White Paper - QUANTUM RISK

A STRATEGIC FRAMEWORK FOR PQC MIGRATION AND BOARD ACCOUNTABILITY

AUTHOR: BRIAN COUZENS DATE: NOVEMBER 2025

Executive Briefing: The Quantum Solvency Threat

The Solvency Threat That Has Already Begun

Key Indictment: Harvest Now, Decrypt Later (HNDL)

Quantum computing will break RSA and ECC. This is mathematically established by Shor's Algorithm (Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, 1994). The Key Indictment is Harvest Now, Decrypt Later (HNDL) ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022)- an active, silent data theft event that is ongoing for all long-lived or regulated data. Organisations with long-lived data, regulated datasets, or PKI-dependent infrastructure face an elevated risk of future liability if PQC migration is not initiated.

Mathematical Proof: The Deadline Is Day One

The deadline is not Q-Day. The deadline is the time required to migrate. Mosca's Theorem (Mosca, 2018) proves the deadline is mathematically in the past. If the time to migrate (X) plus the time data must remain confidential (Y) exceeds the unknown time to a Cryptographically Relevant Quantum Computer (Z), then data loss probability is almost guaranteed (X + Y > Z). For most enterprises with decade-long data retention, this inequality is already true today, guaranteeing future data loss if migration is not initiated now.

Fiduciary and Governance Mandate

This is a board-level fiduciary issue, not an IT upgrade.

- Standards and Compliance: PQC standards are finalised (FIPS 203, 204, 205) ((NIST) N. I., Federal Information Processing Standards (FIPS) 203, 204, 205: Post-Quantum Cryptography Standards, 2023). Regulators increasingly expect state-of-the-art protections for long-lived data; reliance on RSA/ECC creates foreseeable enforcement risk.
- National Security: The NSA's CNSA 2.0 ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022) mandates migration for national security systems, establishing a minimum benchmark for best practice.
- Liability: Failure to act may increase the risk of regulatory scrutiny, investor claims, and reputational harm; in some jurisdictions this could raise questions about directors' and officers' oversight. Boards should seek legal advice on specific fiduciary implications.

Operational Reality and Survival KPIs

Migration is multi-year and cannot be delegated to vendors. It requires an enterprise-wide mandate.

- The Challenge (X- Migration Time): This visibility gap is the first act of negligence. Most enterprises lack an accurate inventory of cryptographic assets. Shadow Crypto, hard-coded primitives, embedded systems, vendor dependencies, and long-lived datasets guarantee that this transition is multi-year. Security depends on a chain of trust; every dependent system, API, and vendor must complete their transition before final security is achieved.
- Survival KPIs: Visibility → Mitigation → Governance. The Board controls the only variable that prevents failure: starting now. Your first and most critical act of governance is a Cryptographic Bill of Materials (CBOM) to establish visibility and auditability, starting now:

Survival KPI	Board Action	Goal
Visibility	Mandate a **Cryptographic Bill of Materials (CBOM)**.	Provides the required cryptographic inventory to accurately calculate **X (Migration Time)**.
Mitigation	Approve the five-phase PQC roadmap budget.	Systematically transition internet-facing systems, long-lived data, APIs, and vendor cryptography.
Governance	Establish a **Quantum Risk Committee**.	Oversee quarterly Survival KPIs and ensure continuous, non-discretionary budget adherence.

Figure 1-Survival KPIs- The Board Controls all three.

Corroborated Solvency Crisis

Quantum-vulnerable encryption is not a future problem. It is an immediate solvency crisis. Standards bodies, national security guidance, academic analysis, and public cryptographic incidents show long-lived encrypted data is already exposed to retroactive decryption. The threat is demonstrable and auditable, and technical inertia now creates board-level liability. Boards that delay migration may face regulatory enforcement, investor litigation, and personal fiduciary risk. The only defensible response is immediate, measurable action.

Societal and Wellbeing Impacts

Quantum-vulnerable data is a societal threat. Retroactive decryption will cause long-term harm to individuals and communities, undermine trust in essential services, and create systemic economic and social damage. Boards should treat PQC migration as a public-interest duty and act now.

IMMEDIATE ACTION MANDATE

THE FIDUCIARY BOTTOM LINE

The only variable that prevents data loss is the time remaining on X (Migration Time).

The single factor that determines whether your data survives is migration time.

As a director or officer, can you certify to customers, investors, regulators, and your D&O underwriter that your organisation's PQC migration time is zero?

If you cannot, your systems remain exposed, your compliance is incomplete, and your liability may be personal.

The mandate is immediate: act now or accept responsibility for failure.

Our full catalogue of services is detailed in the Appendix: SITG Consulting Service Authority.

Statements about liability, fiduciary duty, and enforceable obligations are jurisdictional and fact-specific; consult legal counsel for binding interpretation.

