



The Executive Guide to Post-Quantum Migration

A strategic handbook for CIOs, CISOs, CTOs, Boards Members, and Cybersecurity Architects navigating the transition to quantum-resilient cryptography.

 EXECUTIVE HANDBOOK

 CRYPTOGRAPHIC RESILIENCE

 BOARD-READY

EXECUTIVE SUMMARY

The Quantum Threat Is Not a Future Problem – It Is a Present Risk

Quantum computing is advancing faster than most enterprise security roadmaps anticipate. The cryptographic standards that protect financial transactions, healthcare records, intellectual property, and critical infrastructure today – RSA, ECC, and Diffie-Hellman – will be rendered obsolete by sufficiently powerful quantum computers. The question is not whether, but when.

NIST has already finalised its first post-quantum cryptographic (PQC) standards (FIPS 203, 204, 205), signalling that the migration window has officially opened. Organisations that delay will face compounding risk: adversaries are actively harvesting encrypted data today, with the intent to decrypt it once quantum capability matures – a strategy known as "Harvest Now, Decrypt Later".

The Core Challenge

Most enterprises have no complete inventory of where cryptography is deployed across their systems, vendors, or supply chains.

The Strategic Imperative

Migration to post-quantum algorithms must begin now – not because quantum computers are here, but because migration itself takes years.

The Leadership Mandate

This is an enterprise risk issue, not solely a security team issue. Board-level awareness and executive sponsorship are prerequisites for success.

📌 Executive Takeaway: Organisations that begin PQC migration planning today will be 3–5 years ahead of those that wait for quantum computers to arrive.

WHY IT MATTERS

Why Post-Quantum Cryptography Matters to Your Business

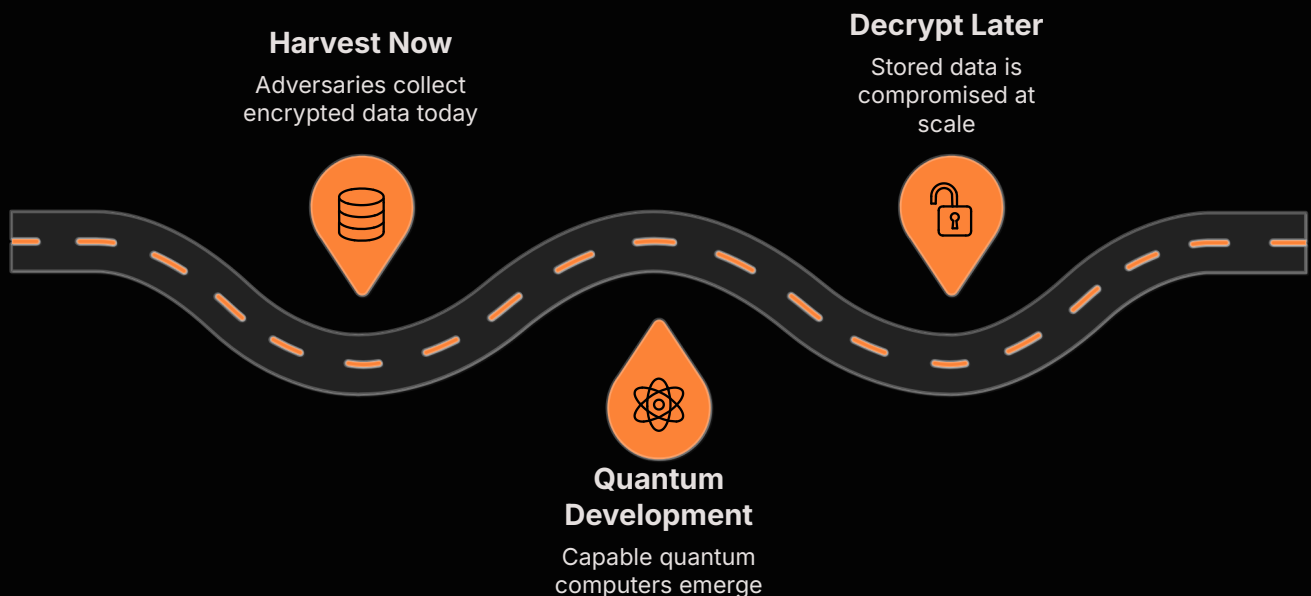
The transition to post-quantum cryptography is not a technology refresh – it is a strategic business continuity decision. Every sector that relies on encrypted communications, long-lived data, or regulated data protection is exposed. The risk is asymmetric: the cost of early action is manageable; the cost of late action could be catastrophic.

Industries at Highest Risk

- BFSI
- Healthcare and Pharmaceutical Industries
- Defence and government
- Critical infrastructure
- Telecommunications and cloud providers
- Data Centres & Automotives

Business Risks That Demand Board Attention

- **Data confidentiality:** Harvested data becomes readable when quantum arrives
- **Regulatory exposure:** NIST, ENISA, and national standards bodies are mandating PQC timelines
- **Vendor dependencies:** Third-party and supply chain cryptography is largely invisible
- **Competitive liability:** Peers and competitors are beginning migration now



This timeline illustrates why "Harvest Now, Decrypt Later" attacks are already underway – data encrypted today with classical algorithms is being stockpiled for future decryption.

