EXECUTIVE ADVISORY

Q→NU

Preparing BFSI for the Post-Quantum Era

An Executive Guide for CIOs, CISOs & Cybersecurity Leaders in Banking, Financial Services & Insurance

---

Co-Presented By

BLUE STAR | DATA SECURITY

Blue Star Engineering & Electronics Ltd.
Technology Partner

This document is an executive advisory brief. It is not a product catalogue or marketing material. It is designed to inform strategic decision-making at the intersection of quantum computing, cryptographic risk, and enterprise resilience in BFSI.

Q→NU

EXECUTIVE SUMMARY

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

> The organisations that will navigate the post-quantum transition successfully are those that begin building cryptographic visibility and governance today - not when quantum computers arrive.

Quantum computing is advancing faster than most enterprise risk models anticipated. While large-scale, fault-tolerant quantum computers capable of breaking today's encryption are not yet commercially available, the conditions for strategic exposure already exist. Adversaries are actively harvesting encrypted data today, storing it for decryption once quantum capabilities mature – a strategy known as **Harvest Now, Decrypt Later (HNDL)**.

For BFSI institutions, the exposure window is particularly acute. Financial data, customer records, regulatory filings, and interbank communications carry long-term sensitivity - often exceeding the anticipated timelines for quantum maturity. The intersection of long data retention requirements and long-lived cryptographic keys creates a structural vulnerability that demands executive attention now.

Why It Matters Now

Encrypted data captured today can be decrypted by quantum computers within 5-10 years.

