibility and reduce dependence on a single new primitive. They also add complexity, processing, message size and failure modes. The operator should define the security property expected from the combination and how downgrade is prevented.

Hybrid deployment may be appropriate where both endpoints can be upgraded and service continuity is critical. It can provide evidence before a complete cutover. The design should specify negotiation, key derivation, authentication, certificate handling, telemetry and incident response.

The financial model should avoid counting hybrid operation as costless insurance. Dual stacks require testing, support and operational skill. Their value comes from controlled transition and reduced cutover risk. The programme should retire transitional complexity when policy and interoperability permit.

13. CREATE THE OPERATOR REFERENCE ARCHITECTURE

A reference architecture defines approved patterns for key establishment, signatures, certificates, trust, algorithm negotiation, hardware security and operations. It should cover network layers, cloud environments, APIs, customer products and external interconnect. It should also describe prohibited patterns and exception governance.

The architecture turns fragmented vendor proposals into comparable solutions. Suppliers can design against stable interfaces, laboratories can build repeatable tests and procurement can price defined outcomes. Changes should be versioned and communicated because an unstable baseline transfers cost into bids and integration.

An anchor operator can use the architecture to organise ecosystem demand. Publishing non-sensitive requirements helps vendors invest in compatible products. Joint testing with equipment providers, cloud platforms and enterprise customers can create evidence that supports larger purchase commitments and external financing.

14. FINANCE LABORATORIES AND SHARED TESTBEDS

Laboratories are core infrastructure for migration. They need representative equipment, traffic, identity systems, management tools, automation, attack testing and performance measurement. A narrow cryptographic benchmark cannot show service behaviour under load, failover or mixed versions.

Shared testbeds can reduce duplication across operators and suppliers when governance protects sensitive information and commercial rights. Industry bodies, government programmes and research institutions may support common conformance work. Operator-specific integration and acceptance remain necessary.

The laboratory budget should have outputs: supported configurations, defect registers, performance envelopes, interoperability reports and deployment runbooks. Capital should be released when these artefacts reach agreed quality. Reusable test automation can become an enduring asset that lowers the cost of later waves.

15. AGGREGATE ANCHOR DEMAND

Suppliers invest faster when demand is specific, timed and credible. An anchor operator can publish volume bands, interface requirements, acceptance criteria and procurement windows. A group of operators can align common requirements while preserving commercial competition. This reduces the risk that each vendor builds a bespoke implementation.

Anchor demand should be conditional on evidence. Framework agreements can reserve capacity and establish prices, while call-off orders follow conformance and service tests. Minimum commitments can be staged across asset cohorts. Remedies should address missed roadmaps and unsupported equipment.

The financing benefit is substantial. Committed demand can support vendor working capital, production tooling and development facilities. It can also support special-purpose deployment vehicles for defined infrastructure. The operator should avoid commitments that transfer technical risk back without control or visibility.

Table 2. Financing instruments for quantum-safe network work packages

Instrument	Suitable work package	Required evidence	Principal risk control
Corporate capital budget	Discovery, architecture, trust systems and core obligations	Board-approved perimeter, milestones and accountable owner	Stage gates, independent assurance and benefits tracking
Vendor finance	Equipment upgrades and committed deployment waves	Accepted specification, volume, delivery dates and support	Payment on acceptance, warranty, roadmap remedies and step-in rights
Term loan or revolving facility	Broad modernisation with predictable spend	Approved capex plan, liquidity headroom and reporting	Draw conditions, covenants, cost-to-complete and contingency
Asset-backed or lease structure	Separable equipment with identifiable useful life	Title, residual value, maintenance and deployment schedule	Asset eligibility, insurance, replacement and technology-obsolescence tests
Strategic co-investment	Shared laboratories, platforms or managed services	Governance, rights, demand commitments and monetisation route	Reserved matters, IP allocation, exit and service-level protections
Sustainability-linked financing	Wider resilience programme with credible security metrics	Measurable targets, independent verification and material economics	Clear baselines, anti-greenwashing controls and limited metric complexity

Instrument choice should follow asset ownership, useful life, cash-flow support and completion risk.

