KQUANTA RESEARCH

Post-Quantum Cryptography: A 2026 Strategic Imperative for Financial Services Boards

Preparing for the Quantum Threat

Contents

Executive Summary

Post-quantum cryptography (PQC) is now a board-level issue for financial services. The reason is simple: quantum computing is expected to make today's most widely deployed public-key cryptography (for example RSA and elliptic-curve cryptography) vulnerable. That creates two distinct, material risks for banks, insurers, capital markets, and financial market infrastructures.

The first is a confidentiality risk commonly described as "Harvest Now, Decrypt Later" (HNDL). Adversaries can collect encrypted traffic and stored ciphertext today, hold it, and decrypt it later when a Cryptographically Relevant Quantum Computer (CRQC) becomes available. Long-lived data – customer identity records, statements, transaction histories, trading strategies, and supervisory communications – is therefore already in scope.

The second is a newer integrity risk that boards should treat as equally, if not more, damaging: *"Trust Now, Forge Later" (TNFL).* Digitally signed artefacts created today – contracts, KYC records, audit evidence, certificates, software/firmware updates, and payment messages – may be harvested now, and later forged at scale if their signature scheme becomes quantum-vulnerable. For financial services, this is existential: the sector's foundation is trust in transaction authenticity, non-repudiation, and auditable records.

Regulators and standards bodies have moved from awareness to action. NIST finalised its first PQC standards (FIPS 203/204/205) in August 2024, creating an implementable baseline for migration. The U.S. government's OMB memo on migrating to PQC (M-23-02) requires agencies to inventory cryptographic systems and plan the transition. Several jurisdictions have issued timelines and expectations that converge on the same message: inventory now, pilot early, and avoid a rushed, brittle migration later.

For India, the strategic context is defined by rapid digitalisation (UPI scale, API-driven fintech growth, expanding digital identity) and rising cyber operational risk. India's cyber resilience frameworks – including RBI's cybersecurity baseline for banks and SEBI's CSCRF for regulated entities – already require strong governance, incident readiness, and third-party control. PQC should now be integrated into those same governance mechanisms as a forward-looking systemic risk. India's National Quantum Mission (approved at Rs 6003.65 crore) signals that quantum capability and its security implications will intensify through this decade.

This whitepaper provides boards with: (1) a threat landscape that clearly separates confidentiality and integrity impacts; (2) a global and India-focused regulatory view; (3) a practical risk assessment framework; and (4) a migration roadmap from 2026 to 2030 that prioritises crypto-agility, hybrid approaches, and measurable governance.

From a board perspective, the most urgent insight is not the exact date of "**Q-Day**". It is the overlap between data longevity and migration lead time. If your institution must preserve confidentiality for 10+ years or authenticity for decades, then the migration window is already open. Boards should treat PQC as a strategic resilience programme – comparable to enterprise-wide payments modernisation or core banking transformation – not as a point product purchase.

Board Action Timeline (Indicative 2026–2030)

Horizon	Board Decision Focus	Minimum Outcomes
Q1–Q2 2026	**Governance, inventory mandate, funding guardrails**	**Board-approved PQC programme, crypto inventory underway, TNFL exposure mapped**
H2 2026	**Pilots and vendor posture**	**Hybrid/PQC pilots in non-critical paths; vendor contracts updated for crypto-agility**
2027–2028	**Scale in critical systems**	**PQC/hybrid rollout in priority systems (PKI, signing, key exchange); SOC monitoring**
2028–2030	**Completion and optimisation**	**Legacy decommissioning plan; audit-ready evidence; continuous crypto-agility**

Indicative investment: Most institutions should plan for a multi-year programme spanning architecture work, cryptographic discovery, platform upgrades (PKI, HSMs, TLS stacks), testing, vendor remediation, and staff training. A realistic board posture is to approve a staged programme budget and demand measurable outcomes each quarter, rather than defer funding until compliance deadlines compress timelines.

Executive Summary: Key Takeaways

1. Dual threat: Encrypted data harvested now will be decrypted later; quantum forgery will break digital signatures and financial trust.

2. Timeline: 3–5 year migration. Act now if data must stay secure beyond 2030.

3. 2026 actions: Inventory all cryptography, assign executive owner, pilot hybrid solutions.

1. The Quantum Threat Landscape

1.1 What is Post-Quantum Cryptography (PQC) in business terms?

Quantum computing harnesses the principles of quantum physics to perform certain calculations far more rapidly than conventional computers. Put simply, quantum computers exploit quantum mechanical properties—such as superposition and entanglement—to process information in fundamentally different ways, enabling them to solve certain complex problems that would take traditional computers thousands of years to crack. By 2026, it has moved beyond theoretical study: sustained government and private-sector investment is reducing technical barriers, and early commercial and state-level capabilities are emerging. Whilst today's quantum systems cannot yet break encryption at scale, the trajectory is clear. As these capabilities mature—widely anticipated between 2030 and 2035—they will undermine the cryptographic foundations of financial services. RSA (Rivest–Shamir–Adleman), which protects data by relying on the difficulty of factoring large numbers, and ECC (Elliptic Curve Cryptography), which secures digital signatures and authentication through elliptic-curve mathematics, are both vulnerable to sufficiently powerful quantum computers.

The implications are far-reaching: for banks, this threatens payments, secure communications, and interbank trust; for asset managers, it risks the integrity of trade records, mandates, and long-lived client data; for insurers, it affects policy records, claims evidence, pricing models, and reinsurance contracts that must remain verifiable for decades.

Post-quantum cryptography (PQC) addresses this exposure by replacing vulnerable cryptography with algorithms designed to remain secure against quantum attacks. For boards, PQC is not simply a technology upgrade but a resilience and continuity obligation—central to safeguarding long-term financial trust. PQC does not require firms to deploy their own quantum computers; rather, it requires them to upgrade the cryptographic foundations that underpin applications, networks, devices, and partner connections before adversaries gain quantum capability.

1.2 The 'Harvest Now, Decrypt Later' (HNDL) threat - confidentiality at risk

HNDL is a strategic cyber threat where adversaries collect encrypted data today with the intent to decrypt it later when quantum capability is sufficient to break widely used public-key algorithms.