Table of Contents

GRAPHICS INDEX IN ORDER OF DOCUMENT

1. Purpose and Scope

1.1 Purpose

This white paper delivers a forensic roadmap for surviving the quantum risk era. The purpose of this white paper is to provide Boards, Regulators, and Transformation Leaders with a forensic roadmap for surviving the quantum risk era. Quantum computing poses an existential threat to current cryptographic foundations. RSA and ECC will collapse under Shor's Algorithm. Symmetric algorithms such as AES-256 remain viable under Grover's Algorithm with adjustments. Data encrypted today may be decrypted tomorrow under the "Harvest Now, Decrypt Later" (HNDL) threat.

This paper fulfils two functions:

Strategic Mandate

- Indict the technical reality with evidence and survival framing.
- Translate cryptographic advances into board accountability and fiduciary liability.
- Define immediate survival KPIs that executives can act on.
- Position SITG Consulting as the benchmark authority in quantum resilience and migration strategy.

Operational Mandate

- Provide CISOs, Risk Officers, and Architects with a structured framework for PQC migration, budgeting, and compliance with emerging standards (NIST FIPS 203/204/205, NSA CNSA 2.0).
- Establish deliverables such as a Cryptographic Bill of Materials (CBOM) to ensure visibility and auditability of cryptographic assets.
- Address the PQC talent gap by outlining workforce strategies for upskilling, vendor reliance, and supply chain resilience.

1.2 Scope

This paper covers the full lifecycle of quantum risk management, from indictment to survival strategy. The scope is board-centric. It avoids theoretical physics while retaining forensic precision. Decision-makers will understand both the urgency and the operational levers required for survival.
In Scope

- Technical Reality Check: Fault tolerance barriers, cryptanalytic advances, PQC standardisation gaps, governance failures, geopolitical race.
- Doomsday Algorithm and Q-Day: Shor's Algorithm, Mosca's Theorem, HNDL threat.
- Solutions Overview: PQC families, security trade-offs, hybrid cryptographic agility.
- Risk Assessment and Inventory: Establishing a CBOM as a standard audit deliverable, prioritising assets, exposing shadow crypto.
- Migration Roadmap and Budget: Three-phase migration model, talent gap, vendor dependencies, cost of delay.
- Legal and Compliance: Data sovereignty, fiduciary duty, liability framing.
- Strategic KPIs and Future-Proofing: Board readiness indicators, Q-Resilience mindset, Quantum Incident Response Plans (Q-IRP).
- Out of Scope
- Theoretical physics such as superposition or entanglement.
- Quantum computing for commercial optimisation such as drug discovery or machine learning.
- Proprietary vendor product reviews. The paper remains vendor-agnostic.

1.3 Target Audience

- Strategic Layer: Boards of Directors, CEOs, CFOs, Regulators, Legal Counsel, Risk Committees, Audit Chairs.
- Operational Layer: Transformation Leaders, CISOs, CIOs, Enterprise Architects, Compliance Officers, Vendor Managers, Supply Chain Officers.

1.4 Visuals Note

This paper employs diagrams and timelines including Mosca's Theorem inequality, HNDL timeline, CBOM flow, migration roadmap, and resilience cycle to ensure clarity for non-technical audiences and reinforce board comprehension.