16. SELECT FINANCING BY ASSET AND RISK

Core security obligations normally remain on the operator's balance sheet because service continuity and control are central. Vendor finance can support equipment where specifications, acceptance and support are clear. Loans can fund a broader modernisation programme when cost and liquidity are predictable. Leasing or asset-backed structures require separable equipment, enforceable rights and credible residual value.

Strategic co-investment may suit shared test infrastructure, managed-security platforms or wholesale services. The vehicle needs clear governance, intellectual-property rights, service obligations and exit mechanics. A structure should not separate an asset from the operator when operational control remains inseparable.

Financing tenor should follow useful life and milestone risk. Short-lived software or discovery work should not be funded through long-dated asset debt merely to reduce annual cash expense. Long-lived equipment can support longer tenor after technical acceptance. Construction-like risk belongs in staged draws and completion protection.

17. DEFINE MILESTONE-LINKED CAPITAL RELEASE

Milestones should represent completed risk reduction. Examples include verified asset-inventory coverage, approved architecture, successful multi-vendor interoperability, performance within threshold, customer acceptance and stable operation over a defined period. A document submission alone rarely proves completion.

Each milestone needs an evidence owner and acceptance authority. The programme should record the configuration tested, defects accepted, exceptions granted and dependencies remaining. Financial reporting should connect committed, spent and forecast cost to the same work-breakdown structure.

Milestone-linked capital protects the programme from premature scale. It also creates a learning loop. A completed cell updates unit cost, deployment rate, defect expectations and supplier performance. The next tranche can be resized before the operator repeats an error across the estate.

18. PROTECT LIQUIDITY AND CONTINGENCY

Migration competes with spectrum, coverage, cloud, energy and normal lifecycle investment. The board should model the programme within liquidity headroom and downside scenarios. It should include vendor delay, accelerated replacement, customer support, parallel operation and regulatory change.

Contingency should be allocated by risk rather than held as a single percentage. Hardware obsolescence, protocol redesign, supplier failure and deployment productivity have different triggers and responses. The programme should release contingency through governance that preserves urgency.

Cash-flow timing matters. Prepayments may secure scarce equipment or development capacity. Customer migration can create temporary support peaks. Delayed acceptance can shift revenue or grant reimbursement. Treasury should model these timing effects alongside accounting cost.

19. GOVERN SUPPLIER ROADMAPS

Supplier readiness is a portfolio risk. The operator should maintain a roadmap register with product, version, algorithm support, validation, release date, upgrade method, performance and contractual commitment. It should identify where multiple critical services depend on one vendor or component.

Roadmap statements should be converted into procurement terms. The operator can require delivery milestones, source-code escrow where appropriate, extended support, migration tooling, test participation and remedies. Vendor concentration can be addressed through second sources, interface standards and inventory.

The governance forum should include technology, security, procurement, legal, finance and operations. A delayed roadmap can change asset life, capex and service risk. The response should be an investment decision rather than an isolated supplier-management issue.

20. COORDINATE INTERCONNECT AND ROAMING

Telecom services cross organisational boundaries. Interconnect, roaming, wholesale access, cloud exchange and managed enterprise services require compatible endpoints and trust. One operator cannot complete migration unilaterally when the service depends on another party's protocol and schedule.

The programme should catalogue external dependencies and establish joint test plans. Industry specifications can reduce fragmentation, while bilateral acceptance may remain necessary. The operator should define how legacy peers are contained and how downgrade or weak negotiation is detected.

Commercial agreements may need amendment. Costs, responsibilities, incident notification, certificate management and migration dates should be explicit. Shared milestones can support coordinated investment, but each party should retain evidence of its own controls.