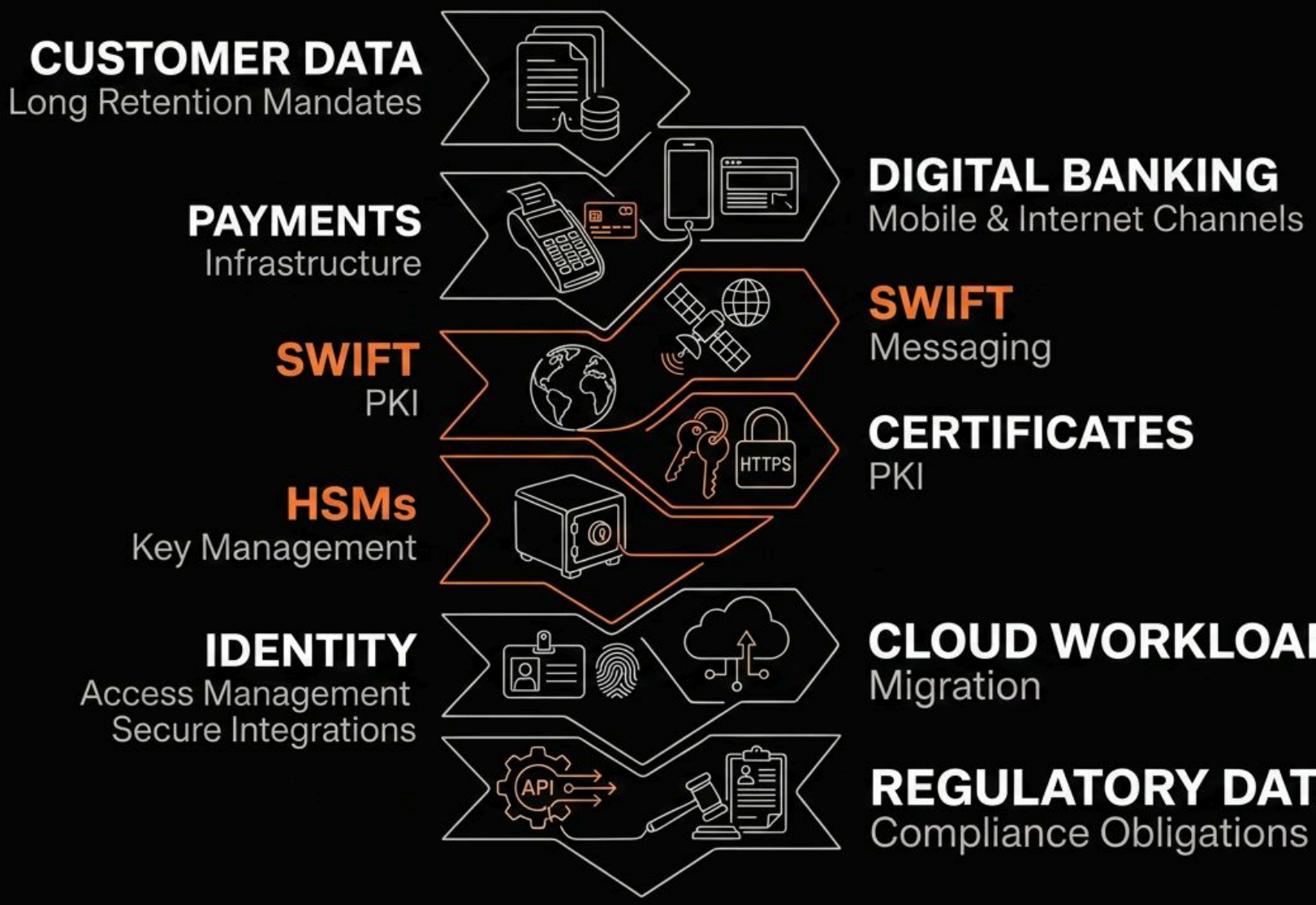
Visibility First

You cannot migrate what you cannot see. Cryptographic discovery precedes all strategic planning.

Q→NU

Why BFSI Is Uniquely Exposed

Financial institutions are among the most cryptographically dense organisations in any sector. Every transaction, customer identity, regulatory submission, and inter-bank message relies on cryptographic primitives - many of which are vulnerable to quantum attack. The combination of long data retention mandates, high operational complexity, and systemic regulatory expectations places BFSI in a structurally distinct risk category.



Long Data Retention

Regulatory mandates require BFSI firms to retain sensitive data for 7-15+ years – well within the quantum decryption horizon.

High Cryptographic Density

Thousands of certificates, keys, and cryptographic protocols operate simultaneously across legacy and modern infrastructure.

Regulatory Expectations

RBI, SEBI, IRDAI, and global standards bodies are increasingly signalling quantum readiness as a governance obligation.

THREAT MODEL

Understanding the Quantum Threat Horizon

The threat from quantum computing to cryptographic security is not a binary event - it is a progressive exposure that has already begun. The most immediate and underappreciated risk is the Harvest Now, Decrypt Later (HNDL) strategy, which requires no quantum capability today but delivers adversarial advantage in the future.

The strategic implication is clear: the window for action is not defined by when quantum computers arrive - it is defined by the sensitivity lifetime of the data encrypted today. For BFSI institutions holding long-lived customer and regulatory data, the exposure has already begun.

Business Implication

Customer PII, transaction histories, and regulatory records encrypted under RSA-2048 or ECC today may be readable by adversaries within a decade. The cost of inaction compounds annually.

⚠ Data encrypted today under classical algorithms may offer zero confidentiality by 2030-2035 against a quantum-capable adversary.

ENTERPRISE ARCHITECTURE

Where Cryptography Lives Across a Modern Bank

Before an institution can plan a migration to post-quantum cryptography, it must first understand the full breadth of its cryptographic estate. In a modern BFSI enterprise, cryptography is not confined to one system – it is embedded across every operational layer, from customer-facing applications to back-office infrastructure and third-party integrations.

Cryptographic visibility is the prerequisite for all migration planning. Organisations that lack an accurate inventory of where cryptography operates cannot safely plan, sequence, or execute a post-quantum transition without introducing significant operational risk.

Q→NU

EXECUTIVE GOVERNANCE

Four Questions Every CIO and CISO Must Answer

Quantum readiness is fundamentally a governance challenge before it is a technical one. Executive leaders should be able to answer these four foundational questions with confidence. Organisations that cannot answer them today face material gaps in their cryptographic risk posture.

1

Cryptographic Inventory

Do we know where cryptography exists across our entire enterprise - applications, infrastructure, APIs, cloud, and third-party integrations?

2

Algorithmic Dependency

Which critical business systems - payments, identity, SWIFT, core banking - depend on algorithms that are vulnerable to quantum attack?

3

Migration Feasibility

Can we migrate cryptographic algorithms and key infrastructure without disrupting live operations, SLAs, or regulatory obligations?