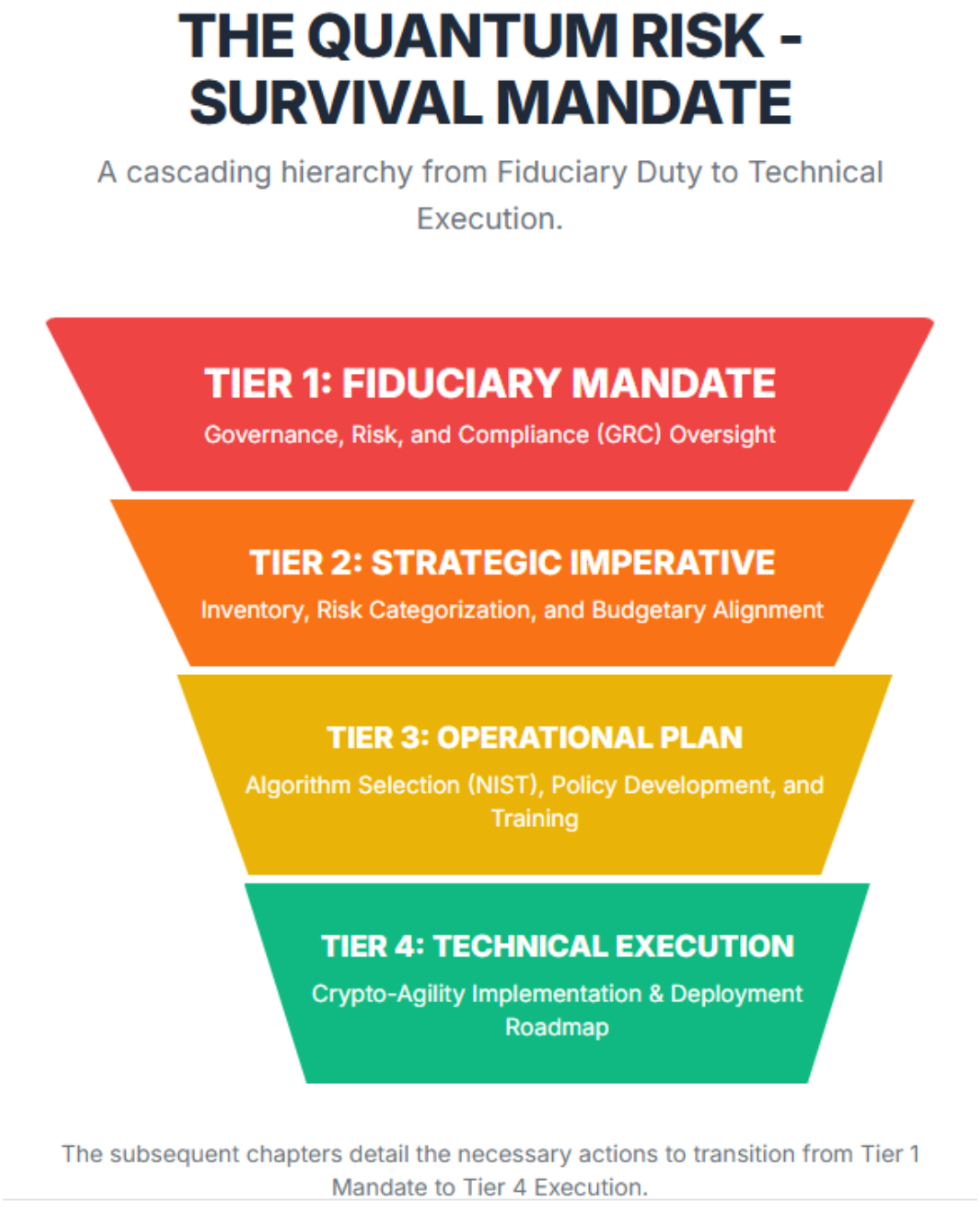

Figure 2-Survival Mandate Tiers - One Solvency Outcome.

2. Executive Summary

Quantum-vulnerable encryption is not a future problem. It is a present societal crisis. Standards bodies, national security guidance, academic analysis, and public cryptographic incidents show that long-lived encrypted data is already exposed to retroactive decryption. This exposure will produce real human harms: identity theft, irrevocable privacy loss, compromised medical records and disruption of critical services. Technical delay converts into social harm, regulatory liability, and material loss. Immediate, measurable action is required.

2.1 The Quantum Imperative

The threat posed by a Cryptographically Relevant Quantum Computer is a foreseeable solvency crisis requiring immediate board governance. RSA and ECC will fail under Shor's Algorithm. AES-256 remains viable under Grover's Algorithm with adjusted key sizes. The deadline for corrective action is not Q-Day but today. Failure to act may be solvency liability attaching directly to fiduciary duty.

2.2 Mathematical Proof of Failure

Data security is already compromised. Mosca's Theorem, X+Y>Z, provides the mathematical justification for immediate action. Any data with a shelf-life (Y) which, when added to the time required for migration (X), exceeds the time remaining until a quantum break (Z), is guaranteed to fail. The Harvest Now, Decrypt Later threat compounds this reality. Adversaries are exfiltrating encrypted high-value data now to decrypt later. Opaque nation-state programmes accelerate unpredictability, making the quantum break horizon unknowable. Inaction may be a breach of fiduciary duty.