21. MANAGE CUSTOMER-PREMISES EQUIPMENT

Customer-premises equipment creates scale and access challenges. Devices may be owned by the operator, customer or third party. Some receive remote software updates; others require physical replacement. Enterprise configurations can be customised and tied to critical business processes.

The operator should segment the installed base by capability, service importance, contract, location and replacement path. It should identify customers requiring early engagement and maintenance windows. New sales should stop adding equipment that cannot meet the migration plan.

Financing can combine normal refresh, customer contribution and managed-service pricing. The commercial model should avoid charging customers for a vague security promise. It should specify the upgraded service, assurance, equipment, migration support and ongoing obligations.

22. ADDRESS CONSTRAINED IOT ESTATES

IoT devices can have limited processing, memory, bandwidth and update capability. They can also remain deployed for long periods in industrial, utility, transport and public environments. Post-quantum algorithms and larger credentials can exceed original design assumptions.

The operator should separate device, gateway and network responsibilities. A gateway or service-layer control may reduce immediate device change for some use cases, subject to the threat model. Devices without secure update or adequate trust may require replacement.

The investment case should include fleet inventory, field access, outage windows, logistics and disposal. A low unit price can conceal a high migration cost when millions of devices are dispersed. Early procurement rules can prevent the legacy population from growing.

23. INTEGRATE CLOUD AND VIRTUAL NETWORKS

Telecom networks increasingly use cloud-native functions, containers, orchestration and programmable infrastructure. Cryptography appears in service meshes, workload identities, APIs, images, secrets, software supply chains and management planes. Cloud providers and open-source projects therefore sit inside the migration perimeter.

The operator should obtain provider roadmaps, supported algorithms and shared-responsibility boundaries. It should test how changes affect scaling, latency, observability and incident response. Multi-cloud claims should be verified against the actual cryptographic and identity services used.

Platform investment can create leverage when common identity, certificate and policy services support many network functions. Governance should preserve workload-specific risk assessment. A common platform should expose exceptions rather than conceal them.

24. BUILD OPERATIONAL TELEMETRY

Operations teams need visibility into algorithms, certificates, negotiation, errors, downgrade attempts, performance and expiry. Telemetry should link technical events to services and customers. It should protect sensitive information and avoid creating a new attack surface.

The programme should define dashboards, alerts, retention, escalation and evidence. It should test failure scenarios before deployment. A migration that passes a laboratory test but cannot be monitored in production is incomplete.

Operational telemetry is an enduring investment. It supports assurance, incident response and future algorithm change. Its business case should include reduced discovery time, faster remediation and fewer manual processes, supported by measured baseline and target performance.

25. ESTABLISH ASSURANCE AND VALIDATION

Assurance should cover algorithm implementation, libraries, hardware modules, software signing, key management, configuration and operations. Standards compliance is part of the evidence. The operator should also test integration, misuse resistance and service behaviour.

Validation schedules can affect deployment. Products may support an algorithm before a validated implementation is available. The operator should define where validation is mandatory, where compensating evidence is acceptable and how later certification changes are handled.

Independent review can improve lender and board confidence for material work packages. The reviewer should examine scope, configuration, defects and residual risk. Assurance should remain proportionate and should not create an indefinite gate without decision criteria.

Table 4. Evidence and ownership across a migration cell

Evidence domain	Accountable owner	Minimum acceptance evidence	Capital decision
Asset and service scope	Service owner	Complete asset cohort, dependencies, data horizon and exceptions	Confirm eligible perimeter and cost baseline
Architecture and security	Chief technology and security functions	Approved pattern, threat assumptions, algorithms, trust and fallback	Authorise build and laboratory expenditure
Supplier and implementation	Procurement and programme leadership	Contracted roadmap, delivery plan, support, interoperability and remedies	Place conditional orders and reserve capacity
Operations and customers	Operations and product leadership	Telemetry, runbook, training, service acceptance and customer migration	Release deployment wave and commercial launch
Finance and assurance	Chief financial officer and independent reviewer	Spend reconciliation, cost to complete, milestone evidence and residual risk	Draw financing, release retention and approve next wave

Technical evidence and financial authority should meet at the same acceptance gate.

