MatchPoint Research Working Paper No. 2026/T10

# Quantum-Resistant Security for Financial Data: Preparing for Q-Day

*A governed cryptographic inventory, migration architecture and operating model for family offices and family businesses*

**Chennakeshav (CK) Adya**
Independent Researcher
August 2026

## ABSTRACT

**Background.** A future cryptographically relevant quantum computer would threaten public-key mechanisms used to protect financial data, while long-lived information can be collected before that capability exists. **Objective.** This paper develops a proportionate quantum-readiness operating model for family offices, SMEs and family businesses. **Approach.** The analysis reviews 27 primary standards, official roadmaps, financial-system experiments, regulatory publications and foundational research available through 1 August 2026; status, jurisdiction and experiment boundaries are retained. **Findings.** The proposed design connects data-life decisions to a living cryptographic dependency graph, separates algorithm, protocol, product, validation and organisation-acceptance states, and releases change through accepted quantum-readiness migration packets with interoperability, performance, recovery, rollback and residual-risk evidence. **Implications.** Organisations can begin with classification, inventory and supplier assurance, then test bounded hybrid or post-quantum migrations as standards and products mature. Productivity is measured per accepted packet; attributed revenue, cost reduction and loss reduction remain zero until approved observed evidence supports attribution.

### Highlights

**Threshold.** Q-Day is unknown; decisions use data life and migration lead time rather than a date forecast.

**Inventory.** A living dependency graph connects services, financial data, protocols, libraries, keys, certificates, devices and suppliers.

**Evidence.** Standards, protocol status, product support, validation and organisation acceptance remain separate states.

**Release.** Interoperability, performance, recovery, rollback and named residual-risk authority are required.

**Productivity.** Measurement uses accepted quantum-readiness migration packets after human review.

**JEL Classification:** G21, G23, G28, G32, L86, M15, O31, O32, O33

**Keywords:** post-quantum cryptography, quantum-resistant security, financial data, crypto agility, ML-KEM, ML-DSA, cryptographic inventory, family office, family business, migration governance

*Research paper only. This document is not investment, cybersecurity, cryptographic-engineering, legal, regulatory, tax, accounting or technology-procurement advice. Q-Day is not forecast. All productivity scenario inputs are unverified illustrative management assumptions.*

## 1. INTRODUCTION

Financial information remains valuable long after it is created. Family-office records can expose beneficial ownership, investment terms, succession plans, tax positions, counterparties and private correspondence. An operating company's records can reveal customer identities, payroll, pricing, supplier terms, bank instructions, forecasts, acquisition plans and intellectual property. Encryption protects much of this information in transit and at rest, but many current public-key systems depend on mathematical problems that a sufficiently capable quantum computer could solve.

The relevant threshold is a cryptographically relevant quantum computer, or CRQC: a general-purpose quantum computer capable of attacking cryptographic systems at the scale needed to compromise real deployments. The date on which such a machine may exist is unknown. This paper uses **Q-Day** only as shorthand for that uncertain threshold. It does not forecast a calendar date.

Shor showed in 1994 that a quantum computer could solve integer-factorisation and discrete-logarithm problems in polynomial time [23]. These problems support RSA, finite-field Diffie-Hellman and elliptic-curve cryptography. Grover showed a quadratic speed-up for unstructured search [24]. The two results have different security implications. A CRQC threatens widely deployed public-key cryptography directly. Symmetric cryptography and hash functions are affected differently and are not correctly described as simply "broken" by the same result. Algorithm choice, key size, construction and implementation still matter.

The confidentiality risk starts before a CRQC exists. An adversary may collect encrypted traffic or stored ciphertext now and attempt to decrypt it later. NIST, the UK National Cyber Security Centre, the Bank for International Settlements and the G7 Cyber Expert Group all treat long-lived data and lengthy migration programmes as reasons to begin preparation [8,9,15,18]. The risk is greatest where the required confidentiality life exceeds the time available to discover, replace and validate vulnerable cryptographic dependencies.

The standards base has moved from research selection to implementation. NIST published FIPS 203 for ML-KEM, FIPS 204 for ML-DSA and FIPS 205 for SLH-DSA on 13 August 2024 [1-3]. NIST published final KEM guidance in September 2025 [4], updated its final crypto-agility paper in June 2026 [5] and published the IR 8547 transition proposal as an initial public draft [6]. IETF work defines shared terminology for post-quantum and traditional hybrid schemes, while protocol-specific work continues [12-14]. The resulting programme is broader than substituting one algorithm for another. Certificates, protocols, libraries, hardware security modules, secure boot, identities, vendors, backups and historical records form a connected cryptographic estate.

Financial authorities have also moved towards structured transition. BIS Paper No. 158 sets out a quantum-readiness roadmap for the financial system and emphasises awareness, cryptographic inventory, crypto agility, defence in depth, hybrid models and phased migration [15]. BIS Project Leap tested post-quantum mechanisms between central-bank systems and later in an operational payment-system setting, demonstrating feasibility while identifying performance, integration and coordination issues [16]. The Bank of England's July 2026 Financial Stability Report asks firms to begin planning, map cryptographic dependencies and seek assurance from material third parties [17]. The G7 Cyber Expert Group published a non-prescriptive financial-sector roadmap in January 2026 [18].

This paper translates that evidence into a practical operating model for primary ICP A2, family offices, and secondary ICP B4, SMEs and family businesses. Its central production unit is the **accepted quantum-readiness migration packet**: a versioned record that defines one cryptographic dependency or service, its data and business context, present algorithms, supplier and technical dependencies, target design, test evidence, approvals, deployment state, rollback evidence and residual risk.

The proposed system has seven objectives:

1. identify long-lived financial data and the services that create, transmit, store, sign or recover it;
2. establish a cryptographic inventory connected to business services, data flows and suppliers;
3. prioritise work using confidentiality life, integrity life, operational criticality and migration lead time;
4. separate standards status, product support, algorithm validation, module validation and organisation acceptance;
5. introduce crypto agility and post-quantum mechanisms through tested, reversible changes;
6. preserve named authority, evidence, rollback and incident response at every release; and

7. measure productivity per accepted migration packet while treating revenue and risk reduction as unproven until observed evidence supports them.

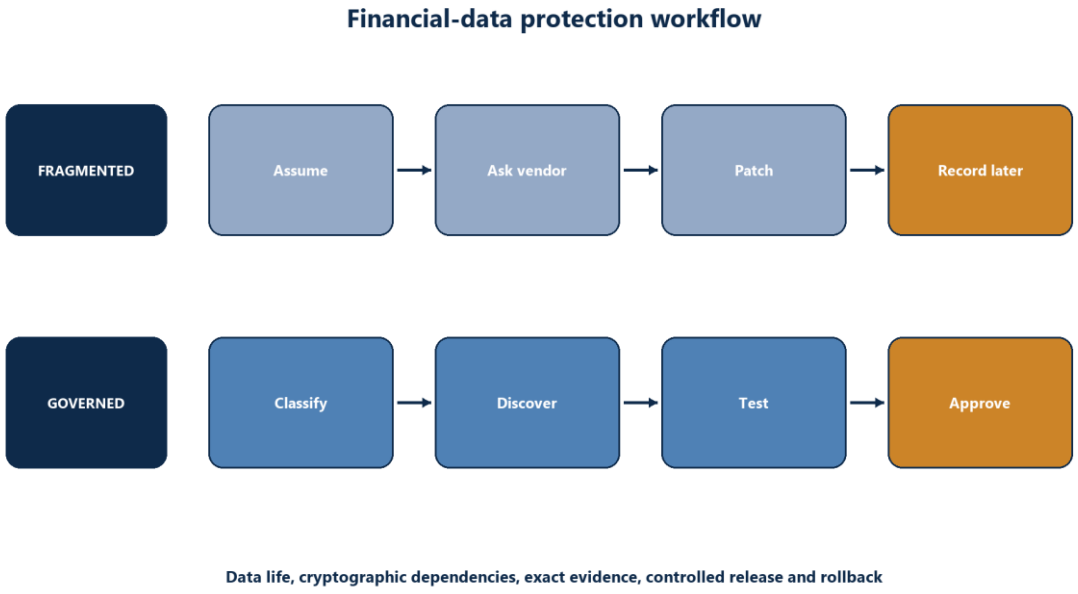


**Figure 1. Financial-data protection workflow before and after governed post-quantum preparation**
*Source: Matchpoint framework.*

The operating model is vendor-independent. It can accommodate on-premises systems, public cloud, managed software, banks, administrators, trustees, legal advisers, payment providers and data-room vendors. Each dependency retains its owner, protocol, implementation, data class, support status and evidence. The resulting programme improves visibility into current cryptography while preparing for post-quantum change.