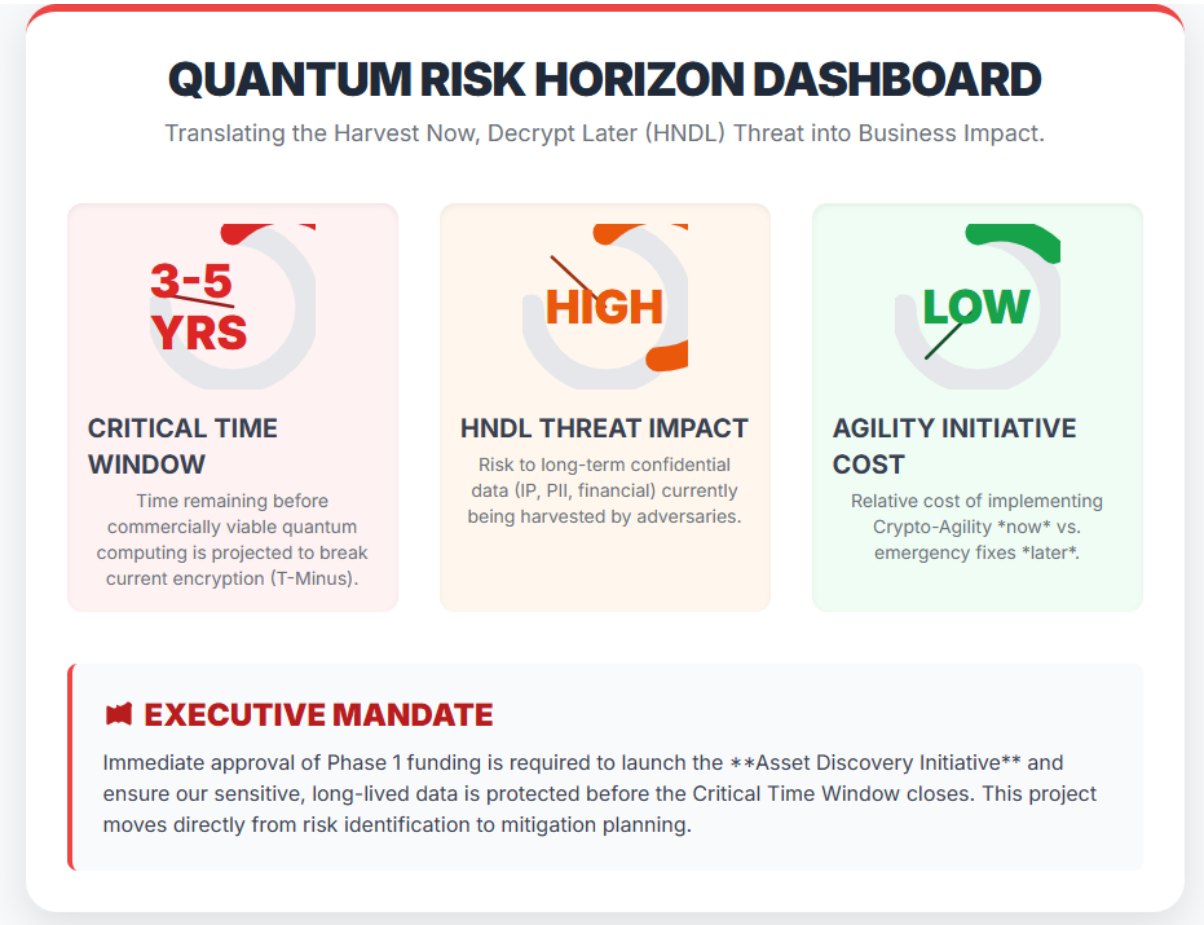

Figure 3-Quantum Risk Dashboard (time, threat level, and cost).

2.3 Indictments

2.3.1 Technical Reality: Fault tolerance barriers remain but cryptanalytic advances are closing. PQC standardisation is in final stages, but implementation gaps persist. Governance failures are the greatest internal risk.
2.3.2 Geopolitical Race: The race for quantum supremacy involves opaque state-sponsored programmes in major economic powers including IBM, Google, China, Russia, India, and Europe.
2.3.3 Doomsday Algorithm: Shor's Algorithm ends public-key encryption. Grover's Algorithm weakens symmetric systems, forcing key-size adjustment.
2.3.4 HNDL Exposure: Any long-lived data stolen today, including intellectual property, contracts, and state secrets, will be decrypted tomorrow.

2.4 Strategic and Operational Challenge

The transition to PQC is not a software patch. It is a multi-year, multi-departmental transformation requiring cryptographic agility. This paper provides a forensic roadmap addressing:
2.4.1 Inventory and Assessment: Establish a Cryptographic Bill of Materials as an auditable inventory to expose shadow crypto and profile risk.
2.4.2 Resource and Talent Gap: Allocate budget for a three-phase roadmap (Discovery → Pilot → Deployment). Address the cryptography talent gap through workforce strategy, upskilling, and vendor reliance.
2.4.3 Legal and Compliance Failure: Failure to initiate PQC migration could, in certain circumstances and jurisdictions, increase the risk of regulatory enforcement under regimes such as GDPR or sectoral laws; boards should consult counsel to understand specific obligations and exposure.

2.5 Immediate Board Actions

Executive leadership should act now to secure enterprise longevity and satisfy standards set by NSA CNSA 2.0 and NIST.
2.5.1 Mandate the CBOM Project: Authorise and fund a centralised, auditable CBOM as the first strategic KPI.
2.5.2 Approve the PQC Migration Roadmap: Allocate resources for a planned transition. Delay is the most expensive option.
2.5.3 Embed Q-Resilience Governance: Incorporate survival KPIs into governance structures and mandate a Quantum Incident Response Plan. Survival KPIs must be embedded into board reporting and reviewed quarterly.