26. PRICE SERVICE CONTINUITY

Migration can affect availability, latency, capacity and support. The cost model should include parallel operation, maintenance windows, rollback, spare capacity and incident response. Customer compensation and regulatory consequences may apply when service levels fail.

Continuity design should identify the security state during failure. A fallback should be deliberate, observable and governed. Silent downgrade can preserve traffic while defeating the

purpose of migration. The operator should specify which services stop, degrade or continue under exception.

Financial analysis should test the cost of delay and the cost of interruption. A cheaper deployment path can be unattractive if it concentrates cutover risk. Staged cells create options to learn while protecting critical services.

27. DEVELOP QUANTUM-SAFE PRODUCTS CAREFULLY

Operators may offer managed quantum-safe connectivity, migration assessment, certificate services, secure edge or critical-route products. Product development should follow verified customer needs and the operator's delivery capability. A label alone does not create a defensible service.

The product definition should state the protected workflow, algorithms, endpoints, assurance, monitoring, service level and customer responsibilities. Pricing should cover equipment, migration, operations and future change. Contract language should avoid absolute security claims.

Anchor customers can co-design early products and provide acceptance evidence. Their commitments should be documented and contribution-tested. Grant-funded pilots can provide learning, but the commercial case should distinguish grant income from repeatable customer demand.

28. USE PUBLIC PROGRAMMES WITHOUT DISTORTING ECONOMICS

Public funding can support laboratories, standards, skills and critical-infrastructure migration. It can accelerate shared assets whose benefits extend beyond one operator. Funding conditions can also create reporting, procurement, intellectual-property and timing obligations.

The operator should record the full economic contribution. A grant may cover equipment while internal staff, integration and future support remain unfunded. A pilot may require continued operation after the funded period. These obligations belong in the cost model.

Investment decisions should survive the end of public support. The operator should identify which capability is mandatory, which has strategic option value and which depends on a further subsidy. Transparent classification prevents temporary funding from becoming an unsupported permanent cost.