## 2. DEFINITIONS, SCOPE AND EVIDENCE METHOD

### 2.1 Definitions

**Post-quantum cryptography**, or PQC, means cryptographic algorithms designed to be secure against attacks using quantum computers as well as classical computers. RFC 9794 notes that "post-quantum", "quantum-resistant" and "quantum-safe" are used in practice, and cautions that a design label does not establish that an algorithm can never be compromised [12]. This paper therefore uses **post-quantum** for standards and implementations and **quantum-resistant** for the programme title.

**Traditional public-key cryptography** means asymmetric algorithms based on integer factorisation, finite-field discrete logarithms, elliptic-curve discrete logarithms or related problems, following RFC 9794 [12]. Examples include RSA, Diffie-Hellman, ECDH, DSA and ECDSA. These algorithms are not interchangeable; an inventory records exact algorithm, parameters, purpose, library and protocol.

**Key-encapsulation mechanism**, or KEM, means a set of algorithms used by two parties under stated conditions to establish a shared secret key over a public channel [4]. ML-KEM is the NIST-standardised module-lattice KEM in FIPS 203 [1]. The shared secret is subsequently used with symmetric cryptography within a protocol or construction.

**Digital signature** means a cryptographic mechanism used to detect unauthorised modification and authenticate the signatory. ML-DSA in FIPS 204 and SLH-DSA in FIPS 205 are NIST post-quantum signature standards [2,3]. Their key sizes, signature sizes, implementation properties and operational use differ.

**PQ/T hybrid scheme** follows RFC 9794: a multi-algorithm scheme with at least one post-quantum component and at least one traditional asymmetric component [12]. The construction and combiner matter. Putting two algorithms beside each other without an analysed protocol does not establish the intended security property.

**Crypto agility** means the capabilities needed to replace and adapt cryptographic algorithms in protocols, applications, software, hardware, firmware and infrastructure while preserving security and operations [5]. It includes governance, abstraction, configuration, inventory, testing, observability and change processes.

**Cryptographic dependency** means a specific use of cryptography by a business service, data flow, identity, device, application, protocol, library, certificate, key store, backup, supplier or control. A product name alone is insufficient. The dependency record identifies purpose, algorithm, parameters, implementation, version, endpoints, owner and evidence.

**Accepted quantum-readiness migration packet** means the governed unit approved for its stated stage. It contains scope, data class, current dependency, source evidence, standards and supplier state, target design, tests, exceptions, deployment, rollback, review and residual risk. An inventory-only packet and a production-release packet have different acceptance criteria.

## 2.2 Scope and ICPs

Primary ICP A2 includes single-family offices, multi-family offices, private investment companies, holding structures and their investment or operating teams. Secondary ICP B4 includes SMEs and family businesses with material financial data and a dependence on commercial technology providers. The framework also supports advisers, administrators, banks, insurers and trustees when roles and confidentiality boundaries are defined.

The paper covers public-key cryptography used for transport security, file and message protection, virtual private networks, identity, code signing, document signing, APIs, secure boot, key wrapping and selected payment or treasury interfaces. It discusses symmetric cryptography and hashes only to distinguish their transition treatment. It does not design a new algorithm, certify a product, provide penetration testing or replace legal, regulatory or cryptographic-engineering advice.

The framework is proportionate. A family office with outsourced IT may have a small internal team and a large supplier estate. Its main work may be data classification, contract and supplier assurance, identity and device inventory, and validation of managed-service roadmaps. An SME with proprietary software may need code-level discovery, protocol testing and release engineering. A larger financial institution may require sector-wide coordination beyond the scope of this paper.

UAE sources are used for the present control environment, not as a claim that they prescribe a specific PQC migration. The UAE Information Assurance Regulation requires a documented policy for cryptographic controls, automated key-management processes and risk-based protection of sensitive information [22]. Joint CBUAE, SCA, DFSA and FSRA enabling-technology guidance addresses cryptographic key management in covered financial-technology contexts [21]. Neither source cited here establishes a UAE-specific Q-Day or a universal PQC deadline.

## 2.3 Evidence method

The analysis uses primary standards, official government and regulator publications, official financial-system experiments, standards-development documents and foundational research available through 1 August 2026. Status is recorded as final standard, final guidance, draft, roadmap, experiment, regulation or research result.

| Evidence class | Use in this paper | Boundary retained |
|---|---|---|
| Final cryptographic standard | Algorithm specification and approved parameters | Does not establish secure product integration or organisation acceptance |
| Final implementation guidance | KEM use, crypto agility, validation and transition practice | Retains jurisdiction, programme and use-case scope |
| Draft standard or Internet-Draft | Protocol direction and interoperability work | Draft may change, expire or be replaced |
| Official roadmap | Timing, governance and transition activities | Target dates are policy guidance, not a CRQC forecast |
| Official financial experiment | Feasibility, performance and integration observations | Test design and environment do not establish universal production performance |

| Evidence class | Use in this paper | Boundary retained |
|---|---|---|
| Regulation or supervisory publication | Applicable control and resilience context | Legal entity, jurisdiction and effective-date boundaries apply |
| Foundational research | Quantum algorithm and temporal-risk logic | Does not predict engineering availability or a date for Q-Day |
| Matchpoint framework | Inventory, controls, packet and scorecard design | Requires organisation-specific legal and technical validation |
| Matchpoint scenario | Productivity calculation structure | Unverified illustrative management assumptions |

Vendor claims, survey headlines and quantum-hardware roadmaps are excluded from the evidence base for Q-Day. The paper makes no claim that a particular product is post-quantum secure, that a CRQC currently exists, or that a migration produces a stated reduction in loss probability.

### 2.4 Standards status is part of the data model

The estate must distinguish several states that are often collapsed in procurement language.

| State | What it establishes | What it does not establish |
|---|---|---|
| NIST final algorithm standard | Normative algorithm and parameter specification | Correct library, protocol or product implementation |
| CAVP algorithm validation | Tested implementation of an approved algorithm component | FIPS 140 module validation or secure application use |
| CMVP module validation | Module assessed against FIPS 140 requirements within stated boundary and mode | Suitability for every architecture or business service |
| Protocol standard or final profile | Interoperable construction for a defined protocol | Availability in every client, server, gateway or certificate ecosystem |
| Vendor support statement | Product roadmap or claimed feature | Independent validation, deployed configuration or end-to-end interoperability |
| Organisation acceptance | Approved evidence for a defined business service | Acceptance for other services, data classes or threat models |

NIST states that a product does not meet FIPS 140 requirements merely because it implements an approved algorithm or holds an algorithm validation certificate [26]. This distinction belongs in procurement, testing and evidence records.

## 3. THE FINANCIAL-DATA RISK MODEL

### 3.1 Which cryptography is exposed

Shor's algorithm changes the security assumption for integer factorisation and discrete logarithms [23]. In a future CRQC scenario, RSA encryption and signatures, finite-field Diffie-Hellman, elliptic-curve key agreement and elliptic-curve signatures become exposed. The affected functions include TLS handshakes, VPN key establishment, public-key infrastructure, code signing, document signatures, secure software update, device identity, key wrapping and some blockchain or digital-asset mechanisms.