4

Standards Readiness

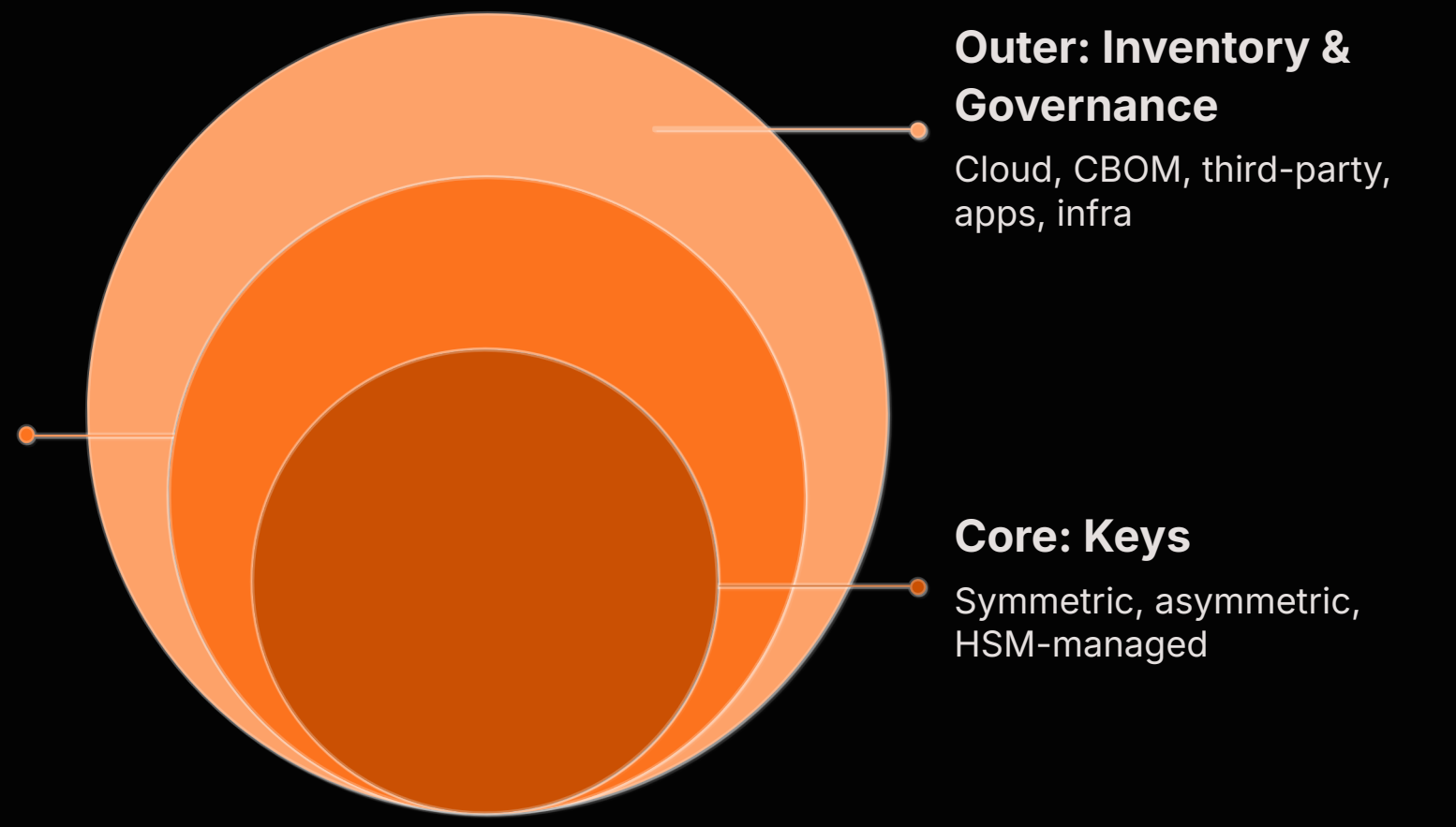
How prepared are we to adopt evolving NIST PQC standards, RBI circulars, and international regulatory guidance as they are published?

> Organisations that can answer all four questions with documented evidence are demonstrably ahead of the curve. Most cannot - and that gap is itself a governance risk.