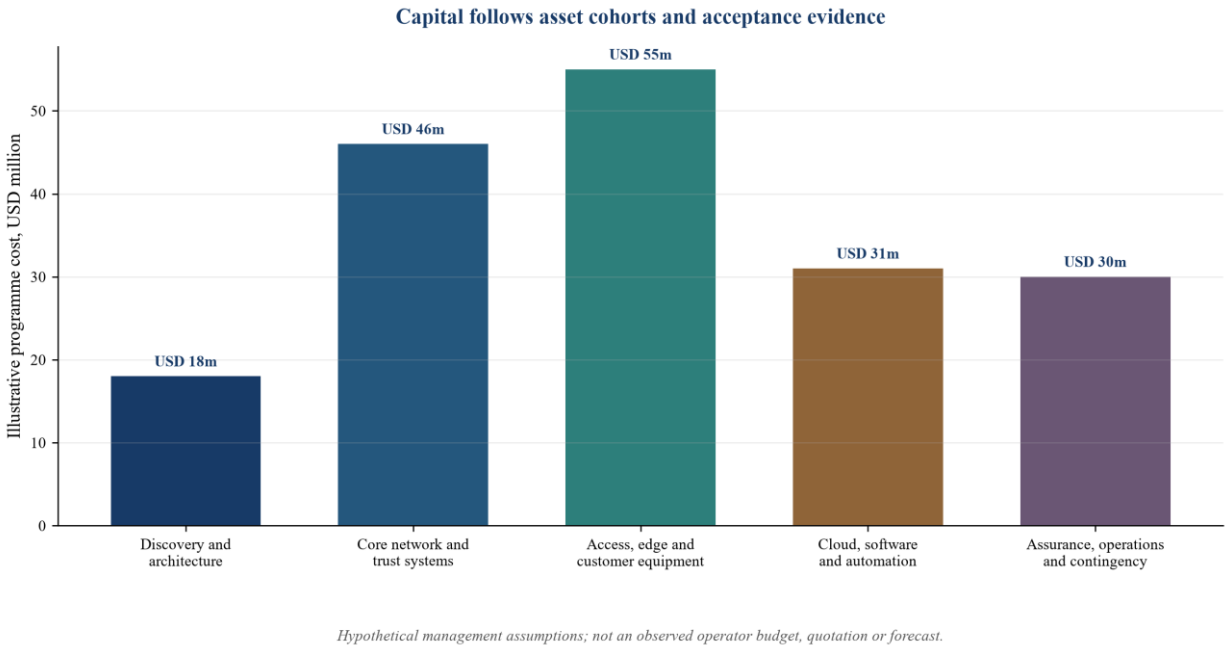


Figure 2. Illustrative allocation of a quantum-safe network programme

Amounts are hypothetical management assumptions used only to demonstrate the financing method.

29. APPLY A HYPOTHETICAL OPERATOR CASE

Consider a hypothetical regional operator with mobile, fibre, enterprise connectivity, cloud and managed-security services. It has a mixed estate from five principal network suppliers, a large customer-premises fleet and several long-lived trust systems. Management adopts the 2028, 2031 and 2035 milestones as programme anchors.

Illustrative management assumptions place total programme cost at USD 180 million. Discovery and architecture account for USD 18 million, core network and trust systems USD 46 million, access and customer equipment USD 55 million, cloud and software USD 31 million, and assurance, operations and contingency USD 30 million. The base case spans nine years.

Every amount, asset quantity, schedule, customer response and financing outcome in this case is hypothetical. The case demonstrates the framework. It is not observed operator data, a market forecast, an investment recommendation, a quotation or an offer.

30. SEQUENCE THE HYPOTHETICAL PROGRAMME

The first phase funds discovery, architecture, laboratories and procurement controls. It also begins trust-system design and stops the purchase of equipment without a supported migration path. The operator aims to complete estate coverage and an initial plan before 2028.

The second phase migrates the highest-priority management, signing, identity and enterprise services. It proves two multi-vendor network patterns and moves selected customer cohorts. Capital release follows interoperability, performance and operational acceptance. The operator targets completion of priority services before 2031.

The third phase scales accepted patterns across access, customer equipment and remaining platforms. It retires transitional mechanisms and closes exceptions. The programme retains a small tail for technically constrained assets, subject to explicit risk acceptance and replacement dates.

31. STRUCTURE THE HYPOTHETICAL FINANCING PLAN

The operator funds discovery, architecture, trust systems and programme governance from its corporate capital budget. It uses a term facility for approved modernisation waves after the first reference architecture is accepted. Vendor finance supports defined equipment cohorts with payment after installation and service acceptance.

A strategic co-investment vehicle funds a shared test environment and managed enterprise service. Governance reserves architecture, security and customer-data decisions to the operator. A small equipment lease supports separable laboratory and edge hardware where useful life and maintenance are clear.