This is especially relevant to financial services because:

(a) sensitive data has long shelf-life, and

(b) institutions must retain records for regulatory and legal obligations.

Real-world harvesting behaviour is consistent with standard intelligence tradecraft: large-scale collection of network traffic, email, backups, and cloud data stores.

Financial data at risk includes customer identity and KYC records, payment and transaction histories, confidential supervisory communications, proprietary trading and risk models, and M&A documentation.

Data 'shelf-life' is often longer than the encryption used to protect it. If confidentiality must hold for 10–20 years, then harvesting today can still be damaging even if CRQCs arrive later.

1.3 The 'Trust Now, Forge Later' (TNFL) threat - integrity and authenticity at risk

TNFL is the integrity analogue of HNDL. It assumes that adversaries can copy digitally signed artefacts now and later create convincing forgeries once the signature scheme is quantum-vulnerable. For financial services, this is a governance-level risk because it undermines non-repudiation, evidentiary value, and the reliability of audit trails.

Examples of artefacts vulnerable to TNFL include: digital contracts, board and committee approvals executed electronically, KYC attestations, signed regulatory submissions, software/firmware signing records, certificate chains, and cryptographically signed logs.

Board-level implication: while HNDL is comparable to a confidentiality breach, TNFL can enable retroactive disputes about transactions and obligations. This threatens the legal enforceability of agreements, the evidentiary strength of records, and the credibility of compliance reporting. UK guidance on PQC migration timelines explicitly emphasises the need to start early to avoid a rushed transition that could impair trust.

1.4 Timeline to 'Q-Day' and why data shelf-life matters more

There is no single agreed date for when Cryptographically Relevant Quantum Computers (CRQCs) will be available. Timelines vary based on technical breakthroughs in error correction, scaling, and control systems. Boards should avoid anchoring on a single year and instead govern to data longevity.

Quantum timeline framing for Boards (illustrative)

View	Assumption	Board posture
Conservative	CRQC arrives nearer the 2030s	Still start now: migration takes years; long-lived confidentiality and signature integrity remain exposed
Aggressive	CRQC arrives earlier in the 2030s or late 2030s	Compress timeline: prioritise highest-value assets and signing/PKI; accelerate vendor remediation
Operational reality	Exact date unknown	Govern to data shelf-life + dependency mapping; build crypto-agility to absorb new standards

Regardless of whether CRQCs arrive later or sooner, the governance conclusion for boards is the same: action must begin now. Cryptographic migration takes many years, while sensitive data, contracts, and digital signatures created today must remain secure and trustworthy for decades. If quantum arrives earlier, timelines must be compressed and priority given to high-value data, signing systems, and vendor readiness. Because the exact arrival date is unknowable, the most prudent board posture is to govern to data longevity and system dependencies, building crypto-agility so the organisation can adapt to new standards without disruption.

1.5 Financial services exposure - where PQC matters first

- Payments and transaction security: TLS, key exchange, message authentication, and signing in payment rails and gateways.
- Customer data and identity: encryption-at-rest, secure APIs, identity proofing records, and long-lived customer communications.
- Digital signatures and PKI: certificates, signing services, document workflows, code signing, and signed logs (TNFL exposure).
- Market infrastructure and cross-border messaging: SWIFT-related security controls, settlement, and regulatory reporting exchanges.
- Blockchain and digital assets: signature schemes, wallet security, smart contracts, and long-lived on-chain records.

Section 1: Key Takeaways

1. Quantum risk has two faces: HNDL targets confidentiality, while TNFL targets authenticity and non-repudiation - a direct threat to financial trust.

2. Boards should govern to data and signature longevity, not to an uncertain 'Q-Day'; long-lived records create exposure today.

3. The first financial priorities are PKI and signing (TNFL), plus high-value communications paths (TLS/key exchange) in payments and critical interconnections.

2. Global PQC Regulatory and Standards Landscape

The global direction is clear: standard-setters are finalising implementable algorithms and governments are establishing migration timelines. Financial institutions should expect heightened supervisory scrutiny, particularly where systemic infrastructures and cross-border dependencies are concerned.

2.1 United States

The United States has moved from defining PQC standards to actively driving adoption. In August 2024, NIST finalised the first federal PQC standards—ML-KEM (FIPS 203) for secure key exchange and ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures—providing a clear baseline for government and regulated industries.

In March 2025, NIST reinforced this approach by selecting *Hamming Quasi-Cyclic* (HQC) as an additional encryption method, deliberately diversifying cryptographic foundations to reduce systemic risk. Further standards are expected to follow through 2026–2027.

Implementation is now being enforced through policy and timelines. Federal agencies are required to inventory quantum-vulnerable cryptography and execute funded, multi-year migration plans, while national security systems are following a phased transition roadmap through 2035, with earlier requirements for software, firmware, and network protections. Legislative momentum has added near-term pressure, with pilot deployments of PQC in high-impact systems expected by 2027.

For boards, the message is clear: PQC is no longer a future technology consideration, but a live compliance and resilience issue requiring capital allocation, vendor readiness assessment, and sustained governance oversight over the next decade.

2.2 European Union

The European Union is pursuing a coordinated, risk-based transition to post-quantum cryptography (PQC), focused on early planning and regulatory alignment rather than rapid technical change. The EU cybersecurity agency ENISA has issued guidance clarifying the status of PQC standards and the practical realities of migration, helping organisations focus on performance, interoperability, and vendor readiness. This work signals that quantum-safe planning will increasingly sit within existing EU cyber-resilience and digital operational resilience expectations, rather than being treated as a niche technology issue.

This approach has been formalised through an EU-wide roadmap led by the European Commission and developed by the *NIS Cooperation Group*, a forum bringing together Member States and EU institutions to align national cybersecurity priorities.

Published in June 2025, the roadmap sets out a phased transition:

- by December 2026, Member States should have national PQC transition plans focused on awareness and system identification;
- by December 2030, high-risk use cases should be addressed with resources allocated and PQC deployed by default in priority systems; and
- by 2035, a full transition should be completed wherever technically feasible.

The roadmap also promotes the use of standardised and tested hybrid cryptographic solutions during the transition. For boards, this frames PQC as a long-term governance and resilience obligation, closely tied to regulatory compliance, third-party risk, and continuity of digital trust.