STRATEGIC FOUNDATION

Visibility Before Migration

A recurring failure pattern in cryptographic modernisation programmes is attempting to plan migration before achieving visibility. The result is incomplete inventories, unplanned disruptions, and rework that compounds cost and timeline. Cryptographic visibility - knowing precisely what algorithms, keys, and certificates exist, where they are, and what systems depend on them - is the non-negotiable foundation of every successful post-quantum programme.



What is a CBOM?

A **Cryptographic Bill of Materials (CBOM)** is a structured, machine-readable inventory of all cryptographic assets in an organisation's environment - including algorithms, key lengths, certificate expiry, dependencies, and risk classification. It is the cryptographic equivalent of an asset register and is the starting point for all quantum readiness planning.

Why It Matters

Without a CBOM, organisations cannot prioritise which systems to migrate first, cannot assess the blast radius of a cryptographic failure, and cannot demonstrate governance readiness to regulators or auditors. The CBOM transforms cryptographic risk from invisible to manageable.

Q→NU

The Hidden Risk in Your Software Supply Chain

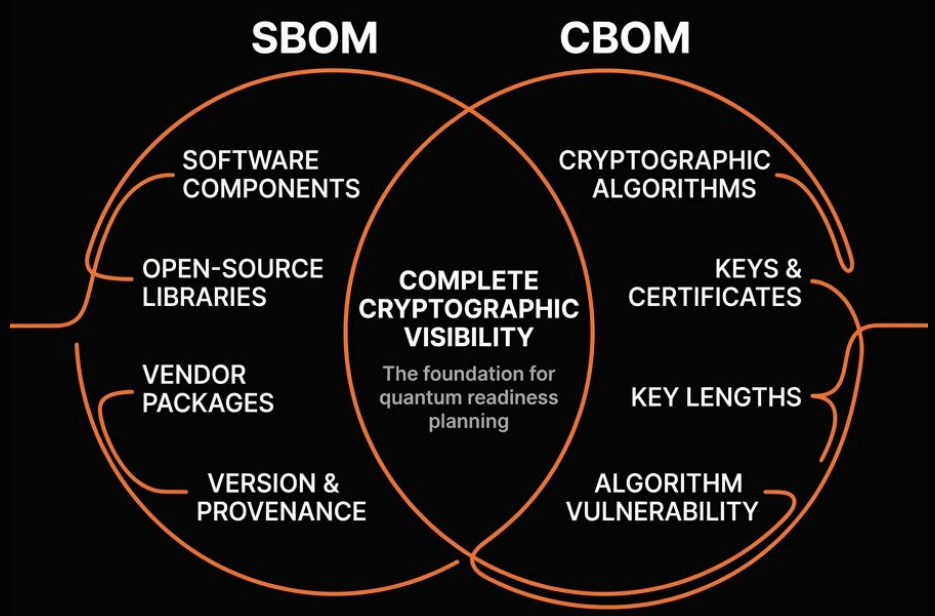
Most BFSI institutions focus cryptographic risk assessments on internally developed systems. However, a significant and frequently underestimated exposure lies within third-party software, open-source libraries, and vendor-supplied components that are embedded throughout the enterprise. These dependencies carry their own cryptographic implementations - often invisible to the enterprise security team.

SBOM - Software Bill of Materials

A structured inventory of all software components - including open-source libraries, commercial packages, and vendor-supplied code - that identifies version, provenance, and known vulnerabilities within an application or system.

CBOM - Cryptographic Bill of Materials

An extension of the SBOM that specifically catalogues every cryptographic primitive, algorithm, key, and certificate used within software components - including those embedded in third-party code invisible to conventional scanning.



Combined Visibility

The intersection of SBOM and CBOM provides complete cryptographic visibility - the only foundation from which a credible quantum readiness programme can be built.