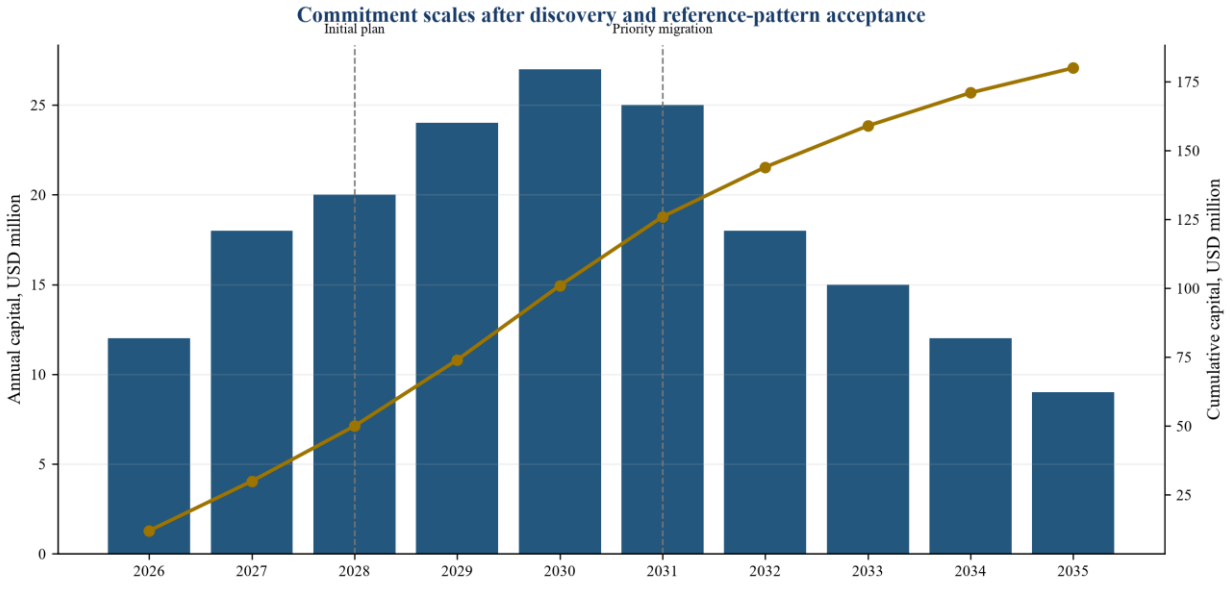
The financing mix follows control and evidence. The operator does not place core trust or incident responsibility outside its governance. Debt draws require cost-to-complete reporting, milestone status and minimum liquidity. Vendor commitments include roadmap and support remedies.

32. BUILD THE HYPOTHETICAL VALUE CASE

The programme protects service continuity and reduces exposure to accelerated replacement. It also creates reusable inventory, certificate automation, testing and operational telemetry. The operator models enterprise product revenue only after two anchor customers sign paid migration scopes and accept the service architecture.

Illustrative management assumptions assign USD 54 million of avoided accelerated replacement and incident-response cost on a probability-weighted basis, USD 38 million of lifecycle and automation benefit, and USD 64 million of enterprise-product contribution value. These figures are scenario outputs rather than observed benefits.

The board should test value against programme cost, financing cost and downside. The mandatory resilience case should remain supportable without speculative product revenue. Commercial upside can justify acceleration when customer commitments and contribution are verified.



Hypothetical management assumptions; not a forecast, financing commitment or observed budget.

Figure 3. Illustrative milestone-linked capital profile

The profile demonstrates staged commitment rather than an observed operator plan.

33. STRESS-TEST DELAY AND SUPPLIER FAILURE

The downside case should test a two-year vendor delay, failure of a critical interoperability pattern and accelerated retirement of unsupported equipment. These events affect cost, liquidity and milestone compliance. They may also concentrate deployments into a shorter period with scarce engineering capacity.

The response can include second-source qualification, bridge controls, extended support and reprioritisation. Each response has cost and residual risk. The operator should establish decision triggers before the delay occurs.

Financing documents should avoid incentives that force deployment before acceptance. Draw availability can be extended subject to evidence and revised cost-to-complete. Vendor remedies and reserved capacity can offset part of the risk. Core continuity funding should remain available under downside conditions.

34. STRESS-TEST PERFORMANCE AND INTEROPERABILITY

Post-quantum mechanisms can change processing, message size and handshake behaviour. The operator should test peak load, constrained devices, lossy links, failover and mixed versions. An average laboratory benchmark is insufficient for a service-level decision.