2.3 United Kingdom

In January 2026, the UK's National Cyber Security Centre (NCSC) clarified its national approach to post-quantum cryptography (PQC), stressing early preparation, disciplined prioritisation, and phased execution rather than rapid or fragmented change. The central message for boards is governance-led migration: organisations are expected to understand their cryptographic exposure early, run controlled pilots, and manage transition well before deadlines tighten. PQC is framed not as a technical upgrade, but as a long-term resilience and risk-management programme requiring sustained oversight.

Building on guidance issued in 2025, the NCSC set out a three-phase national roadmap for PQC migration. The first phase, Discover and plan (to 2028), focuses on full system discovery and inventory of quantum-vulnerable cryptography.

The second phase, Prioritise and pilot (2028–2031), targets high-risk and high-value systems, with pilots and testing in controlled environments. The final phase, Complete adoption (2031–2035), aims for full PQC migration across systems, services, and products.

Throughout, the NCSC emphasises careful testing, validation, and central coordination to avoid introducing new security or operational risks.

For boards, this underscores that PQC readiness in the UK represents a multi-year governance obligation, intrinsically linked to asset prioritisation, vendor assurance, and long-term investment planning—not a last-minute compliance exercise.

2.4 Australia

Australia has adopted a clear, directive approach to PQC, with defined planning and transition expectations anchored in national security guidance. The Australian government's position is set out in the *Australian Signals Directorate* (ASD) Information

Security Manual, which states that traditional asymmetric cryptography should not be relied upon beyond 2030.

Organisations are expected to have a refined and approved transition plan in place by the end of 2026, with migration of critical systems and high-value data commencing by 2028.

For boards, the Australian position is notable for its specific time-bound expectations rather than high-level principles. PQC readiness is treated as a national security and resilience issue, with implications for government agencies, critical infrastructure operators, and organisations handling sensitive or long-lived data.

2.5 Canada

Canada released its post-quantum cryptography (PQC) roadmap in June 2025, setting a phased transition for non-classified government IT systems through 2035.

Initial departmental migration plans are due by April 2026, with annual progress reporting thereafter.

High-risk and high-priority systems must be migrated by 2031, with remaining systems completed by 2035, under guidance from the Canadian Centre for Cyber Security.

2.6 Asia

Asian regulators and central banks are exploring quantum security implications. Singapore's Monetary Authority of Singapore (MAS) issued an advisory on addressing quantum-related cybersecurity risks, including monitoring developments and beginning preparations to protect financial services.

Japan is following a dual-track quantum strategy, combining post-quantum cryptography (PQC) with selective use of Quantum Key Distribution (QKD).

PQC evaluation and guidance are led by CRYPTREC, with a strong focus on the "2030 Cryptography Problem"—the risk that today's systems may not remain secure through the decade. Overall coordination of Japan's quantum strategy is signposted by the Cabinet Office of Japan.

Several Asian jurisdictions are also running proof-of-concept projects integrating PQC into payment rails and critical infrastructures.

2.6 International bodies and market infrastructures

International coordination is increasing through financial stability and market infrastructure channels. Global cyber resilience guidance from bodies such as the Financial Stability Board (FSB) reinforces the principle that cyber incidents can become systemic. Quantum risk should be governed within that same systemic lens, especially for FMIs and cross-border networks.

Global signals - what boards should watch

Signal type	Examples	Implication for boards
Standards	NIST FIPS 203/204/205; ISO/IEC work	Vendor products will converge on standard algorithms; boards can demand roadmaps tied to standards
Government mandates	OMB M-23-02; CNSA 2.0 timelines	Supervisory scrutiny and procurement requirements will flow into critical suppliers
Regulator expectations	NCSC timelines; MAS advisory; EU cyber resilience	PQC becomes an audit and resilience programme, not optional research
Market infrastructure	Cross-border messaging and settlement dependencies	Institutions must coordinate migration with counterparties and vendors

Taken together, these global signals indicate that PQC is moving rapidly from a technical horizon issue to a board-level matter of governance, resilience, and accountability. Standards are crystallising, governments are setting explicit timelines, regulators are signalling supervisory expectations, and market infrastructure dependencies mean no institution can migrate in isolation.

For boards, the implication is clear: PQC readiness should now be overseen as a structured, multi-year transition programme—embedded in enterprise risk, audit, and supplier governance—rather than treated as discretionary experimentation. Early board attention will shape credibility, regulatory confidence, and long-term trust as quantum-era risks become operational realities.

Section 2 : Key Takeaways

1. Regulatory and standards convergence means boards should assume PQC will become an expected element of cyber resilience and third-party assurance.

2. Jurisdictional differences matter most in timing and reporting; institutions should map which regulators, counterparties, and markets drive their earliest deadlines.

3. First movers can reduce transition risk and avoid rushed cutovers, but governance must prevent 'crypto panic' purchases that create lock-in or fragile designs.

3. India's PQC Readiness and Regulatory Environment

India's financial sector has achieved rapid digital scale (UPI and API ecosystems), which increases the importance of cryptographic trust at the system level. India's regulatory approach to cyber resilience already emphasises governance, monitoring, and third-party discipline. PQC should now be incorporated as a forward-looking component of cyber resilience and operational risk.

3.1 Government initiatives and national capability

India's National Quantum Mission (NQM) was approved by the Union Cabinet with a total outlay of ₹6,003.65 crore (approximately USD 730 million) for the period 2023-24 to 2030-31. The mission aims to seed and scale research and industrial capability across quantum computing, communication, sensing, and materials - and therefore implicitly expands the urgency of quantum-safe security planning.

Agencies and research bodies (for example C-DAC and leading IITs) continue to build domestic capability in quantum computing and cryptography research.

For boards, the relevance is practical: national capability accelerates ecosystem adoption, which raises the priority of standards-aligned security migration in regulated sectors.