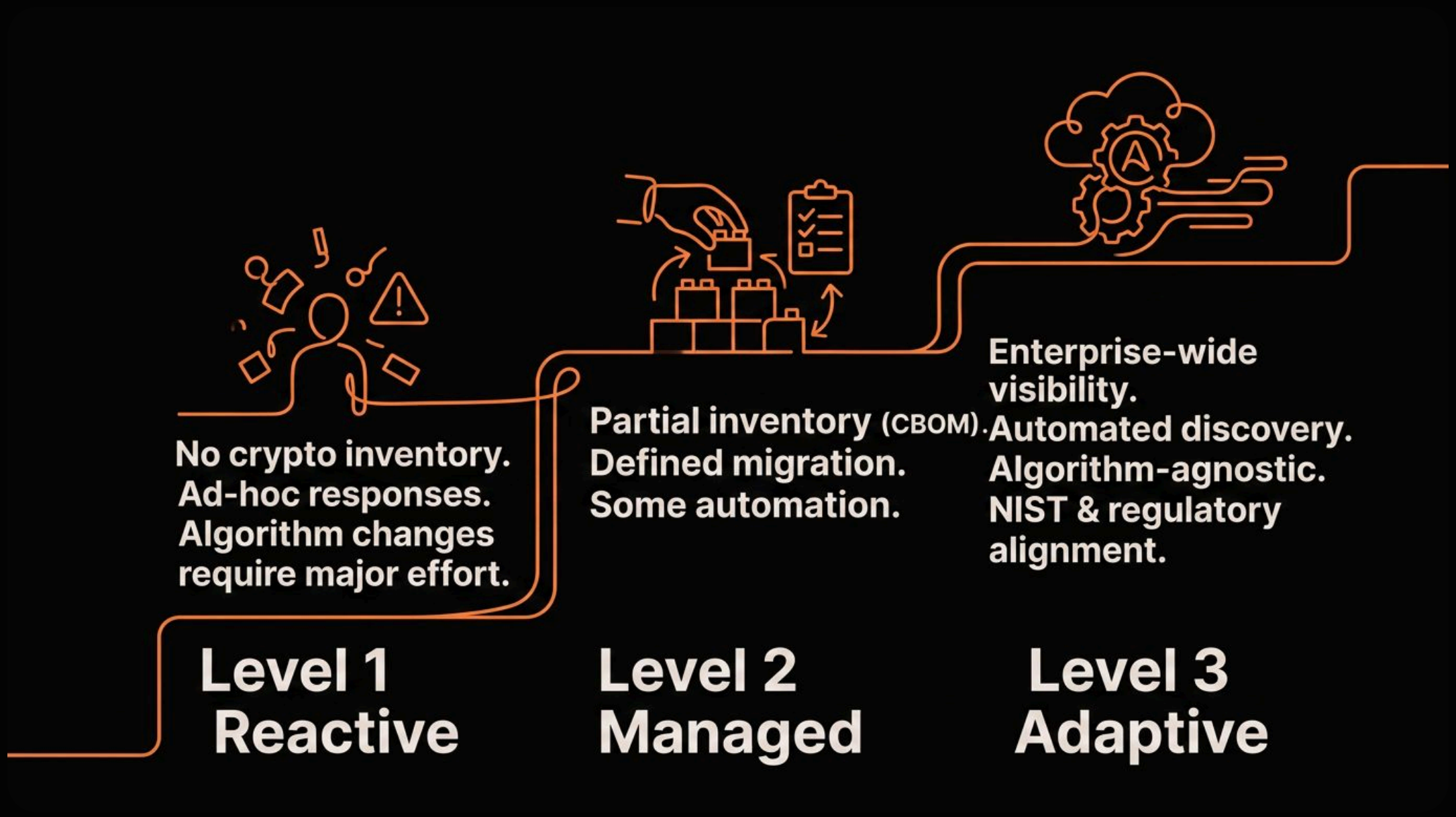
Third-party and open-source software often contains cryptographic libraries that are not visible through standard vulnerability scanning. SBOM combined with CBOM is the only method that provides complete supply chain cryptographic coverage.

STRATEGIC CAPABILITY

Crypto Agility: Beyond a One-Time Migration

A common misconception in post-quantum planning is that the goal is a single migration event – replacing RSA and ECC with NIST-approved post-quantum algorithms and declaring the work complete. In reality, the cryptographic landscape will continue to evolve. New standards will be published, new vulnerabilities discovered, and new regulatory requirements introduced. Organisations that treat migration as a destination rather than a capability will find themselves in perpetual reactive mode.