Grover's algorithm gives a quadratic rather than exponential speed-up for an unstructured search problem [24]. This informs symmetric-key and hash-security margins, but the engineering implications depend on construction, parameters and achievable quantum resources. A programme should therefore avoid blanket replacements. It should map each primitive to purpose and approved transition guidance.

| Cryptographic function | Common financial-data use | Quantum concern | Programme response |
|---|---|---|---|
| RSA or elliptic-curve key establishment | TLS, VPN, secure email, API sessions | Shor exposure for recorded exchanges or future sessions | Prioritise long-lived confidentiality and protocol roadmap |
| RSA, DSA or ECDSA signatures | documents, code, certificates, transactions | Future forgery or authenticity challenge if keys and formats remain exposed | Map verification life, update paths and trust anchors |
| AES and other symmetric encryption | databases, disks, files and session traffic | Different security-margin impact from Grover-style search | Review key size, mode, lifecycle and approved guidance |
| SHA-2/SHA-3 and related hashes | integrity, signatures, certificates and identifiers | Construction-specific quantum security margin | Preserve exact function and context; follow standards guidance |
| Password hashing | identity and secrets | Quantum risk is one part of parameter and implementation risk | Maintain memory-hard, rate-limited, salted practice and migration capability |
| Proprietary or unknown crypto | legacy applications and devices | Unverifiable properties and weak upgrade route | Treat as an exception requiring discovery and replacement analysis |

## 3.2 The confidentiality clock

Mosca's temporal model compares three durations: the time information must remain secure, the time required to migrate the system, and the time until a relevant quantum threat may arrive [25]. If the required confidentiality life plus migration time exceeds the remaining threat horizon, preparation has already started too late under the scenario. The last term is uncertain. The first two can be estimated and measured.

For a family office, selected ownership, succession, trust, tax, legal and investment records may require confidentiality for decades. For an SME, trade secrets, source code, regulated personal data, pricing and strategic transactions can also retain value over long periods. The organisation should assign a confidentiality horizon by data class and record the owner and legal basis for that estimate.

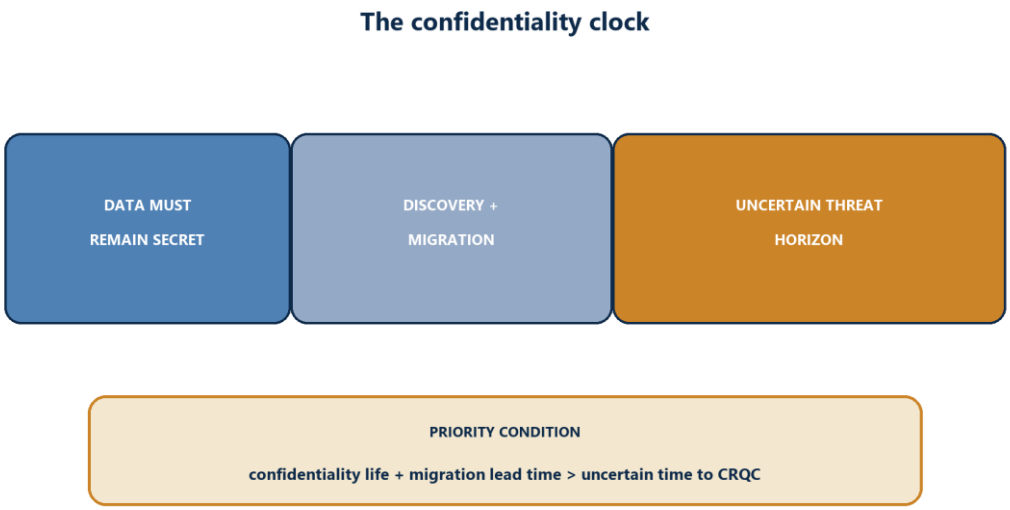


**Figure 2. Confidentiality life, migration lead time and uncertain Q-Day horizon**

*Source: Matchpoint synthesis based on Mosca [25] and official migration guidance [8,9,15,18].*

The model creates four practical priority bands.

| Priority band | Data and service condition | Initial action |
|---|---|---|
| Immediate discovery | Long confidentiality life, externally observable traffic, unknown public-key crypto or no supplier roadmap | Identify flows, capture evidence, restrict unnecessary exposure and obtain roadmap |
| Early migration candidate | Critical service with mature supported PQ/T or PQ option and a safe rollback path | Lab test, interoperability test, shadow or canary deployment |
| Planned dependency | Material service whose protocol, trust ecosystem or product support is still developing | Contract, architecture and upgrade preparation; monitor standards and vendor evidence |
| Routine managed upgrade | Low-complexity managed service with short-lived data and credible supplier plan | Record dependency, verify release and acceptance evidence when available |

The band is a governance decision. It is not an automated prediction of attack probability.

### 3.3 Integrity and authenticity clocks

Harvest-now, decrypt-later applies most directly to confidentiality. Signatures create a related but distinct timing problem. A signed financial statement, contract, software image or transaction record may need verification years after signing. The organisation must decide whether future verification depends on a now-vulnerable public key, whether trusted timestamps or archival evidence are used, and how re-signing or evidence renewal will be governed.

Long-lived devices introduce another clock. A hardware root of trust, secure-boot key or firmware-verification path may remain in service for years and may be hard to replace. NCSC guidance identifies long-lived hardware roots and supplier dependencies as migration-planning concerns [9]. The inventory therefore records both data life and device or signature verification life.

### 3.4 Concentration and ecosystem risk

Financial services depend on shared cloud, identity, certificate, telecommunications, banking, payment and software providers. A small internal estate can conceal a large cryptographic dependency graph. The Bank of England notes that firms' preparation depends on material third parties and asks firms to seek assurance on provider plans [17]. BIS and the G7 emphasise coordination because weak links can affect connected services [15,18].

Concentration is assessed at several layers: one identity provider; one certificate authority; one HSM or key-management service; one managed-service provider; one cryptographic library embedded in many applications; one gateway terminating many connections; and one administrator controlling multiple holding entities. The result should inform sequencing and contingency plans, not create an unsupported numerical loss estimate.

## 4. CRYPTOGRAPHIC INVENTORY AND DEPENDENCY GRAPH

### 4.1 Start from business services and data

The programme begins with business services rather than a list of algorithms. A business service creates the decision context for confidentiality, integrity, availability, legal evidence and recovery. Examples include treasury payments, portfolio reporting, investor communications, payroll, customer invoicing, board papers, data rooms, backups, remote access, source-code release and trust administration.

Each service is connected to data classes and flows. A treasury instruction may originate in an ERP system, pass through an API gateway or browser, use an identity provider, enter a bank portal, create signed approval evidence, be archived in email and appear in backups. Each link can use a different cryptographic implementation.

| Inventory object | Minimum fields | Acceptance evidence |
|---|---|---|
| Business service | owner, purpose, criticality, recovery objective, jurisdictions | approved service record |

| Inventory object | Minimum fields | Acceptance evidence |
|---|---|---|
| Data class | owner, sensitivity, confidentiality life, integrity life, retention | classification and legal basis |
| Data flow | source, destination, protocol, network path, frequency, external visibility | observed configuration and diagram |
| Cryptographic use | function, algorithm, parameters, library, version, mode | scan, configuration, code or vendor evidence |
| Key or certificate | purpose, owner, store, issuer, algorithm, expiry, rotation, recovery | key-management or PKI record |
| Device or workload | platform, firmware, secure boot, update path, support life | asset and supplier evidence |
| Supplier | service, dependency, contract, roadmap, validation and exit route | current attestation and contract record |
| Migration decision | target, construction, test plan, rollback, approvers, residual risk | accepted migration packet |

### 4.2 Discovery methods and evidence hierarchy

No single scanner finds the full estate. Discovery combines configuration-management databases, cloud inventories, certificate stores, network observations, code and dependency scanning, HSM/KMS records, database configuration, device management, software bills of materials, procurement records, supplier questionnaires and interviews.