The financial model should connect performance failure to remediation. Extra hardware, software optimisation, architecture changes or customer-device replacement can increase cost. A failed pattern can also delay revenue or acceptance.

Reference patterns should therefore have explicit performance envelopes. Deployment remains conditional until representative tests pass. Exceptions should be quantified and assigned a retirement plan rather than carried indefinitely.

35. STRESS-TEST CUSTOMER MIGRATION

Customers can delay upgrades because of maintenance windows, application dependencies, internal approvals or equipment ownership. The operator should model adoption by cohort and identify the cost of parallel service. Enterprise customers may require bespoke testing and contractual change.

The commercial plan should prioritise customers with long confidentiality horizons, regulated operations or expiring equipment. Early anchor customers can improve the product and deployment method. Their requirements should not turn a common platform into a collection of unsupported variants.

The operator should track signed scope, scheduled migration, technical acceptance, collected revenue and contribution. Pipeline interest should not finance committed cost. Capital for commercial expansion should follow observable adoption.

36. ESTABLISH GOVERNANCE AND REPORTING

The programme needs one executive sponsor and a joint technology, security, operations, finance, procurement and commercial forum. The board should receive scope coverage, milestone status, cost, liquidity, supplier risk, exceptions, service incidents and benefits evidence.

Reporting should reconcile technical and financial structures. A work package should have the same identifier across architecture, procurement, project management and finance. This permits cost-to-complete analysis and prevents accepted defects from disappearing between teams.

Independent assurance should focus on material gates and reported evidence. Governance should be capable of pausing a deployment, reallocating capital or changing a supplier. It should also close completed work and retire transitional complexity.

Table 3. Quantum-safe programme decision gates

Gate	Evidence	Board or management decision	Financial consequence
Discovery complete	Inventory coverage, service map, data horizons and exceptions	Approve migration perimeter and priority	Release architecture and early-design capital
Reference architecture approved	Interfaces, patterns, threat assumptions and supplier baseline	Authorise laboratory and procurement framework	Commit test facilities and conditional vendor capacity
Pattern accepted	Interoperability, performance, rollback, telemetry and assurance	Authorise bounded deployment wave	Draw wave capital and place call-off orders
Service accepted	Customer or operations acceptance, stable run and defect closure	Scale, amend or stop the pattern	Release retention, recognise benefits and resize forecast
Wave closed	Asset records, costs, lessons, residual exceptions and retirement	Approve next wave and updated completion plan	Reallocate contingency and confirm cost to complete

A gate should release capital only after the relevant uncertainty has been reduced.

37. LIMITATIONS

The framework does not predict when a cryptographically relevant quantum computer will exist. It uses published standards and migration milestones to organise an investment response. Operators should update their plans as standards, protocols, validation programmes, regulation and supplier products develop.

The hypothetical case excludes jurisdiction-specific tax, accounting, spectrum, procurement, data-protection and national-security requirements. All numerical inputs are illustrative management assumptions and should not be used as market benchmarks. Financing availability and terms depend on the operator, assets, lenders and market conditions.

Implementation requires specialist cryptography, telecom, cybersecurity, operations, finance, accounting, legal and regulatory advice. Each operator should apply its own threat model, service obligations, asset estate and risk appetite.

38. CONCLUSION

Quantum-safe migration is a telecom infrastructure programme with a security deadline. The operator must discover embedded cryptography, align assets and suppliers, prove interoperable

patterns, migrate customers and operate the resulting estate. The size of the task makes undifferentiated funding difficult and staged investment essential.

The Quantum-Safe Network Financing Framework converts the programme into bounded migration cells, observable gates and appropriate financing instruments. It gives early priority to long-lived trust and network assets, aligns replacement with lifecycle where possible, and uses anchor demand to improve supplier readiness. It keeps core security accountability with the operator while allowing vendors, lenders and strategic partners to fund defined components.