3.2 Regulatory frameworks relevant to PQC governance

PQC is not yet uniformly mandated in India across all regulators; however, existing cyber resilience obligations provide a strong governance foundation for PQC adoption:

- RBI's cybersecurity framework for banks establishes baseline expectations including governance, security operations monitoring, and resilience controls.
- SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) for regulated entities defines requirements and timelines for cyber controls and audit readiness.
- CERT-In directions require time-bound reporting of specified cyber incidents and operational cyber hygiene measures, reinforcing the need for cryptographic visibility and logging integrity.

3.3 Payment and market infrastructure considerations

Payment systems and Financial Market Infrastructure (FMI) depend on cryptographic integrity across interbank messaging, authentication, device security, and audit trails. PQC considerations should be integrated into critical infrastructure programmes (for example certificate management, hardware security module (HSM) lifecycle, transaction signing, and secure APIs), coordinated with operators and major vendors.

3.4 Industry readiness in India - emerging but uneven

Evidence from industry surveys and public commentary suggests that awareness of quantum risk is increasing, but practical readiness (inventory, testing, vendor alignment) remains uneven. Boards should assume that the biggest blockers will be legacy dependencies, vendor readiness, and limited internal cryptographic visibility - not algorithm selection.

3.5 Opportunity for India: leadership through governance discipline

India's scale and digital public infrastructure create an opportunity to lead in PQC transition governance.

Institutions that start early can:

(a) influence vendor roadmaps,

(b) reduce systemic transition risk, and

(c) position themselves as trusted cross-border counterparties as global standards adoption accelerates.

Section 3 : Key Takeaways

1. India's cyber resilience frameworks (RBI, SEBI CSCRF, CERT-In) already provide governance levers that can incorporate PQC without waiting for a single new 'PQC law'.

2. Boards must manage both domestic and international compliance pull: cross-border counterparties and global vendors may set earlier de facto deadlines than local mandates.

3. Early movers in India can lead on ecosystem coordination (payments, PKI, vendors) and reduce systemic risk created by rushed, fragmented migrations.

4. Financial Services Quantum Risk Assessment Framework

Boards need a structured method to quantify exposure and prioritise action. This section provides an assessable framework aligned to enterprise risk management (ERM), third-party risk, and audit expectations.

4.1 Asset inventory and classification

A PQC risk programme starts with cryptographic asset discovery. Institutions should inventory where cryptography is used - not just in obvious security tools, but embedded inside applications, APIs, devices, and vendor products.

- Cryptographic use cases: key exchange (TLS, VPN), digital signatures (documents, code signing), encryption-at-rest, tokenisation, identity and authentication, and signed logging.
- Classify by data longevity: how long confidentiality must hold and how long authenticity must be defensible (often longer than confidentiality).
- Classify by system criticality: customer-facing, payment and settlement, regulatory reporting, treasury/markets, and internal governance artefacts.

4.2 Vulnerability analysis - where quantum breaks first

- Legacy systems: older TLS libraries, embedded devices, long-lived certificates, and hard-coded cryptographic assumptions.
- Third-party and vendor dependencies: HSMs, PKI vendors, cloud services, API gateways, fintech partners, and market infrastructure providers.
- Supply chain cryptographic risks: code signing and software update chains are a primary TNFL surface.
- Cloud and hybrid infrastructure: shared responsibility and versioning complexity demand explicit PQC roadmaps from providers.

4.3 Impact scenarios - confidentiality failures (HNDL)

HNDL impact is primarily economic and regulatory: historic customer data exposure, leakage of strategic information, and increased fraud risk. Boards should assess which data categories would be materially harmful if revealed years later (for example, high-net-worth client communications, sensitive corporate actions, privileged supervisory records).

4.4 Impact scenarios - integrity failures (TNFL)

TNFL impact is legal, operational, and systemic. Boards should examine where signatures and audit trails serve as proof of truth.

- Disputed historic transactions: the credibility of signed payment or settlement evidence could be questioned.
- Contract repudiation: electronically signed agreements may face evidentiary challenges if the signing scheme becomes vulnerable.
- Compliance record tampering: signed logs and regulatory submissions risk losing integrity if quantum-vulnerable signatures can be forged.
- Reputational harm: loss of digital trust can trigger customer flight and supervisory escalation.

4.5 Risk mitigation strategies - design principles

- Hybrid cryptography: combine classical and PQC mechanisms during transition to reduce single-point algorithm risk.
- Crypto-agility: build the ability to swap algorithms and parameters without redesigning systems; enforce configuration-driven cryptography.
- Vendor governance: require PQC roadmaps, test evidence, and migration support clauses in contracts and RFPs.
- Risk transfer: assess cyber insurance posture; ensure underwriting discussions reflect quantum and long-horizon integrity risks.

Practical Board Risk Matrix (illustrative)

Domain	Quantum impact	Board priority
PKI and signing	High TNFL exposure; systemic trust dependency	Immediate
Payments and secure channels	High HNDL + integrity risk; ecosystem coupling	Immediate
Customer identity and records	Long-lived confidentiality + authenticity	High
Market infrastructure links	Cross-border dependency and coordination	High
Internal enterprise apps	Mixed; depends on longevity and exposure	Medium