Evidence strength should be explicit:

1. observed runtime configuration or validated scan with timestamp;
2. signed or system-generated configuration record;
3. current supplier documentation for the exact product and version;
4. contract or attestation linked to a defined service;
5. owner statement awaiting technical verification; and
6. unknown.

An unknown field is a valid inventory state. A guessed algorithm or supplier capability creates false assurance. Automated discovery outputs remain candidates until the system boundary and interpretation are reviewed.

### 4.3 Dependency graph

The graph represents business and technical relationships:

business service -> data class -> data flow -> protocol -> library -> algorithm;

business service -> identity provider -> certificate authority -> trust anchor;

application -> operating system -> HSM or KMS -> backup and recovery;

device -> secure boot -> firmware signature -> update supplier;

supplier -> subcontractor -> cloud region -> exit or contingency route;

migration packet -> tests -> approval -> release -> monitoring -> retirement.

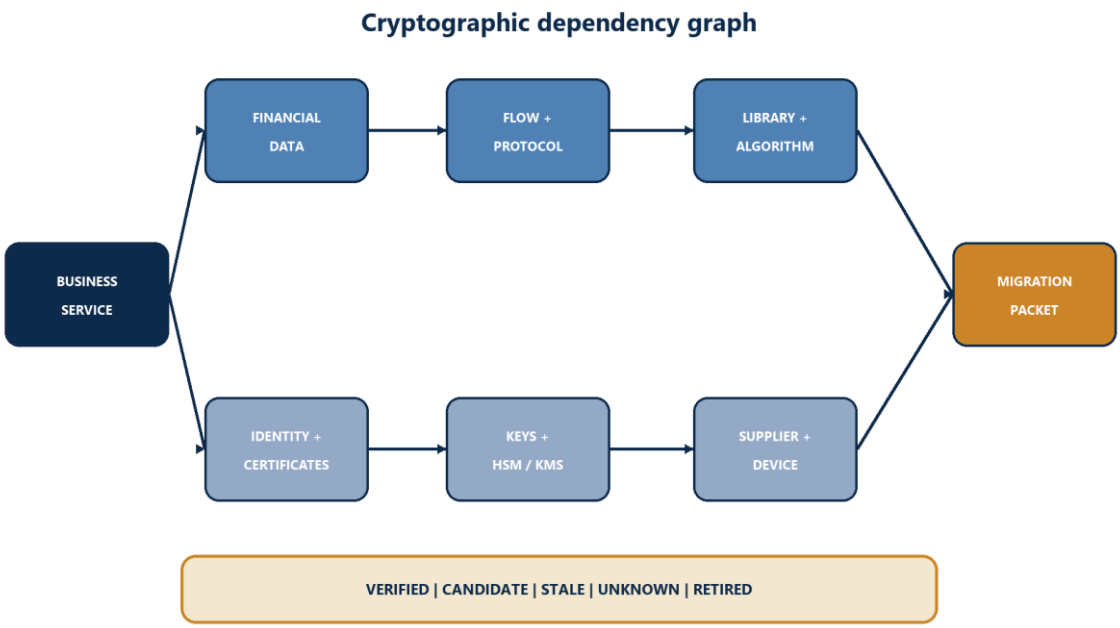


**Figure 3. Cryptographic dependency graph for financial data and business services**

*Source: Matchpoint framework; inventory and coordination references [5,8,9,15,17-20].*

This graph supports change impact. A vulnerable or unsupported library can be traced to every dependent service. A certificate authority's PQC roadmap can be connected to affected websites, APIs, signing workflows and archival verification. It also makes duplicated work visible when several holding entities use the same provider.

### 4.4 Inventory quality controls

Inventory completeness is measured against defined populations rather than an unknowable total. Reconciliation populations can include all externally accessible endpoints, managed devices, production applications, active certificates, key stores, critical suppliers and Tier 1 business services. Each population has an owner and extraction date.

| Control | Test | Failure state |
|---|---|---|
| Population reconciliation | inventory records tie to source-system population and exclusions | missing or unexplained objects |
| Evidence currency | evidence timestamp falls within approved interval | stale |
| Identity resolution | endpoint, certificate, service and owner are linked | orphaned |
| Algorithm precision | algorithm, parameters, purpose and implementation recorded | ambiguous |
| Supplier precision | exact product/version and contractual service identified | generic claim |
| Data-life approval | confidentiality and integrity horizons have named owner | unapproved estimate |
| Change detection | additions, removals and material configuration changes create review | silent drift |

The inventory is a living control. A one-time spreadsheet becomes obsolete as certificates rotate, applications deploy and vendors change libraries.

# 5. GOVERNED POST-QUANTUM ARCHITECTURE

## 5.1 Architectural layers

The target design separates cryptographic policy, implementations and business logic.

| Layer | Core components | Control objective |
|---|---|---|
| Business and data | services, records, retention, criticality and authority | connect cryptography to an approved purpose |
| Policy and orchestration | allowed algorithms, profiles, negotiation, feature flags and stops | centralise controlled choice and transition |
| Identity and trust | PKI, certificates, trust anchors, signing and timestamping | preserve authenticated relationships and evidence life |
| Cryptographic services | KMS, HSM, secret management, libraries and APIs | expose governed implementations through stable interfaces |
| Protocol and application | TLS, VPN, email, files, APIs, databases, updates and signatures | apply reviewed constructions in context |
| Evidence and observability | inventory, telemetry, tests, validation, releases and incidents | make deployed state and failure visible |
| Supplier and assurance | contracts, roadmaps, SBOMs, validation and exit plans | govern external dependencies |

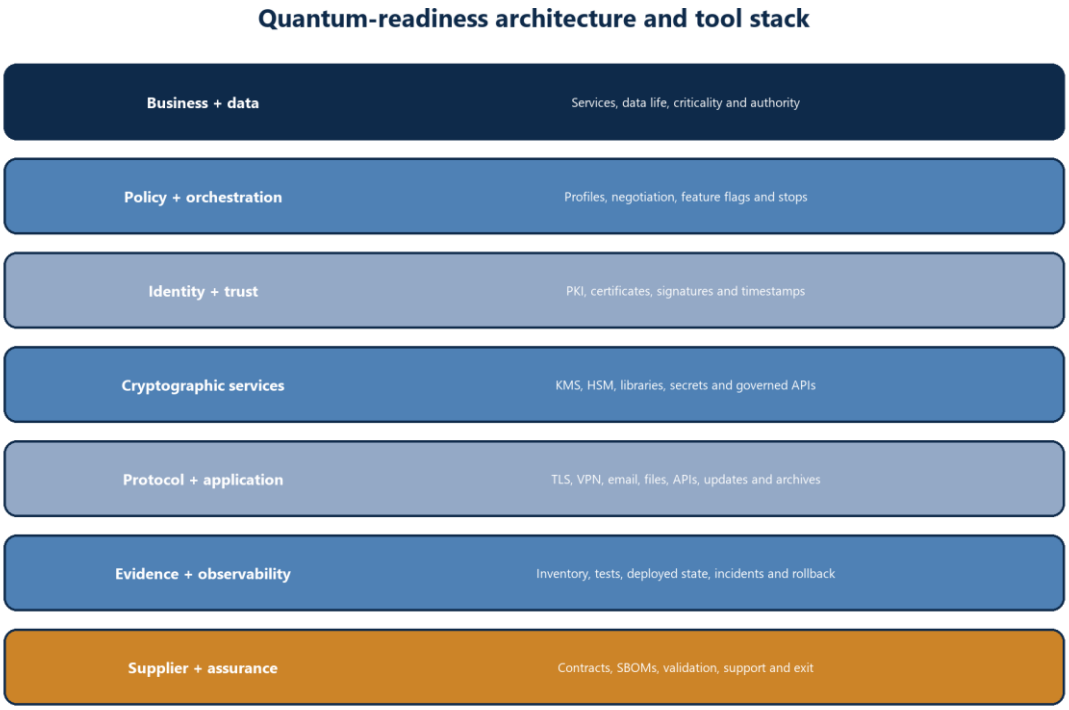


**Figure 4. Quantum-readiness architecture and tool stack for financial data**

*Source: Matchpoint architecture; standards and guidance [1-5,12-16,26,27].*

Crypto agility appears at each layer. Application code calls a governed interface rather than embedding an algorithm assumption. Policy can allow a tested PQ/T group for a defined endpoint and disable it through a controlled

rollback. Certificates and keys are discoverable and renewable. Telemetry records negotiated algorithms without exposing secret material. Suppliers provide version-specific evidence.