Crypto agility is the organisational and architectural capability to discover, assess, and replace cryptographic algorithms rapidly – without requiring bespoke engineering effort for each change. It is a strategic capability, not a product feature.

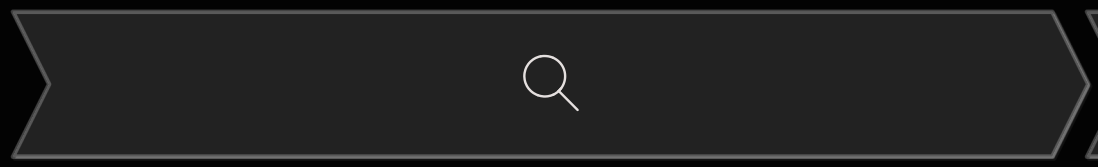


Crypto Agility is not a technology outcome - it is an enterprise governance capability. Organisations at Level 3 can respond to new cryptographic standards within weeks, not years.

Q→NU

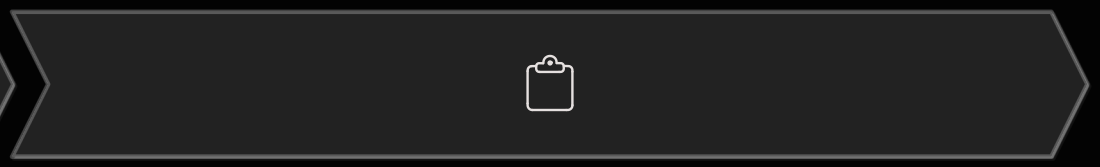
A Practical Quantum Readiness Roadmap

Quantum readiness is best approached as a phased programme rather than a project. Each phase builds on the previous, and each delivers standalone value independent of the full journey. This structure allows institutions to demonstrate governance progress to regulators and boards at each milestone, whilst managing operational risk throughout the transition.



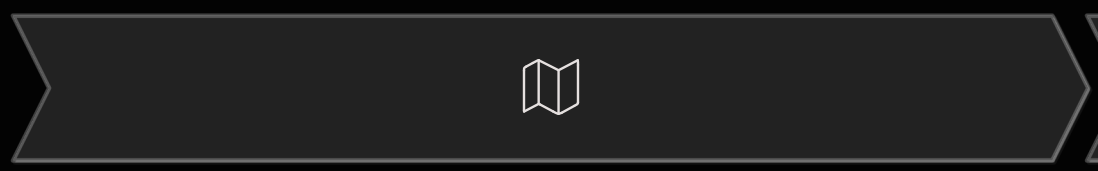
Phase 1 - Discover

Deploy CBOM and SBOM scanning across enterprise applications, infrastructure, and third-party components. Establish cryptographic asset inventory. Identify all algorithms, key lengths, and certificates in use.



Phase 2 - Assess

Classify cryptographic assets by quantum vulnerability and business criticality. Map algorithmic dependencies to business systems. Quantify migration complexity and operational risk per system.



Phase 3 - Plan

Develop a sequenced migration strategy prioritised by risk exposure and operational impact. Define target-state cryptographic architecture. Align with NIST PQC standards and regulatory guidance.

Phase 4 - Execute

Implement post-quantum algorithms in the highest-risk systems first. Validate interoperability across vendor and partner ecosystems. Establish continuous monitoring and crypto agility governance.

Milestone 1

Complete enterprise CBOM with risk classification

Milestone 2

Quantum Risk Assessment Report delivered to board

Milestone 3

PQC migration roadmap approved and resourced

Milestone 4

First production systems migrated; crypto agility framework operational

Q→NU

EXECUTIVE TAKEAWAYS

Five Strategic Imperatives for BFSI Leadership

> The post-quantum transition is not a technology upgrade - it is a strategic programme that requires board-level governance, multi-year planning, and enterprise-wide coordination.

1 Understand Your Cryptographic Landscape

Commission a structured cryptographic discovery exercise to establish a baseline inventory of all algorithms, keys, certificates, and dependencies operating across your enterprise. Without this baseline, all subsequent planning is speculative.

2 Build Cryptographic Visibility Through CBOM

Establish a Cryptographic Bill of Materials as a living, maintained asset. Make it the central input to your security governance, risk reporting, and technology architecture review processes.