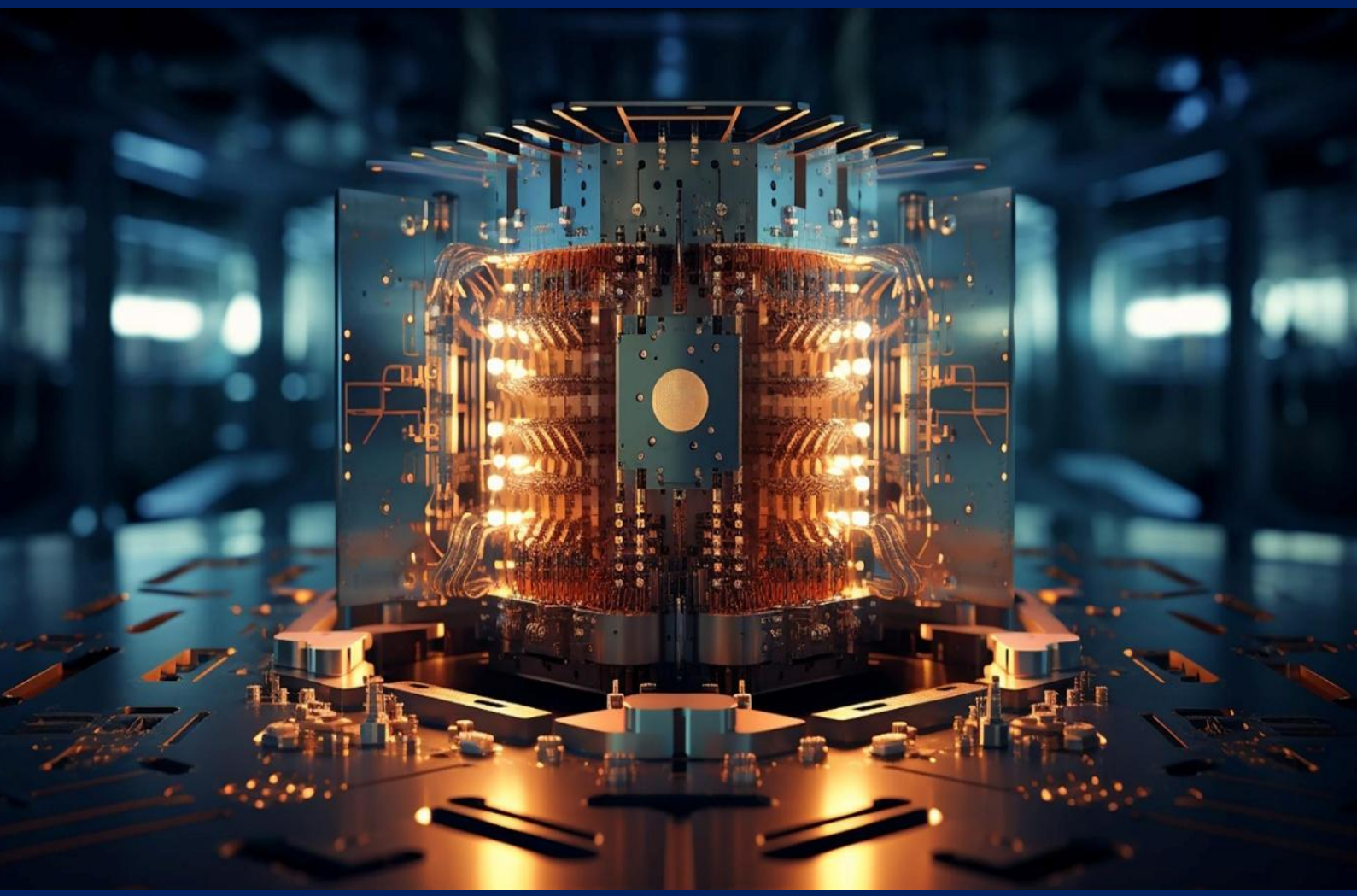
This matrix underscores that quantum risk is uneven across the organisation and should be addressed through a risk-weighted governance lens. Areas tied to systemic trust—particularly PKI, signing, and payments—require immediate board attention, while other domains can be sequenced based on data longevity and external dependency. The core board imperative is to prioritise trust-critical functions and treat quantum readiness as a staged resilience programme, not a blanket technology refresh.

Section 4 : Key Takeaways

1. Quantum risk cannot be managed without cryptographic visibility; a board-mandated inventory is the first control.

2. TNFL turns signature integrity into a legal and systemic risk; boards should prioritise PKI, signing, and audit evidence early.

3. Mitigation is an architecture programme (hybrid + crypto-agility + vendor governance), not a single algorithm swap.



5. PQC Migration Roadmap for Financial Institutions (2026–2030)

A realistic PQC programme is phased, measurable, and coordinated with vendors and regulators. The objective is to avoid rushed cutovers that create outages, broken interoperability, or fragile cryptography.

Phase 1: Assessment and Planning (2026)

- Complete cryptographic inventory across enterprise, cloud, vendors, and embedded environments.
- Execute risk assessment covering HNDL and TNFL, including data and signature longevity mapping.
- Approve budgets and business case; define KPIs and quarterly reporting cadence.
- Evaluate vendor readiness; initiate RFP language for PQC and crypto-agility.
- Stand up governance: steering committee, risk ownership, and audit alignment.

Phase 2: Pilot and Testing (2026–2027)

- Proof-of-concept implementations for TLS/key exchange and signatures in controlled environments.
- Hybrid deployments in non-critical services to validate interoperability and performance.
- Cryptographic performance testing (latency, bandwidth, HSM compatibility, certificate sizes).
- Training programmes for security architects, engineers, and procurement teams.
- Independent assessment and readiness reviews; create a production cutover playbook.

Phase 3: Production Deployment (2027–2028)

- Prioritise critical systems: PKI, signing services, payments gateways, identity, and cross-border connections.
- Protect high-value assets and long-lived records first (customer identity, governance artefacts, regulatory reporting).
- Upgrade customer-facing channels (web, mobile) and API gateways in line with vendor readiness.
- Update SOC monitoring, incident response, and key management procedures for hybrid/PQC environments.
- Strengthen third-party oversight: evidence of PQC support, patching, and migration timelines.

Phase 4: Full Migration and Optimisation (2028–2030)

- Complete migration of remaining systems and decommission legacy cryptographic dependencies.
- Implement continuous crypto-agility: scheduled reviews, algorithm lifecycle management, and configuration baselines.
- Prepare for audit and supervisory scrutiny: evidence, testing artefacts, and governance records.
- Embed PQC controls into architecture standards, SDLC, vendor onboarding, and resilience testing.

Success metrics boards can track quarterly

Metric	What 'good' looks like
Inventory coverage	Measured coverage across apps, infra, cloud, vendors; shrinking 'unknown crypto'
TNFL exposure mapped	Named list of critical signing workflows, PKI chains, and long-lived signed artefacts
Pilot outcomes	PQC/hybrid pilots meet performance and interoperability thresholds
Vendor readiness	Top vendors provide PQC roadmaps and test evidence; contracts include crypto-agility clauses
Cutover readiness	Approved playbooks, rollback plans, incident scenarios tested

These metrics enable boards to move from abstract awareness to measurable oversight, tracking whether quantum risk is being actively reduced rather than merely discussed. Consistent quarterly progress across inventory, TNFL mapping, pilots, vendor readiness, and cutover planning signals genuine readiness and defensible long-term trust.