### 5.2 Standards-aligned algorithm roles

FIPS 203 defines ML-KEM for key establishment [1]. FIPS 204 and FIPS 205 define two signature approaches [2,3]. NIST selected HQC in March 2025 as a future backup KEM based on a different mathematical family; the standard was still under development in the cited official status [7]. A selected algorithm is not treated as a final standard before publication.

Algorithm selection requires use-case analysis. Key and ciphertext sizes, signature sizes, verification performance, side-channel resistance, state requirements, interoperability and implementation maturity differ. NIST SP 800-227 provides KEM implementation and usage guidance [4]. A general business paper cannot select the correct parameter set for every service.

### 5.3 Hybrid transition

RFC 9794 defines consistent terminology for PQ/T hybrid schemes and notes that protocol constructions may combine traditional and post-quantum components for transition or risk management [12]. An active IETF draft published in May 2026 defines specific ECDHE-MLKEM groups for TLS 1.3; it remains an Internet-Draft and may change before becoming an RFC [13]. RFC 9980 specifies post-quantum cryptography in OpenPGP and was published in June 2026 [14]. Protocol status must therefore be tracked separately.

A hybrid design is accepted only when:

1. the exact construction and combiner are identified;
2. both component implementations and parameter sets are recorded;
3. downgrade and negotiation behaviour are tested;
4. endpoints and middleboxes interoperate under expected failure cases;
5. logging exposes the negotiated state without leaking secrets;
6. rollback does not silently weaken unrelated services; and
7. the relevant authority accepts residual traditional and post-quantum implementation risk.

### 5.4 Key, certificate and HSM lifecycle

Keys and certificates create operational dependencies across issuance, storage, use, rotation, revocation, recovery, archive and destruction. Larger post-quantum keys or signatures can affect certificate chains, protocol messages, HSM capacity, network devices, smart cards, embedded systems and archival formats. The inventory records maximum object sizes, latency budgets and compatibility limits where material.

Validation evidence is scoped. NIST's CAVP tests approved algorithm implementations. CMVP assesses cryptographic modules within defined boundaries and modes [26]. Procurement requirements should ask for the exact module certificate, security policy, algorithm certificates, version and approved mode where those validations are required. A future roadmap is recorded as a roadmap.

### 5.5 Backups, archives and historical evidence

Backups can preserve both protected data and vulnerable wrapped keys for many years. The programme maps encryption, key wrapping, recovery keys, offline copies, administrators and restoration workflows. A migration plan must state whether old backups will be re-encrypted, retained under compensating controls, expired, or restored through a controlled legacy environment.

Historical signatures need an explicit verification strategy. Contracts, board minutes, valuations, financial statements and software artefacts may need evidence after the original certificate expires or its algorithm is deprecated. The solution may include trusted timestamps, evidence records, archival renewal or re-signing, subject to legal and technical advice. Silent conversion or re-signing can damage evidential meaning.

### 5.6 Security boundary

PQC does not address stolen credentials, malicious administrators, vulnerable endpoints, poor random-number generation, insecure implementations, compromised updates or weak access control. Crypto-agility code can itself expand attack surface if it allows ungoverned algorithms or downgrade. The programme therefore retains defence in depth, least privilege, secure software development, key custody, segmentation, monitoring, recovery and incident response.

## 6. MIGRATION CONTROL SYSTEM

### 6.1 Governance and authority

The accountable executive approves scope and risk appetite. The business-service owner owns availability and data outcomes. The data owner approves confidentiality and integrity horizons. Security architecture approves profiles and design. Engineering owns implementation and rollback. Legal and compliance interpret applicable obligations. Procurement obtains supplier evidence and contractual commitments. Internal audit or independent assurance can test the control system.

| Decision | Recommends | Reviews | Approves |
|---|---|---|---|
| Data-life classification | data owner and records lead | legal, privacy and security | accountable business owner |
| Cryptographic profile | security architecture | engineering and relevant specialists | security authority |
| Supplier acceptance | procurement and service owner | security, legal and resilience | delegated supplier-risk authority |
| Lab exit | engineering | security testing and service owner | change authority |
| Production release | engineering and service owner | security, operations and resilience | named production authority |
| Residual-risk acceptance | service and risk owner | security, legal and finance as relevant | authorised risk acceptor |
| Legacy retirement | engineering and records owner | legal, recovery and operations | service owner and change authority |

### 6.2 The migration packet

Every accepted packet includes:

1. business service, data classes, owners and materiality;
2. current data flows, algorithms, parameters, libraries, keys and certificates;
3. evidence sources, timestamps, gaps and confidence state;
4. confidentiality life, integrity life, device life and migration lead time;
5. standards status and exact supplier/product support;
6. proposed target construction and rationale;
7. threat model, dependencies, performance budget and failure modes;
8. lab, interoperability, load, recovery and security-test results;
9. deployment plan, feature flags, monitoring, rollback and incident playbook;
10. approvals, exceptions, residual risk and next review date; and
11. post-release evidence and legacy-retirement state.

The packet is versioned. Inventory acceptance, design acceptance, pilot acceptance, production acceptance and retirement are separate transitions.

### 6.3 Test design

Testing covers functional correctness and operational behaviour.

| Test class | Questions | Evidence |
|---|---|---|
| Known-answer and implementation | Does the approved implementation behave as specified? | validation records and test results |
| Interoperability | Do all expected clients, servers, gateways and recovery paths work? | version matrix and failures |
| Negotiation and downgrade | Is the selected mode visible and can policy stops be enforced? | captured configuration and telemetry |
| Performance | What happens to latency, throughput, CPU, memory, packet size and HSM capacity? | repeatable baseline and test distribution |
| Availability | How does the service behave during partial support, certificate failure and dependency outage? | fault-injection and recovery evidence |
| Security | Are parsing, side channels, randomness, key handling and error paths within reviewed scope? | specialist test and code evidence |
| Operations | Can keys rotate, certificates renew, backups restore and incidents be diagnosed? | exercised runbooks |
| Archive | Can required historical records still be decrypted and verified? | restoration and verification test |

BIS Project Leap found that PQC integration in financial-system experiments was feasible and also exposed performance and system-modification considerations [16]. Those results support testing. They do not provide a universal latency figure for a family office, SME or vendor product.