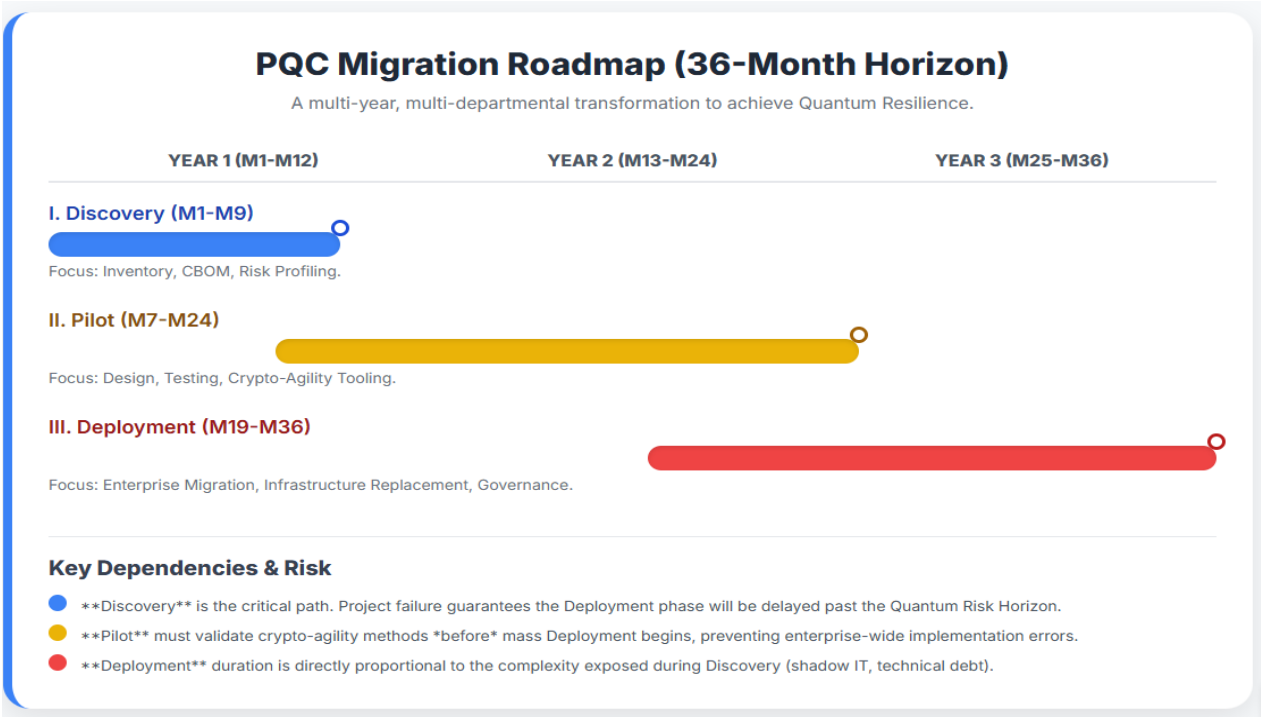

Figure 4-PQC Migration Roadmap - Three Phases.

2.6 Mandate

Boards should lead this transition. The choice is clear: secure data longevity and affirm fiduciary duty or risk failure of security, compliance, and corporate survival in the quantum era.

3. Technical Reality Check

The quantum threat is often dismissed based on raw qubit counts reported by public labs. This is a critical error. The true benchmark is a Cryptographically Relevant Quantum Computer (CRQC), a machine with enough stable logical qubits to execute Shor's Algorithm efficiently. This chapter details the non-negotiable scientific and geopolitical facts that define the current state of play.

3.1 Fault Tolerance Barriers: The Scale of the Challenge

3.1.1 Quantum Error Correction
Quantum computers require extensive Quantum Error Correction (QEC) to achieve fault tolerance. Physical qubits are highly susceptible to environmental noise.
3.1.2 Conversion Problem
Current prototypes demand thousands of noisy physical qubits to stabilise a single logical qubit capable of running Shor's Algorithm. This conversion overhead defines the engineering challenge.
3.1.3 Scaling Progress
Scaling barriers are being reduced through coherence and coupling breakthroughs. Once viability is proven, sustained engineering and financial resources will solve scaling. The technical difficulty does not delay the long-term threat horizon.