Section 5 : Key Takeaways

1. The critical path is inventory + PKI/signing + vendor readiness; delays here compress every later phase.

2. Investment should be phased but committed; underfunded pilots lead to rushed deployments under regulatory pressure.

3. Boards should demand outcome-based KPIs (coverage, pilots, vendor posture, cutover readiness) rather than 'activity' reporting.

6. Governance and Board Responsibilities

PQC is a governance issue because it affects trust, systemic stability, legal enforceability, and long-term resilience. Boards should ensure PQC is integrated into enterprise risk management, operational resilience frameworks, and third-party oversight.

6.1 Board oversight requirements

- Establish a PQC steering committee (or sub-committee under Technology/Risk) with clear executive accountability.
- Integrate PQC into enterprise risk management: define risk appetite for long-lived confidentiality and signature integrity.
- Approve budget guardrails and multi-year programme funding with quarterly KPI reporting.
- Align audit committee oversight: evidence retention, auditability of migrations, and integrity of signed records.
- Mandate third-party governance: supplier PQC roadmaps, contract clauses, and independent assurance.

6.2 Key questions boards should ask

i. What is our quantum risk exposure across confidentiality (HNDL) and integrity (TNFL)?
ii. Have we completed a cryptographic asset inventory across applications, infrastructure, cloud, and vendors? What remains 'unknown'?
iii. Which of our data sets must remain confidential beyond 10 years, and how are they protected today?
iv. Which of our digitally signed artefacts must remain verifiable for decades (contracts, audit trails, regulatory submissions)?
v. What is our exposure to TNFL? Which signing workflows would be most damaging if forged in the future?
vi. What is our current PKI architecture, certificate lifecycle, and vendor dependency profile?
vii. Which critical systems (payments, identity, customer channels, FMIs) depend on vulnerable public-key cryptography?
viii. What is our target timeline for pilots, production rollout, and decommissioning of legacy algorithms?
ix. What investment is required over 2026–2030, and what is the cost of delay (operational, legal, reputational)?
x. Which vendors and third parties are on the critical path, and what evidence do we have of their PQC readiness?
xi. Do our procurement contracts mandate crypto-agility and timely patching for cryptographic changes?

xii. How are we validating performance, interoperability, and resilience impacts of PQC/hybrid deployments?
xiii. How will we ensure business continuity during cryptographic cutovers (rollback plans, incident playbooks)?
xiv. What supervisory expectations apply (domestic and cross-border), and what deadlines could become binding?
xv. How will we preserve evidentiary value of historic records signed with vulnerable algorithms (archival strategy)?
xvi. Do we have a strategy for signed logging integrity and tamper-evident audit trails in a post-quantum world?
xvii. How are we educating senior leadership and relevant staff (technology, risk, legal, procurement) on PQC?
xviii. What KPIs will we review quarterly, and what triggers escalation to the board?
xix. How are peers approaching PQC, and where do we need to match or exceed market practice?

6.3 Regulatory compliance and reporting posture

Boards should anticipate that quantum-safe planning will increasingly be evaluated through existing cyber resilience and operational risk expectations. This includes governance evidence (inventories, plans, funding), third-party assurance, and the integrity of audit trails and incident reporting processes.

Section 6 : Key Takeaways

1. Board accountability is clear: PQC is a strategic resilience programme that should be governed like other multi-year transformations.

2. The most important board questions relate to TNFL exposure, PKI/signing dependency, vendor readiness, and cutover discipline - not algorithm details.

3. Governance should integrate PQC into ERM, audit, and third-party oversight, using outcome-based KPIs reviewed quarterly.

7. Strategic Recommendations

Immediate actions (Q1–Q2 2026)

- Approve a board-sponsored PQC programme charter, including explicit ownership for TNFL (signing/PKI) and HNDL (confidentiality).
- Mandate a cryptographic inventory and classification exercise with a 90–120 day reporting milestone.
- Require top vendors and critical third parties to provide PQC and crypto-agility roadmaps; embed obligations in procurement immediately.
- Initiate pilots for hybrid TLS and signature verification in controlled environments; capture performance and interoperability evidence.
- Direct Legal/Compliance to assess evidentiary risks: how long must signatures remain defensible and how will historic signed records be validated?

Medium-term priorities (H2 2026–2027)

- Expand pilots into priority domains: PKI, signing services, code signing, secure channels for payments and critical APIs.
- Adopt crypto-agility patterns: configuration-driven cryptography, algorithm negotiation, and modular cryptographic services.
- Create an archival and validation strategy for long-lived signed records to preserve evidentiary value through transition.
- Strengthen third-party assurance: require test artefacts and independent validation where feasible.
- Develop ecosystem coordination plans with market infrastructures and payment partners to avoid fragmented migrations.

Long-term positioning (2027–2030)

- Complete migration for critical systems, decommission legacy dependencies, and embed continuous crypto lifecycle management.
- Use quantum readiness as a trust signal for cross-border counterparties and institutional clients.
- Participate in industry bodies and standards dialogues to shape interoperable, financially practical implementations.

Investment thesis and ROI framing

Boards should frame PQC investment as avoided loss and resilience: preventing long-horizon confidentiality breaches, preventing integrity crises that could trigger legal disputes, and reducing the probability of disruptive rushed migrations. Early investment also improves vendor leverage and reduces costly emergency remediation.

Section 7 : Key Takeaways

1. In 2026, the minimum viable programme is governance + inventory + vendor posture + pilots; without these, later phases become high-risk and rushed.

2. Investment should be justified as resilience ROI: avoided legal disputes (TNFL), reduced breach impact (HNDL), and lower migration disruption risk.

3. Strategic advantage comes from coordinated ecosystem migration and verifiable crypto-agility, not from isolated 'quantum-safe' product purchases.

8. Conclusion

PQC is entering the same category as other board-visible systemic risks: it is foreseeable, multi-year, and depends on disciplined preparation.

Financial services face not only the confidentiality risk of future decryption (HNDL) but also the deeper integrity risk of future forgery (TNFL). Because finance is built on authenticity, signatures, and auditable truth, the TNFL dimension elevates PQC from a technical upgrade to a trust preservation mandate.