The practical investment question is clear: which service and asset cohort can be moved to an accepted quantum-safe state, by what date, at what complete cost and with which accountable counterparties? An operator that can answer that question can finance progress before migration deadlines compress choice and increase cost.

REFERENCES

[1] National Institute of Standards and Technology, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024, https://doi.org/10.6028/NIST.FIPS.203

[2] National Institute of Standards and Technology, FIPS 204, Module-Lattice-Based Digital Signature Standard, 2024, https://doi.org/10.6028/NIST.FIPS.204

[3] National Institute of Standards and Technology, FIPS 205, Stateless Hash-Based Digital Signature Standard, 2024, https://doi.org/10.6028/NIST.FIPS.205

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

[5] National Institute of Standards and Technology, Migration to Post-Quantum Cryptography, National Cybersecurity Center of Excellence, accessed September 2026, https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/

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

[7] UK National Cyber Security Centre, Timelines for Migration to Post-Quantum Cryptography, 2025, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[8] UK National Cyber Security Centre, Preparing for Post-Quantum Cryptography, 2024, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

[9] European Telecommunications Standards Institute, ETSI TR 103 619 V1.1.1, Migration Strategies and Recommendations to Quantum Safe Schemes, 2020, https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[10] European Telecommunications Standards Institute, ETSI TR 104 016 V1.1.1, A Repeatable Framework for Quantum-Safe Migrations, 2024, https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf

[11] European Telecommunications Standards Institute, TC CYBER Quantum-Safe Cryptography Roadmap, accessed September 2026, https://www.etsi.org/cyber-security/tc-cyber-roadmap

[12] European Union NIS Cooperation Group, A 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] National Security Agency, Commercial National Security Algorithm Suite 2.0 Cybersecurity Advisory, 2022 with later updates, https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[14] National Security Agency, Post-Quantum Cybersecurity Resources, accessed September 2026, https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

[15] Cybersecurity and Infrastructure Security Agency, Preparing Critical Infrastructure for Post-Quantum Cryptography, accessed September 2026, https://www.cisa.gov/quantum

[16] Global System for Mobile Communications Association, PQ.03 Post Quantum Cryptography Guidelines for Telecom Use Cases, version 2.0, referenced by NIST NCCoE, https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum-cryptography/

[17] Internet Engineering Task Force, Post-Quantum Cryptography Use in Protocols Working Group, accessed September 2026, https://datatracker.ietf.org/wg/pquip/about/

[18] Internet Engineering Task Force, Hybrid Key Exchange in TLS 1.3, current work accessed September 2026, https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[19] International Telecommunication Union, Security and Trust Programme, accessed September 2026, https://www.itu.int/itu-t/recommendations/index.aspx?ser=X

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

[21] European Central Bank, Quantum Readiness and Cryptographic Migration Materials, accessed September 2026, https://www.ecb.europa.eu/

[22] Cloud Security Alliance, Quantum-Safe Security Working Group Resources, accessed September 2026, https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security

[23] Open Quantum Safe, Open-Source Software for Prototyping Quantum-Resistant Cryptography, accessed September 2026, https://openquantumsafe.org/

[24] Linux Foundation, Post-Quantum Cryptography Alliance, accessed September 2026, https://pqca.org/

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

[26] International Organization for Standardization, ISO 31000:2018 Risk Management Guidelines, https://www.iso.org/iso-31000-risk-management.html

[27] IFRS Foundation, IAS 16 Property, Plant and Equipment, https://www.ifrs.org/issued-standards/list-of-standards/ias-16-property-plant-and-equipment/

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

[29] IFRS Foundation, IFRS 9 Financial Instruments, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-9-financial-instruments/

[30] Basel Committee on Banking Supervision, Principles for the Sound Management of Operational Risk, 2021, https://www.bis.org/bcbs/publ/d515.htm

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.