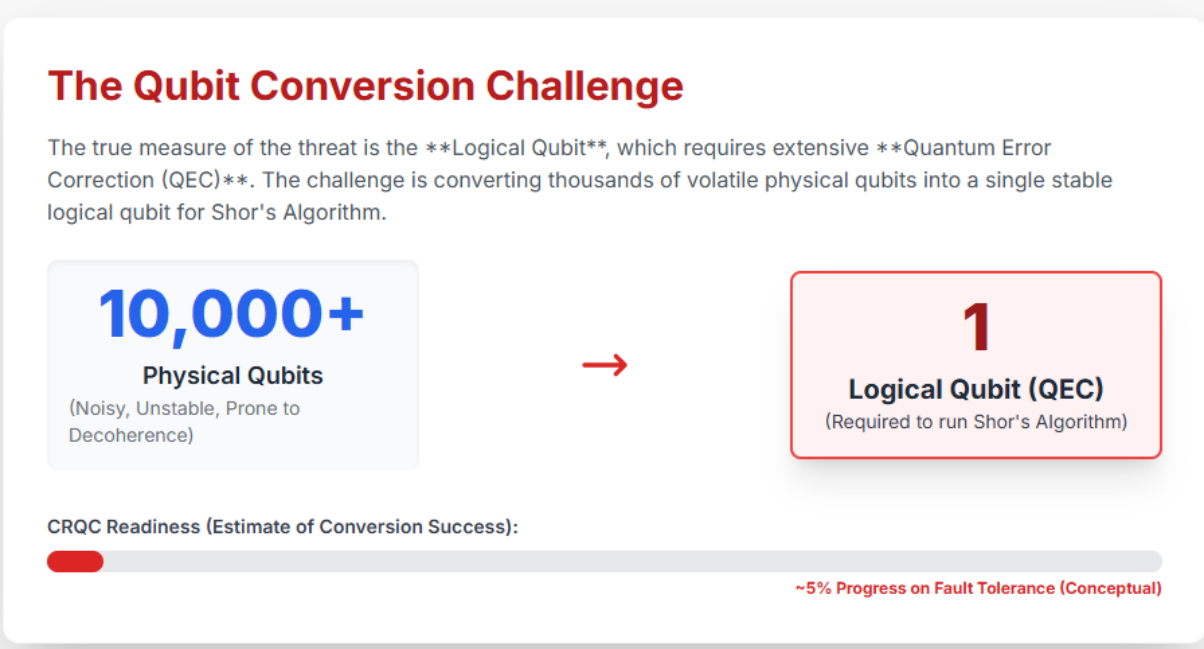

Figure 5-Qubit Conversion Challenge.

Thousands of unstable qubits needed for one logical qubit. Progress remains below 5 percent.

3.2 Cryptanalytic Advances

3.2.1 Doomsday Algorithms
Shor's Algorithm is the definitive end of RSA and ECC. Grover's Algorithm reduces brute force complexity against symmetric systems, forcing mandatory key-size adjustment. AES-128 becomes AES-256.
3.2.2 Vulnerability Exposure
Hybrid and lattice-based PQC schemes remain vulnerable to side-channel and implementation flaws. Algorithm strength alone is insufficient defence.
3.2.3 Accelerated Timelines

Optimisations or non-public state-sponsored research could reduce logical qubit requirements and accelerate CRQC readiness.

Cryptographic Algorithm Impact Matrix

Assessment of the impact of the two "Doomsday Algorithms" on current enterprise cryptography.

CURRENT ALGORITHM	QUANTUM THREAT	IMPACT LEVEL	REQUIRED ACTION
RSA (Asymmetric)	Shor's Algorithm	**BREAK (Total Failure)**	REPLACE with PQC (ML-KEM/ML-DSA)
ECC (Asymmetric)	Shor's Algorithm	**BREAK (Total Failure)**	REPLACE with PQC (ML-KEM/ML-DSA)
AES-128 (Symmetric)	Grover's Algorithm	**WEAKENED (Key Halved)**	KEY SIZE INCREASE to AES-256
AES-256 (Symmetric)	Grover's Algorithm	SAFE (Adequate Protection)	No immediate change required

*Based on current consensus; symmetric keys can be considered secure if length is doubled (e.g., 256 bits for quantum resistance).

Figure 6-Algorithm Impact Matrix.

Shor breaks RSA and ECC. Grover weakens AES-128. Action is mandatory.

3.3 PQC Standardisation Gaps

3.3.1 Standards Finalised

NIST has finalised three PQC standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA) ((NIST) N. I., Federal Information Processing Standards (FIPS) 203, 204, 205: Post-Quantum Cryptography Standards, 2023).

3.3.2 Uneven Adoption

Many enterprises have not inventoried cryptographic assets. Implementation guidance is fragmented, and vendor ecosystems remain immature.

3.3.3 Compliance Disparity

NSA CNSA 2.0 ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022)mandates PQC transition for national security systems. Commercial enforcement is absent. This lack of regulatory pressure fosters organisational inertia.

3.4 Infrastructure and Key Management Issues

3.4.1 Hard-Coded Crypto

Legacy systems and embedded devices often have cryptographic primitives hard-coded into firmware or source code, making updates costly and complex.

3.4.2 Key Management Sprawl

Key management systems are incomplete. Thousands of keys reside across dispersed Hardware Security Modules and vaults.

3.4.3 CBOM Necessity

Without a comprehensive Cryptographic Bill of Materials, accurate risk profiling and migration planning is impossible. Liability remains unaddressed.

3.5 Governance Failures

3.5.1 Delegation of Solvency Risk
Boards and regulators have not mandated cryptographic inventories or migration timelines. PQC is often funded under standard cybersecurity budgets, leading to under-resourcing.
3.5.2 Lack of C-Suite Ownership
Responsibility is delegated too far down the organisation chart. Shadow Crypto remains unaddressed, hiding liabilities.
3.5.3 Fiduciary Liability
This inertia converts technical risk into potential solvency liability. Fiduciary duty requires immediate board ownership.