The window for low-disruption preparation is open now. Institutions that invest early in cryptographic visibility, crypto-agility, and controlled pilots will reduce systemic risk and avoid rushed transitions. Boards should require clear ownership, quarterly metrics, and credible vendor-aligned roadmaps across 2026–2030.

Conclusion : Key Takeaways

1. The opportunity window is defined by migration lead time; delaying inventory and pilots increases the likelihood of disruptive, costly cutovers.

2. Boards have a fiduciary duty to preserve digital trust, including long-horizon authenticity of signatures and records (TNFL).

3. Next step: approve a PQC programme charter in 2026, mandate inventory, and fund pilots that prove crypto-agility and signing/PKI readiness.

Appendix A: Board Assessment Form (Self-Assessment)

Instructions: Answer Yes/No for each question. Use the scoring rubric to identify your current maturity.

Category	Question	Yes/No
Governance & Awareness	Board has designated an executive owner for PQC (including TNFL).	
Governance & Awareness	PQC is included in enterprise risk management and operational resilience planning.	
Governance & Awareness	Board has ensured quantum-aware skilling for key technical, risk, and compliance personnel.	
Governance & Awareness	Management provides quarterly PQC progress reporting with measurable KPIs.	
Governance & Awareness	Legal/Compliance has assessed signature longevity and evidentiary risk for critical records.	
Governance & Awareness	Third-party governance requires vendors to disclose cryptographic dependencies and PQC roadmaps.	
Risk Assessment	Cryptographic inventory is completed (or underway with defined deadline) across critical systems.	

Category	Question	Yes/No
Risk Assessment	Data is classified by confidentiality longevity (e.g., 5/10/20+ years).	
Risk Assessment	Signed artefacts are classified by authenticity longevity (e.g., contracts, audit evidence).	
Risk Assessment	Top quantum risk scenarios (HNDL and TNFL) are documented with business impact.	
Risk Assessment	Risk appetite and prioritisation criteria are approved for PQC migration sequencing.	
Technical Readiness	Crypto-agility principles are embedded in architecture standards (configuration-driven cryptography).	
Technical Readiness	Pilots for PQC/hybrid TLS and signatures have been executed with performance results.	
Technical Readiness	PKI and signing services have a PQC migration plan (certificates, HSMs, workflows).	

Category	Question	Yes/No
Technical Readiness	Incident response and SOC monitoring incorporate PQC/hybrid environments.	
Technical Readiness	Legacy cryptographic dependencies and hard-coded algorithms are being retired or isolated.	
Vendor & Supply Chain	Critical vendors have provided PQC readiness statements and timelines.	
Vendor & Supply Chain	Contracts include crypto-agility and timely cryptographic upgrade obligations.	
Vendor & Supply Chain	Supply chain security includes code signing integrity reviews and PQC roadmap for signing.	
Vendor & Supply Chain	Cloud providers' PQC capabilities and constraints are assessed and documented.	
Vendor & Supply Chain	Third-party audits/assurance address cryptographic posture and migration readiness.	

Category	Question	Yes/No
Regulatory Compliance	Regulatory mapping is complete (RBI/SEBI/CERT-In + cross-border supervisors where relevant).	
Regulatory Compliance	Audit evidence retention strategy exists for cryptographic migrations and signed records.	
Regulatory Compliance	Compliance reporting includes PQC milestones where supervisors expect forward-looking resilience.	
Regulatory Compliance	Cyber incident reporting and logging integrity controls are reviewed for long-horizon trust.	
Regulatory Compliance	Board has reviewed potential 2026+ mandates and contingency plans for accelerated timelines.	

Scoring: Count total Yes answers (0–25)

20–25: Advanced - maintain momentum; validate vendors; accelerate PKI/signing transformation and continuous crypto-agility.

15–19: Progressing - close inventory and TNFL mapping gaps; expand pilots into critical systems; strengthen procurement clauses.

10–14: Developing - establish governance, fund programme, start inventory, and run first pilots within 6 months.

0–9: Needs Immediate Action - treat as priority risk; initiate inventory and board oversight immediately; engage independent support if required.

Appendix B: Glossary of Terms

Term	Definition
Post-Quantum Cryptography (PQC)	Cryptographic algorithms designed to remain secure against both classical and future quantum computers, replacing vulnerable public-key methods.
Quantum Computing	A computing approach that uses quantum-mechanical properties to solve certain problems much faster than classical computers.
Cryptographically Relevant Quantum Computer (CRQC)	A quantum computer powerful enough to break widely used public-key cryptography (e.g., RSA, ECC) within practical time.
Q-Day	A shorthand term for the point in time when quantum computers can break currently deployed public-key cryptography at scale.
Harvest Now, Decrypt Later (HNDL)	An adversary strategy of collecting encrypted data today and decrypting it later when quantum capability becomes sufficient.
Trust Now, Forge Later (TNFL)	An integrity threat where adversaries collect digitally signed artefacts today to forge signatures later, undermining authenticity and non-repudiation.

ML-KEM	A NIST standardised post-quantum key establishment (key-encapsulation) mechanism (FIPS 203).
ML-DSA	A NIST standardised post-quantum digital signature algorithm (FIPS 204).
SLH-DSA	A NIST standardised stateless hash-based digital signature algorithm (FIPS 205).
Crypto-agility	The ability of systems to change cryptographic algorithms and parameters with minimal disruption, enabling safe upgrades over time.
Hybrid Cryptography	A transition approach combining classical and post-quantum algorithms to reduce migration risk and maintain interoperability.
Public Key Infrastructure (PKI)	The certificates, keys, policies, and services that support digital identity, encryption, and signatures at scale.
Digital Signature	A cryptographic mechanism that proves who signed a digital artefact and that it was not altered after signing.
Integrity	Assurance that data has not been altered in an unauthorised way.