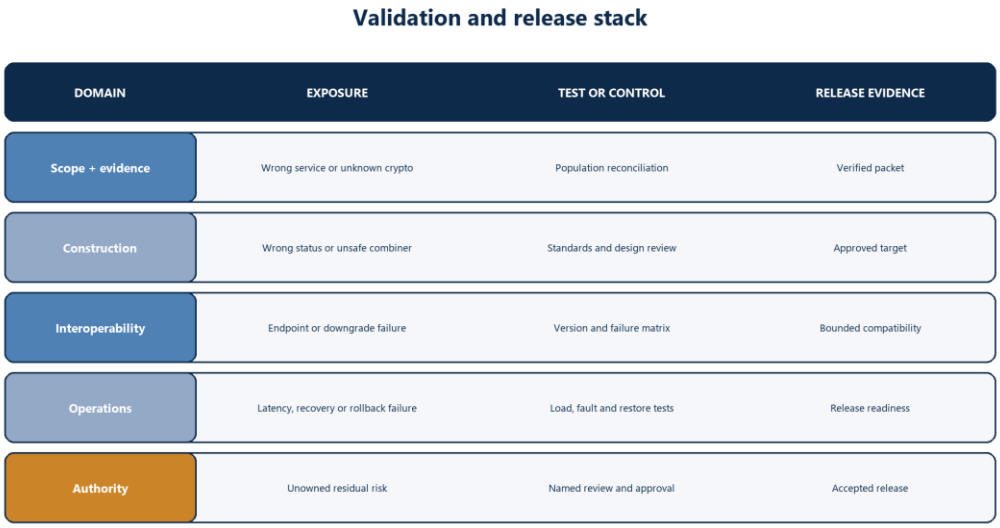


**Figure 5. Validation and release stack for an accepted migration packet**
*Source: Matchpoint synthesis based on [4,5,12,13,15-19,26].*

### 6.4 Stops and rollback

The system should stop a release when the target construction is unidentified, critical endpoints are absent from testing, downgrade behaviour is unobservable, recovery has not been exercised, supplier support is only generic, performance breaches the approved budget, key custody is unresolved, or residual risk lacks an authorised owner.

Rollback is designed before production. It identifies the secure prior state, feature flags, certificate and key state, data written during the new mode, compatibility with old readers, monitoring thresholds and authority. A rollback that exposes long-lived data to a known vulnerable mode may require a separate risk decision.

### 6.5 Supplier assurance

Supplier questionnaires should seek evidence rather than a binary "quantum safe" label:

- exact products, services, versions and cryptographic boundaries;
- current algorithms, parameters, protocols, libraries and certificate dependencies;
- inventory and crypto-agility capability;
- roadmap mapped to final standards and protocol maturity;
- algorithm and module validation state where required;
- hybrid construction and interoperability evidence;
- performance and scaling evidence for relevant service tiers;
- notification process for cryptographic changes or vulnerabilities;
- support, rollback, export and exit provisions; and
- subcontractor and concentrated-service dependencies.

Contractual commitments are labelled as negotiated or proposed until agreed. A public roadmap is not a contractual service level.

## 7. PRODUCTIVITY AND ECONOMICS

### 7.1 The measurable output

The correct unit is an **accepted migration packet at a defined gate**, not a scan result, discovered certificate or generated report. Acceptance requires a complete scope, evidence, review and authority for that stage. This denominator reduces incentives to inflate discovery volume while leaving unresolved dependencies.

Productivity can improve through automated certificate discovery, configuration parsing, dependency matching, evidence retrieval, standards mapping, test orchestration, report assembly and change monitoring. Human review may initially increase because the organisation is seeing previously hidden dependencies. That increase can represent better control rather than lower productivity.

### 7.2 Baseline and pilot design

The organisation selects a bounded population, such as externally accessible services and the identity, email, VPN and data-room dependencies supporting them. It measures a manual baseline on representative cases. It then runs the assisted workflow on a comparable held-out set, preserving case complexity and reviewer criteria.

Metrics include:

- accepted packets per month and per full-time-equivalent team;
- analyst, engineer and reviewer hours per accepted packet;
- time from discovery to each acceptance gate;
- completeness against source populations;
- material-error and rework rate;
- unresolved dependencies and stale evidence;

- test coverage and failed interoperability paths;
- incident, rollback and service-impact measures; and
- direct technology and assurance cost per accepted packet.

### 7.3 Unverified illustrative management scenario

**[Unverified illustrative management assumptions]** The following scenario demonstrates calculation structure. It is not Matchpoint client performance, a forecast, a benchmark or an assurance of savings.

| Input per accepted design-stage packet | Manual baseline | Controlled assisted workflow |
|---|---|---|
| Analyst and engineering hours | 14.0 | 8.0 |
| Reviewer and specialist hours | 4.0 | 4.5 |
| Rework and exception hours | 0.0 included in average | 1.0 |
| Total labour hours | 18.0 | 13.5 |
| Illustrative loaded labour rate | USD 95/hour | USD 95/hour |
| Direct tooling and assurance cost | USD 0 allocated | USD 140/packet |

Under these assumptions, gross labour capacity released is 4.5 hours per accepted packet. At USD 95 per hour, gross capacity value is USD 427.50. After USD 140 of direct tooling and assurance cost, modeled net capacity value is USD 287.50 per packet. At 12 accepted packets per month, the modeled capacity equivalent is USD 3,450 per month.

The scenario does not convert capacity to cash automatically. Cost reduction would require an approved change in actual expenditure. Revenue attribution would require evidence that released capacity caused additional, accepted work and collected revenue. Risk reduction would require an approved model or observed loss evidence. Until those tests are met:

**Attributed revenue: USD 0.**

**Attributed cost reduction: USD 0.**

**Quantified loss reduction: USD 0.**

| Observed labour saving per accepted packet | Gross value at USD 95/hour | Less USD 140 direct cost | Modeled net capacity value |
|---|---|---|---|
| 0.0 hours | USD 0 | USD 140 | USD -140 |
| 2.0 hours | USD 190 | USD 140 | USD 50 |
| 4.5 hours | USD 427.50 | USD 140 | USD 287.50 |
| 7.0 hours | USD 665 | USD 140 | USD 525 |

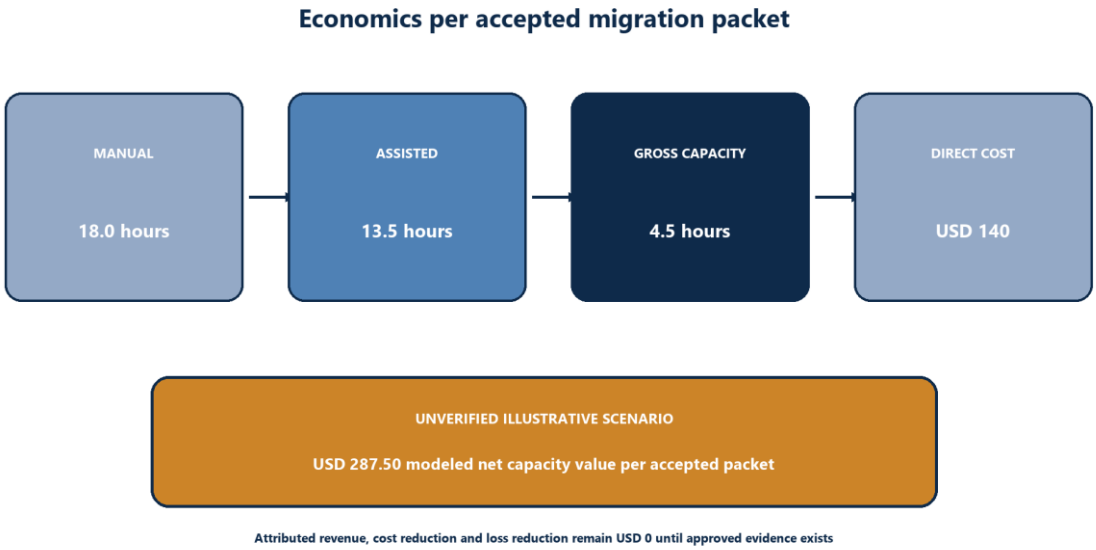


**Figure 6. Productivity and economics per accepted quantum-readiness migration packet**

*Source: Matchpoint scenario analysis. All operating inputs are unverified illustrative management assumptions.*

### 7.4 Revenue and decision value

The Topic Tracker hook asks how the technology multiplies productivity and revenue. The evidence supports a productivity hypothesis that can be tested per accepted packet. It does not support a general revenue multiplier. A credible revenue test would identify the opportunity, capacity constraint, counterfactual, incremental accepted work, pricing, collection and contribution margin. The result would be approved by finance and linked to the deployment cohort.