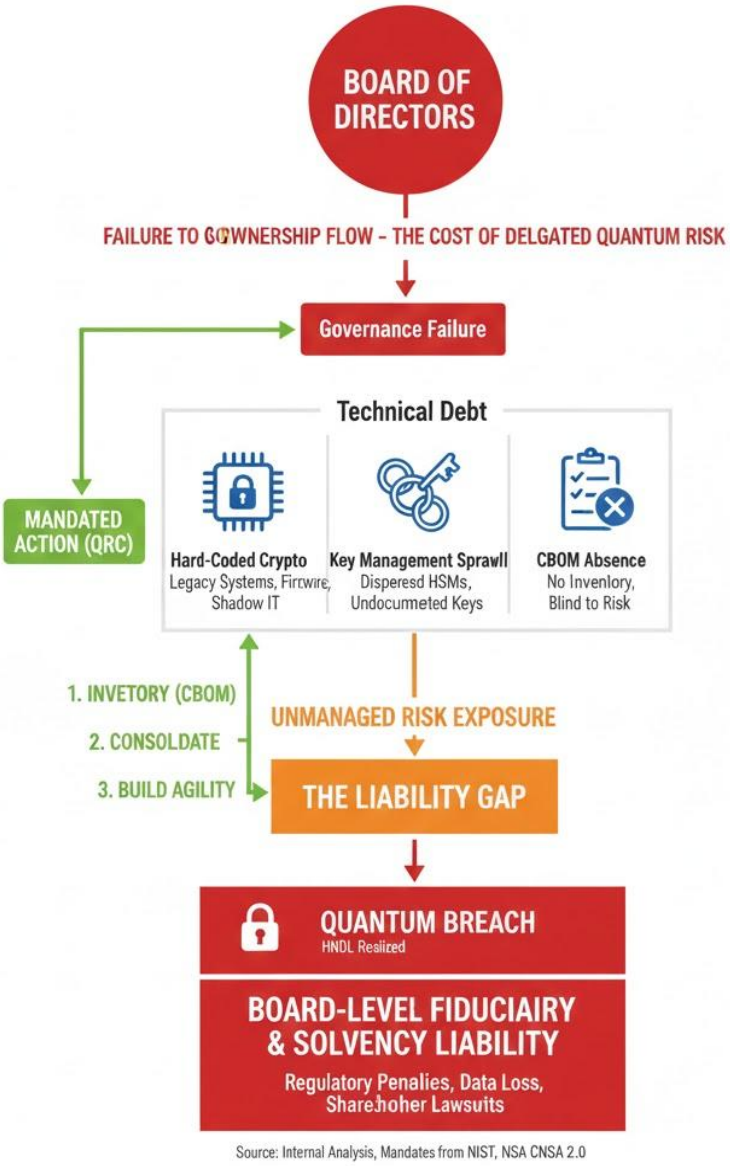

Figure 7-Delegated Quantum Risk.

Board inaction leads to technical debt, exposure, and solvency liability.

3.6 Geopolitical Race for Cryptographic Dominance

3.6.1 Opaque Programmes
IBM, Google, and Microsoft lead commercial research. Opaque state-sponsored programmes in China, Russia, India, and Europe ((ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021) accelerate unpredictability.
3.6.2 Unannounced Weaponisation
Breakthroughs may not be announced until weaponised against economic or state targets.
3.6.3 Parallel Paths
Multiple qubit modalities are being pursued in parallel, increasing the probability of an unannounced breakthrough.

3.7 Mandate

Boards must indict the technical reality. Survival requires governance enforcement of cryptographic inventories, PQC migration planning, and quarterly reporting of survival KPIs including CBOM completion and migration milestones. Delay is indefensible.

4. Doomsday Algorithm and Q-Day

The technical facts established in Chapter 3 must be framed within mathematical and temporal certainty. The threat is defined by two foundational algorithms, a single formula for timing risk, and a liability mechanism that is active today: the Harvest Now, Decrypt Later threat.

4.1 The Doomsday Algorithms: Shor's vs Grover's

4.1.1 Shor's Algorithm: Existential threat

Shor's Algorithm (Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, 1994) enables a Cryptographically Relevant Quantum Computer to solve integer factorisation and discrete logarithms in polynomial time. RSA and ECC collapse immediately and retroactively once CRQC capability is achieved.

- Impact: Complete failure of asymmetric encryption.
- Mandate: Mandatory replacement.

4.1.2 Grover's Algorithm: Weakening threat.

Grover's Algorithm (Grover, 1996) provides a quadratic speed-up for brute force search. Grover halves effective security: AES-256 provides ~128-bit effective security.

- Impact: Symmetric systems require key-size adjustment.
- Mandate: Mandatory adjustment.