Authenticity	Assurance that a message, document, or transaction genuinely comes from the claimed source.
Non-repudiation	A property that prevents a party from credibly denying a signature or transaction they executed.
TLS	Transport Layer Security; the protocol commonly used to secure web and API communications.
HSM	Hardware Security Module; dedicated hardware used to generate, store, and use cryptographic keys securely.
Certificate	A digital credential that binds a public key to an identity, used widely in PKI and secure communications.
Code Signing	Use of digital signatures to assure software/firmware updates are authentic and untampered.
Key Exchange / Key Establishment	Methods used by communicating systems to create shared secret keys used for encryption.
Quantum Key Distribution (QKD)	A quantum-communications technique for distributing symmetric keys; often

	expensive and operationally complex compared with software-based PQC.
CNSA 2.0	NSA's Commercial National Security Algorithm Suite 2.0, a roadmap for adopting quantum-resistant cryptography for national security systems.
NIST	U.S. National Institute of Standards and Technology; publishes cryptographic standards including PQC standards.
ENISA	European Union Agency for Cybersecurity; publishes studies and guidance including on PQC standardisation and migration.
Operational Resilience	Ability to prevent, respond to, recover from, and adapt to operational disruptions, including cyber incidents.
Third-Party Risk	Risk arising from vendors and service providers, including embedded cryptographic dependencies and readiness.
Audit Trail	Records that provide evidence of actions and transactions; integrity is critical for compliance and dispute resolution.
Tokenisation	Replacing sensitive data with non-sensitive tokens; cryptography often

	protects token generation and mapping systems.
Forward Secrecy	A property where session keys are not compromised even if long-term keys are later exposed; relevant to limiting HNDL impact in some contexts.
Data-at-Rest / Data-in-Transit	Data stored on systems versus data moving across networks; both rely on cryptography in different ways.
Algorithm Lifecycle Management	Governed process for selecting, deploying, monitoring, and retiring cryptographic algorithms over time.

Appendix C: Sources and References (selected, organised by section)

Note: URLs are provided for board reference and traceability.

Core standards and government mandates

- NIST, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), Aug 2024. https://csrc.nist.gov/pubs/fips/203/final

- NIST, Post-Quantum Cryptography Project (program overview). https://csrc.nist.gov/projects/post-quantum-cryptography

- U.S. Office of Management and Budget, M-23-02: Migrating to Post-Quantum Cryptography, Nov 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

- NSA, Commercial National Security Algorithm (CNSA) Suite 2.0 (Algorithms and timelines), Sep 2022 (ver. 1.0). https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

Section 1 - Threat landscape (HNDL/TNFL, timelines)

- UK National Cyber Security Centre (NCSC), Timelines for migration to post-quantum cryptography (guidance page). https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

- ENISA, Post-Quantum Cryptography: Current state and quantum mitigation (report PDF). https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf

- Deloitte, Tech Trends 2025 - Quantum computing and cybersecurity (Dec 2024). https://www.deloitte.com/us/en/insights/focus/tech-trends/2025/tech-trends-quantum-computing-and-cybersecurity.html

- McKinsey, When and how to prepare for post-quantum cryptography (May 2022). https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

Section 2 - Global regulatory and standards landscape

- ENISA, Post-Quantum Cryptography: Current state and quantum mitigation (study page). https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

- Australian Signals Directorate, *Information Security Manual (ISM)* — Post-quantum cryptography transition guidance (planning by 2026, migration from 2028, legacy cryptography phased out by 2030).

- MAS, Advisory on addressing the cybersecurity risks associated with quantum (Feb 2024). https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf

- FSB, Cyber resilience work programme overview. https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/

- Deloitte, Quantum computing in financial services (Jul 2023). https://www.deloitte.com/us/en/insights/industry/financial-services/quantum-computing-in-finance.html

- FS-ISAC, PQC Working Group - Current State (Crypto Agility) (2023). https://www.fsisac.com/hubfs/Knowledge/PQC/CurrentState.pdf

Section 3 - India context and frameworks

- Press Information Bureau (PIB), Cabinet approves National Quantum Mission, Apr 2023. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888

- Department of Science & Technology (DST), National Quantum Mission overview. https://dst.gov.in/national-quantum-mission-nqm

- RBI, Cyber Security Framework in Banks (Jun 2016). https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx?Id=1721

- SEBI, Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (Aug 2024). https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

- CERT-In, Directions under Section 70B (Apr 2022). https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

Section 4-5 - Risk assessment and migration

- CISA, Strategy for migrating to automated PQC discovery and inventory tools (Sep 2024). https://www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf

- PwC, Securing data in the post-quantum age (Feb 2025). https://www.pwc.com/m1/en/publications/securing-data-in-the-post-quantum-age.html

- ISO/IEC JTC 1/SC 27 Journal (mentions SC27 preparation for PQC standardisation) (Mar 2022). https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/ISO-IECJTC1-SC27_N22216_SC27_Journal_Vol_1_Issue_3.pdf

Appendix D: About Kquanta Research LLP

Kquanta Research LLP is a pioneering research and advisory firm positioned at the convergence of finance, deep technology, and sustainability. We help organizations navigate the transformative era where advanced technologies like quantum computing and artificial intelligence intersect with responsible finance and environmental stewardship. Through our flagship platform, Quantum Tech in Finance (QTIF), we convene leaders from industry, academia, and policy to foster innovation and collaboration that shapes the future of finance. Our work translates complex research in quantum computing and AI into practical insights, learning programs, and collaborative innovations that enable institutions to make smarter, future-ready, and sustainable decisions.

Our comprehensive offerings address the critical needs of modern financial institutions through integrated solutions:

- **Strategic Innovation & Learning**: We convert cutting-edge quantum and AI research into actionable strategies for portfolio optimization, risk management, and ESG integration, while delivering executive education programs, workshops, and certifications that prepare leaders for the quantum and AI era through partnerships with academic institutions and corporate academies.
- **Intelligence & Collaboration**: Our research spans financial market analysis of digital assets and capital markets, technological disruption from AI and quantum innovations, sustainability and ESG trends, and global policy and regulatory developments. We collaborate with industry partners on pilot projects and applied research to develop practical solutions for real-world challenges, combining the latest scientific research with a focus on measurable outcomes.

Kquanta Research LLP

Mumbai Office: One World Centre,

Lower Parel, Mumbai 400013 MH India.

conctact@kquantaresearch.com

www.kquantaresearch.com

NOTES

KQUANTA RESEARCH