3 Assess Software Supply Chain Cryptographic Dependencies

Extend visibility beyond internal systems to encompass third-party software, open-source libraries, and vendor components. The SBOM-CBOM intersection reveals hidden cryptographic risk that conventional assessments miss entirely.

4 Develop a Phased, Risk-Prioritised Migration Strategy

Define a sequenced roadmap that prioritises migration of the most sensitive and highest-risk systems first. Align the roadmap with regulatory expectations and internal change management capacity.

5 Build Long-Term Crypto Agility as an Organisational Capability

Architect systems and governance processes to support ongoing cryptographic adaptability. The organisations that invest in crypto agility today will navigate future standard changes with minimal disruption and maximum regulatory confidence.

NEXT STEPS

Begin Your Quantum Readiness Journey

The most effective action an institution can take today is to initiate a structured, evidence-based assessment of its cryptographic estate. The following engagement pathway is designed to deliver actionable intelligence within a defined timeframe, without disrupting ongoing operations or requiring large upfront commitments.

📱 Schedule an Executive Briefing

Request a private, confidential briefing session with the Blue Star and QNu Labs advisory team. No commitment required. Tailored to your organisation's specific context and risk profile.

📋 Request a CBOM Assessment

Initiate an automated cryptographic discovery exercise across a defined scope of your enterprise. Receive a structured risk report within a defined engagement timeline.

Blue Star Engineering & Electronics Ltd. | Technology Partner for Quantum-Safe BFSI
QNu Labs | Post-Quantum Cybersecurity | www.qnulabs.com

Q→NU

Glossary of Key Terms

This glossary provides precise, executive-level definitions of the key technical concepts referenced throughout this document. These definitions are aligned with NIST, ISO, and industry-standard usage.

1	**CBOM - Cryptographic Bill of Materials** A structured, machine-readable inventory of all cryptographic assets within an organisation's environment, including algorithms, key types, certificate authorities, key lengths, and system dependencies. The CBOM is the primary tool for cryptographic risk governance and quantum readiness planning.
2	**SBOM - Software Bill of Materials** A formal, structured record of all software components - including open-source libraries, commercial packages, and vendor-supplied code - used within an application or system. The SBOM enables supply chain risk management and, when combined with CBOM, provides complete cryptographic visibility.
3	**PQC - Post-Quantum Cryptography** A class of cryptographic algorithms designed to be secure against both classical and quantum computing attacks. NIST finalised the first set of PQC standards in 2024, including CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures). PQC algorithms run on classical hardware and require no quantum infrastructure.
4	**Crypto Agility** The organisational and architectural capability to discover, assess, and replace cryptographic algorithms rapidly without requiring bespoke engineering effort for each change. Crypto-agile organisations can respond to new vulnerabilities or standards within weeks rather than years.
5	**PKI - Public Key Infrastructure** A framework of policies, procedures, hardware, software, and digital certificates that enables the creation, management, distribution, and revocation of digital identities and encryption keys. PKI is foundational to TLS, digital signatures, and identity management in BFSI environments.
6	**TLS - Transport Layer Security** The cryptographic protocol that secures data in transit across networks, including web browsers, APIs, mobile applications, and inter-system communications. TLS relies on public-key cryptography (RSA, ECC) that is vulnerable to quantum attack.
7	**HSM - Hardware Security Module** A dedicated physical or virtual device that generates, stores, and manages cryptographic keys in a tamper-resistant environment. HSMs are critical infrastructure in BFSI payment processing, PKI, and key management. They require firmware and algorithm updates as part of any PQC migration.
8	**Harvest Now, Decrypt Later (HNDL)** An adversarial strategy in which encrypted data is captured and stored today, with the intent to decrypt it once a sufficiently capable quantum computer becomes available. HNDL creates immediate, present-day exposure for long-lived sensitive data - particularly relevant to BFSI institutions with multi-year data retention obligations.
9	**Quantum Readiness** The state of organisational preparedness to protect data and systems against quantum-enabled cryptographic attacks. Quantum readiness encompasses cryptographic visibility, risk assessment, strategic planning, algorithm migration, and ongoing crypto agility governance. It is a programme outcome, not a product purchase.