Decision value may arise from earlier visibility of long-lived data, lower rework, fewer emergency changes, better supplier negotiations and planned technology renewal. These remain hypotheses until the organisation defines and observes suitable measures.

## 8. ADOPTION ROADMAP

### 8.1 Phase 0: establish authority and scope

Name the accountable executive, security authority, service owners, data owners and risk acceptors. Define the initial population, evidence standard, acceptance gates, prohibited claims and incident route. Select a small set of critical and externally exposed services.

### 8.2 Phase 1: classify data and reconcile services

Approve confidentiality and integrity horizons for priority data. Reconcile business services, applications, endpoints, certificates, key stores, devices and material suppliers. Record unknowns without filling gaps. Complete the first dependency graph.

### 8.3 Phase 2: build crypto-agility foundations

Define algorithm policy, abstraction boundaries, configuration ownership, telemetry, key and certificate inventory, validation evidence and change detection. Add contractual information requests to renewals and procurement. Remove obsolete or unowned cryptography through ordinary security remediation where separately approved.

### 8.4 Phase 3: select bounded migration candidates

Choose services where long-lived data, mature support, manageable interoperability and a reversible architecture justify early testing. Record standards status. A final NIST algorithm standard and a draft protocol are different evidence states.

### 8.5 Phase 4: lab and shadow evaluation

Test exact endpoint versions, gateways, certificates, keys, HSM/KMS paths, logging, performance, failures, backups and recovery. Run existing and new modes in a controlled environment. Complete the packet and obtain gate approval.

### 8.6 Phase 5: controlled production

Use feature flags, canary cohorts, maintenance windows, service monitoring and an exercised rollback. Retain evidence of the negotiated cryptographic mode and business-service health. Investigate exceptions through named incident ownership.

### 8.7 Phase 6: scale and retire

Extend by shared dependency and business priority. Track supplier and standards changes. Re-encrypt, re-sign, archive or retire legacy data and mechanisms under approved records and legal guidance. Repeat restoration and verification tests.

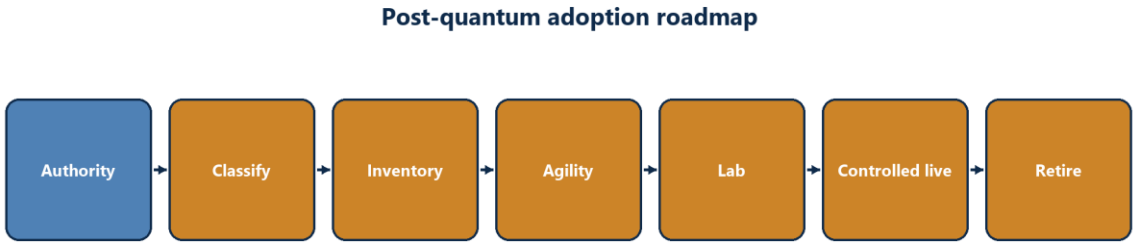


**Figure 7. Adoption roadmap from governance and inventory to controlled migration and legacy retirement**
*Source: Matchpoint framework; external planning references [8-11,15,17-20].*

The NCSC's indicative milestones provide an external planning reference: complete discovery and an initial plan by 2028, highest-priority migration by 2031 and full migration by 2035 [9]. These are target dates for the stated UK guidance. They are not a prediction of Q-Day and do not replace organisation-specific, jurisdiction-specific planning. The EU coordinated roadmap, G7 financial-sector roadmap and BIS framework reinforce early inventory, prioritisation and coordination [10,15,18].

### 8.8 Minimum entry criteria for a family office or SME

An organisation can begin without an internal cryptography laboratory if it has:

1. named business, data and security owners;
2. a defined list of critical services and material suppliers;
3. data-classification and retention decisions;
4. an endpoint, certificate, key-store and application population to reconcile;
5. access to qualified implementation and legal advice;
6. procurement leverage to request version-specific supplier evidence;
7. a change, backup, recovery and incident process; and
8. an evidence repository for accepted packets.

Where these foundations are absent, the first phase is governance and asset management. NCSC describes these activities as central to good cyber-security practice [9].

## 9. CONTROL SCORECARD

### 9.1 Leading indicators

| Dimension | Measure | Required interpretation |
|---|---|---|
| Service coverage | reconciled critical services / defined critical-service population | exclusions approved and current |
| Dependency coverage | verified dependencies / discovered candidate dependencies | candidate and unknown states shown separately |
| Data-life governance | priority data classes with approved confidentiality and integrity horizon | management estimate identified |
| Supplier evidence | material suppliers with version-specific roadmap and evidence | public statements separated from contract commitments |
| Crypto agility | dependencies behind governed abstraction and policy | capability tested, not declared |
| Test readiness | priority candidates with complete interoperability, failure and recovery plan | required endpoints included |
| Release evidence | production migrations with accepted packets | stage and residual risk recorded |
| Legacy retirement | approved legacy dependencies retired or contained | archive and recovery obligations preserved |

### 9.2 Outcome indicators

Outcome measures include service availability during changes, security incidents, emergency rollbacks, material exceptions found before release, restoration success, historical-signature verification success, analyst and reviewer hours, direct cost and accepted packet throughput. There may be long periods without a loss event. The absence of observed loss does not prove quantum readiness.

### 9.3 Reporting boundaries

Management reporting should state:

- the population and cut-off date;
- verified, candidate, stale and unknown counts;
- standards and product status at the reporting date;
- unverified management estimates;
- accepted migration stages and residual risks;
- material suppliers without sufficient evidence;
- service incidents and rollbacks; and
- productivity evidence without translating capacity to revenue unless finance approves attribution.

## 10. LIMITATIONS AND FURTHER RESEARCH

The existence and arrival date of a CRQC remain uncertain. This paper does not estimate either. New cryptanalysis, revised standards, implementation vulnerabilities and protocol evolution can change migration choices. Final algorithm standards do not remove implementation and integration risk.

The paper does not test a specific family office, SME, bank, software product or cloud service. The productivity scenario is unverified and illustrative. The financial-sector experiments cited use their own architectures and test conditions. The UAE regulatory sources establish present cryptographic-control context within their stated scope, not a complete PQC rulebook.

Further research should examine measured migration performance across representative financial protocols, post-quantum certificate and archival-signature operations, HSM and KMS capacity, endpoint and middlebox interoperability, side-channel assurance, supplier-contract evidence, long-lived data classification, and accepted-packet economics. Sector collaboration is particularly important for shared payment, identity, certificate and cloud dependencies.

## 11. CONCLUSION

The central management question is not when Q-Day will occur. The actionable question is whether the organisation can identify, prioritise, change and prove the cryptography protecting financial data before its required protection horizon is exceeded.

NIST's final ML-KEM, ML-DSA and SLH-DSA standards provide a usable algorithm foundation [1-3]. NIST's KEM and crypto-agility guidance, IETF protocol work, the NCSC timeline, the EU roadmap, BIS research and experiments, the G7 financial-sector roadmap, Europol coordination and the Bank of England's 2026 assessment show that transition is a multi-year governance and engineering programme [4,5,9,10,12-20].

Family offices and SMEs can begin with a proportionate operating model: classify long-lived financial data; reconcile business services and suppliers; create a cryptographic dependency graph; establish crypto agility; test exact standards and constructions; release through accepted migration packets; and preserve rollback, archives and named authority.

The accepted quantum-readiness migration packet creates a measurable unit of work. It connects standards to a specific service, data life, implementation, test and approval. Productivity can be tested on observed time, quality and cost. Revenue and risk attribution remain zero until approved evidence supports a claim.