CRYPTOGRAPHIC VISIBILITY

You Can't Migrate What You Can't See

The most underestimated challenge in post-quantum migration is not algorithm selection – it is cryptographic discovery. Before any migration can begin, organisations must answer a deceptively difficult question: **Where is cryptography used across your enterprise?**

The answer is almost always everywhere and invisibly. Cryptography is embedded in TLS certificates, code-signing pipelines, SSH access, API authentication, database encryption, IoT firmware, legacy middleware, and hundreds of third-party integrations. Most enterprises have no centralised visibility into this cryptographic estate.



Network & Infrastructure

TLS/SSL certificates, VPN tunnels, firewall authentication, and network-layer encryption are typically untracked at the certificate level.



Applications & APIs

Custom applications, SaaS integrations, and API gateways embed cryptographic calls that are invisible to standard asset inventories.



Data & Storage

Encrypted databases, backup systems, and data lakes rely on algorithms that may span multiple generations of cryptographic standards.



Supply Chain & Third Parties

Vendor software, outsourced platforms, and cloud services introduce cryptographic dependencies that your organisation cannot directly control.

- ❏ **Executive Takeaway:** A Cryptographic Bill of Materials (CBOM) – a complete inventory of all cryptographic assets – is the foundational deliverable of PQC migration. Without it, no migration programme can succeed.

DECISION FRAMEWORK

The Executive Decision Framework for PQC Migration

Post-quantum migration requires a structured governance approach that bridges technical execution with business risk management. The following four-pillar framework provides executives with a decision-making model that aligns security investment with enterprise priorities.



Discover

Map all cryptographic assets, algorithms, and dependencies across systems, applications, and supply chains.



Prioritise

Rank assets by sensitivity, longevity of data, regulatory obligation, and exposure to Harvest Now attacks.



Migrate

Execute phased algorithm replacement, beginning with highest-risk systems, adopting NIST-approved PQC standards.



Validate

Verify migration completeness, test interoperability, and maintain crypto-agility for future algorithm transitions.

What Leadership Must Decide

- Which business systems carry the highest long-term data risk?
- What is the acceptable timeline for full migration?
- How will third-party vendor compliance be enforced?
- What budget and resourcing does this programme require?

Governance Requirements

- Executive sponsor at C-suite or board level
- Cross-functional steering committee (security, IT, legal, procurement)
- PQC migration included in enterprise risk register
- Annual reporting cadence to the board

LEADERSHIP QUESTIONS

Five Questions Every CIO Should Ask – Starting This Quarter

Leadership accountability for post-quantum migration begins with informed questioning. The following five questions are designed to surface gaps in organisational readiness, drive accountability, and initiate structured action. Bring these to your next CISO briefing or board risk review.

1

Do you have a complete inventory of our cryptographic assets?

If the answer is "no" or "partially", your first investment should be in cryptographic discovery tooling and a CBOM programme before any migration work begins.

2

Which of your data assets have a sensitivity lifespan beyond 5–10 years?

Long-lived data – intellectual property, health records, financial history – is the primary target of Harvest Now, Decrypt Later attacks. This data must be prioritised immediately.

3

Are your key vendors and suppliers PQC-ready?

Your migration is only as strong as your weakest vendor link. Procurement and vendor management must now include PQC readiness as a standard contractual criterion.

4

Does your security architecture support crypto-agility?

Crypto-agility – the ability to swap cryptographic algorithms without re-engineering entire systems – is a strategic capability that reduces the cost of all future transitions.

5

Is PQC migration funded and resourced in our current planning cycle?

If PQC migration does not appear in the budget, it will not happen on the timeline regulators, peers, and risk models demand. Executive sponsorship must translate to resource allocation.



Executive Takeaway: These five questions are a board-ready diagnostic. If your team cannot answer all five with confidence, you have a visibility and governance gap that must be closed before technical migration begins.

90-DAY ROADMAP

Your First 90-Day PQC Migration Roadmap

Post-quantum migration is a multi-year programme, but executive momentum must begin immediately. The first 90 days are about establishing visibility, governance, and a credible migration plan – not about replacing algorithms. The following roadmap is structured for executive accountability and board-level transparency.

Days 1–30: Assess & Align

- Appoint PQC executive sponsor
- Commission cryptographic asset discovery
- Benchmark against NIST PQC standards
- Brief board on risk exposure

Days 61–90: Pilot & Commit

- Launch pilot migration on one priority system
- Publish PQC migration roadmap internally
- Establish crypto-agility design standard
- Set 12-month milestones and KPIs



Days 31–60: Prioritise & Plan

- Identify top 10 highest-risk cryptographic systems
- Draft initial CBOM (Crypto Bill of Materials)
- Engage key vendors on PQC readiness
- Assign budget and cross-functional team

Key Deliverable: Day 30

Executive-sponsored PQC programme charter approved and risk briefing delivered to the board.

Key Deliverable: Day 60

Initial cryptographic asset inventory complete; top-risk systems identified and prioritised.

Key Deliverable: Day 90

Migration pilot underway; 12-month roadmap published with measurable milestones.

READINESS ASSESSMENT

Executive Readiness Scorecard

Use this scorecard to assess your organisation's current post-quantum readiness. Rate each dimension honestly - this is a diagnostic tool, not a compliance checklist. Share results with your CISO and use them to prioritise your first 90-day actions.

Readiness Dimension	Not Started	In Progress	Complete
Cryptographic asset inventory (CBOM)	No visibility	Partial discovery	Full enterprise CBOM
Risk-based prioritisation of data assets	Not assessed	Key systems identified	Ranked and documented
PQC governance and executive sponsor	No owner	CISO-led only	Board-sponsored programme
Vendor and supply chain PQC assessment	Not started	Top vendors assessed	All contracts updated
Crypto-agility in architecture standards	No standard	Pilot systems only	Enterprise-wide standard
NIST PQC algorithm adoption	Not planned	Pilot underway	Deployed in production
Budget allocated for PQC migration	No funding	Partial allocation	Fully funded programme

❏ Scoring Guide: Majority "Not Started" = High urgency - begin the 90-day roadmap immediately. Majority "In Progress" = Moderate urgency – accelerate governance and vendor engagement. Majority "Complete" = mature posture – focus on validation, supply chain, and crypto-agility standards.

KEY TAKEAWAYS

Seven Things Every Executive Must Understand About PQC Migration

1 The threat is present, not future

Harvest Now, Decrypt Later attacks are active today. Data encrypted with classical algorithms is being collected for future quantum-enabled decryption. Waiting is not a neutral choice.

2 NIST standards are final – the migration clock has started

NIST finalised its first PQC standards in 2024. Regulatory and compliance timelines will follow. Organisations that treat this as future-state planning are already behind.

3 Migration takes years, not months

Enterprise cryptographic migration is a multi-year programme. Legacy systems, vendor dependencies, and supply chain complexity make this a sustained transformation, not a patch cycle.

4 Visibility is the first milestone

Without a comprehensive cryptographic bill of materials, no migration programme can succeed. Discovery must precede all technical execution.

5 This is a business continuity issue, not a security team task

PQC migration requires executive sponsorship, cross-functional governance, board-level awareness, and sustained budget commitment. Security teams alone cannot drive this transformation.

6 Crypto-agility is a strategic capability

Organisations that build crypto-agility into their architecture today will manage all future cryptographic transitions – not just PQC – at significantly lower cost and risk.

7 Supply chain risk is cryptographic risk

Your organisation's quantum resilience is bounded by the weakest cryptographic link in your vendor and partner ecosystem. Vendor PQC readiness must become a procurement standard.

LEADERSHIP CALL TO ACTION

Leadership Message and Next Steps

Post-quantum cryptography migration is the most significant cryptographic transition since the advent of public-key encryption. It is a generational challenge that will separate organisations that act with strategic foresight from those that respond reactively to a crisis.

The organisations most at risk are not those without quantum computers - they are the ones without a migration plan. The window to act before quantum capability matures is open now. It will not remain open indefinitely.

For the CIO

Commission a cryptographic asset discovery programme this quarter. Make CBOM a standard deliverable of your enterprise architecture function.

For the CISO

Elevate PQC to your enterprise risk register. Brief the board with a quantified risk exposure and a funded mitigation roadmap.

For the CTO

Mandate crypto-agility as an architecture standard for all new systems and major upgrades. Build PQC readiness into your technology selection criteria.

For the Board

Request a PQC readiness briefing at the next risk committee. Ensure the organisation has executive sponsorship, a funded programme, and a credible 3-year migration plan.

Immediate Actions - This Quarter

- Appoint a PQC executive programme sponsor
- Initiate cryptographic discovery and CBOM development
- Add PQC migration to the enterprise risk register
- Brief the board on Harvest Now, Decrypt Later risk
- Engage top-tier vendors on PQC readiness commitments

Reference Standards and Frameworks

- **NIST FIPS 203, 204, 205** – Finalised PQC algorithm standards
- **NIST SP 1800-38** – Migration to PQC guidance
- **ENISA PQC Guidelines** – European regulatory alignment
- **NSA CNSA 2.0** – US national security algorithm suite
- **ISO/IEC 18033** – Encryption standards framework

📌 **Final Takeaway:** The organisations that will emerge from the quantum transition with a competitive advantage are those that begin now – with visibility, governance, and executive commitment. The first 90 days are yours to define.