## DECLARATIONS

**Author:** Chennakeshav (CK) Adya, Independent Researcher.

**Research status:** Independent working paper prepared from the cited sources available through 1 August 2026.

**Funding:** No external funding was reported for this paper.

**Conflicts of interest:** The author is associated with Matchpoint Partners. The paper describes a Matchpoint operating framework. No vendor product is endorsed.

**Data availability:** No confidential client data, proprietary cryptographic inventory or client performance dataset was used. The productivity scenario uses unverified illustrative management assumptions.

**Use of AI:** AI-assisted tools supported research organisation, drafting and figure production. The author retains responsibility for review and release.

**Disclaimer:** This is a research paper, not investment, cybersecurity, cryptographic-engineering, legal, regulatory, tax, accounting or technology-procurement advice. Organisations should obtain qualified advice and conduct system-specific testing.

## REFERENCES

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

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

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

[4] Alagic, G., Barker, E., Chen, L., Moody, D., Robinson, A., Silberg, H., & Waller, N. (2025). *NIST SP 800-227: Recommendations for Key-Encapsulation Mechanisms*. https://doi.org/10.6028/NIST.SP.800-227

[5] Barker, E., et al. (2026). *NIST CSWP 39upd1: Considerations for Achieving Crypto Agility: Strategies and Practices*. Updated 29 June 2026. https://doi.org/10.6028/NIST.CSWP.39-upd1

[6] Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). *NIST IR 8547 Initial Public Draft: Transition to Post-Quantum Cryptography Standards*. https://csrc.nist.gov/pubs/ir/8547/ipd

[7] National Institute of Standards and Technology. (2025). *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption*. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[8] Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. (2023). *Quantum-Readiness: Migration to Post-Quantum Cryptography*. https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf

[9] UK National Cyber Security Centre. (2025). *Timelines for migration to post-quantum cryptography*. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[10] NIS Cooperation Group and European Commission. (2025). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[11] European Commission. (2024). *Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*. https://eur-lex.europa.eu/eli/reco/2024/1101/oj

[12] Driscoll, F., Parsons, M., & Hale, B. (2025). *RFC 9794: Terminology for Post-Quantum Traditional Hybrid Schemes*. https://www.rfc-editor.org/rfc/rfc9794.html

[13] Kwiatkowski, K., Kampanakis, P., Westerbaan, B. E., & Stebila, D. (2026). *Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3, draft-ietf-tls-ecdhe-mlkem-05*. Internet-Draft, 26 May 2026. https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/

[14] Wussler, A., Kousidis, S., Kampanakis, P., Thomalla, F., & Fluhrer, S. (2026). *RFC 9980: Post-Quantum Cryptography in OpenPGP*. https://www.rfc-editor.org/rfc/rfc9980.html

[15] Auer, R., Dodson, D., Dupont, A., Haghighi, M., Margaine, N., Marsden, D., McCarthy, S., & Valko, A. (2025). *Quantum-readiness for the financial system: a roadmap*. BIS Papers No. 158. https://www.bis.org/publ/bppdf/bispap158.htm

[16] BIS Innovation Hub. (2023-2026). *Project Leap: quantum-proofing the financial system*. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

[17] Bank of England. (2026). *Financial Stability Report - July 2026*, quantum preparedness discussion. https://www.bankofengland.co.uk/financial-stability-report/2026/july-2026

[18] G7 Cyber Expert Group. (2026). *Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector*. https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

[19] Europol and FS-ISAC. (2026). *Prioritising post-quantum cryptography migration activities in financial services*. https://www.europol.europa.eu/media-press/newsroom/news/joint-report-outlines-practical-approach-to-prioritising-post-quantum-cryptography-migration-in-financial-services

[20] Europol Quantum Safe Financial Forum. (2025). *Quantum Safe Financial Forum - A call to action*. https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

[21] Central Bank of the UAE, Securities and Commodities Authority, Dubai Financial Services Authority, & Financial Services Regulatory Authority. (2021). *Guidelines for Financial Institutions adopting Enabling Technologies*. https://rulebook.centralbank.ae/en/rulebook/guidelines-financial-institutions-adopting-enabling-technologies

[22] UAE Telecommunications and Digital Government Regulatory Authority. (2020). *UAE Information Assurance Regulation, version 1.1*. https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/UAE-Information-Assurance-Regulation-v1-1-pdf.ashx

[23] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134. https://doi.org/10.1109/SFCS.1994.365700

[24] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[25] Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? *IEEE Security & Privacy, 16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

[26] National Institute of Standards and Technology. (2026). *Cryptographic Module Validation Program: validated modules and validation caveats*. Updated 15 July 2026. https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

[27] National Institute of Standards and Technology. (2026). *Post-Quantum Cryptography publications*. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/publications

## APPENDIX A. MINIMUM MIGRATION PACKET

1. Packet ID, stage, owner, reviewers, approver and effective date.
2. Business service, materiality, recovery requirement and jurisdictions.
3. Data classes, confidentiality life, integrity life, retention and owners.
4. Current data-flow and cryptographic-dependency diagram.
5. Exact algorithms, parameters, libraries, protocols, keys, certificates and versions.
6. Evidence register with timestamps, source strength, gaps and unknowns.
7. Supplier, subcontractor, support, validation and contractual state.
8. Standards status and proposed target construction.
9. Threat model, performance budget, failure modes and residual risk.
10. Interoperability, security, load, recovery and archive test evidence.
11. Deployment, monitoring, rollback and incident plan.
12. Approval, exceptions, next review and legacy-retirement state.

## APPENDIX B. CRYPTOGRAPHIC INVENTORY FIELDS

- Immutable dependency ID and version.
- Business service and service owner.
- Data class and data owner.
- Source and destination endpoints.
- Cryptographic purpose: key establishment, encryption, signature, hash, authentication, wrapping or secure boot.
- Algorithm, parameter set, mode and protocol.
- Library, module, product, firmware and exact version.
- Key store, HSM or KMS; custody, rotation, recovery and expiry.
- Certificate issuer, subject, trust anchor, chain and renewal path.
- External visibility and collection exposure.
- Confidentiality, integrity, signature-verification and device life.
- Supplier and subcontractor dependencies.
- CAVP, CMVP or other validation evidence where required.
- PQC and crypto-agility support state.
- Target construction, test state, migration stage and rollback.
- Evidence timestamp, confidence, owner and next review.

## APPENDIX C. PILOT ACCEPTANCE CHECKLIST

1. Pilot population reconciles to an approved source population.
2. Every candidate has a business-service and data owner.
3. Exact current algorithms and implementations are verified.
4. Standards and protocol status are dated and correctly labelled.
5. The target construction and combiner are identified.
6. Endpoint, middlebox, identity, certificate and recovery paths are tested.
7. Baseline and target performance distributions are recorded.
8. Negotiated modes and downgrade states are observable.
9. Backups, restoration and historical verification are exercised.
10. Rollback is documented and rehearsed.
11. Exceptions and residual risk have named authority.

12. Productivity evidence uses accepted packets as the denominator.

## APPENDIX D. GLOSSARY

CAVP: NIST Cryptographic Algorithm Validation Program.
CMVP: NIST Cryptographic Module Validation Program.
CRQC: Cryptographically relevant quantum computer.
Crypto agility: Controlled capability to replace and adapt cryptography while preserving security and operations.
HNDL: Harvest now, decrypt later; collection of protected data for possible future decryption.
KEM: Key-encapsulation mechanism.
ML-DSA: Module-Lattice-Based Digital Signature Algorithm, standardised in FIPS 204.
ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism, standardised in FIPS 203.
PQC: Post-quantum cryptography.
PQ/T hybrid: A multi-algorithm scheme with at least one post-quantum and one traditional asymmetric component.
Q-Day: Informal shorthand in this paper for the unknown future point at which a CRQC can attack cryptography at relevant scale.
SLH-DSA: Stateless Hash-Based Digital Signature Algorithm, standardised in FIPS 205.