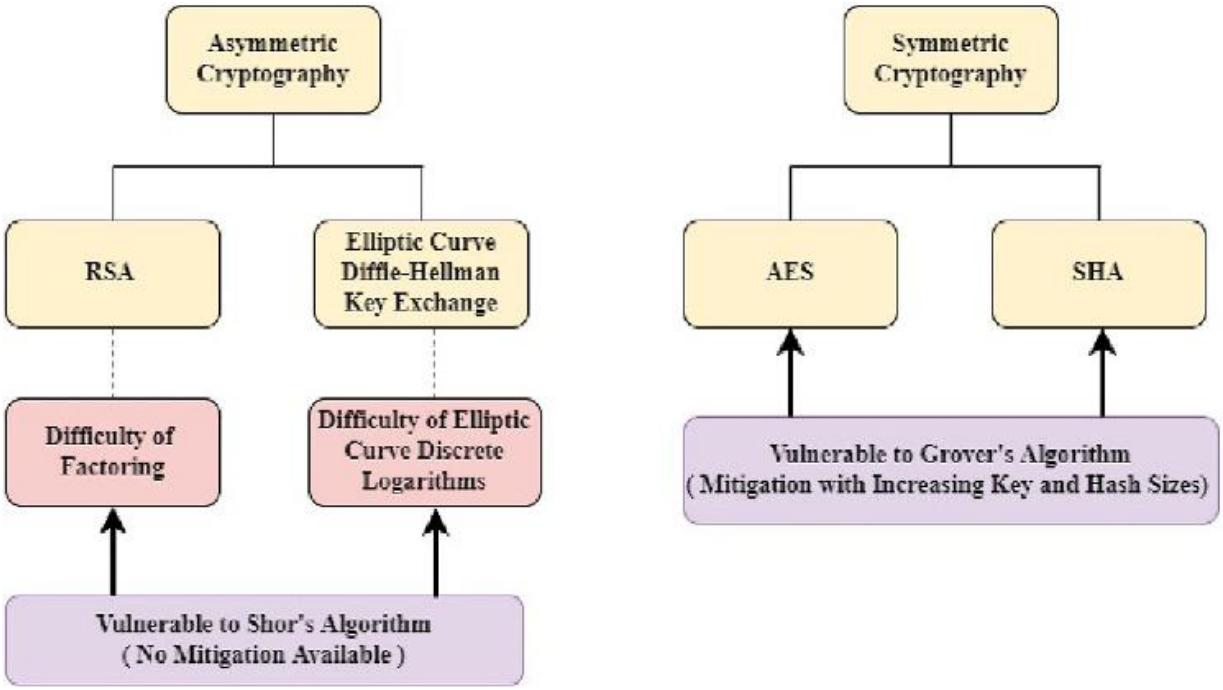

Figure 8-Quantum Algorithm Impact.

Shor breaks asymmetric. Grover weakens symmetric. Mitigation is mandatory.

4.2 The mathematical deadline: Mosca's Theorem

Mosca's Theorem (Mosca, 2018) defines the equation for cryptographic failure:

$$X+Y>Z$$

- X: Time required to complete PQC migration across inventory, pilot, deployment.
- Y: Shelf-life or secrecy period of protected data.
- Z: Time remaining until CRQC capability.

Indictment: If $X+Y>Z$, data is already compromised. For long-lived data, this inequality is true today. Boards control X and Y. Adversaries control Z.

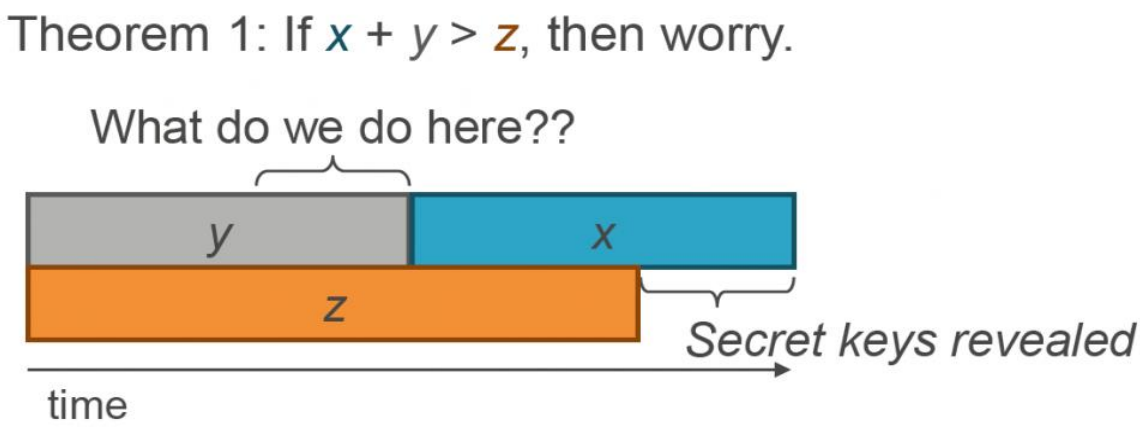

Figure 9-Mosca's Theorem.

If X plus Y exceeds Z, failure is guaranteed.

4.3 The HNDL indictment: Active solvency liability

Adversaries are exfiltrating encrypted data now, storing it indefinitely, and waiting for CRQC capability.

- Retroactive failure: Today's encryption becomes tomorrow's failure.
- Target profile: Intellectual property, M&A data, proprietary algorithms, long-term customer data, internal communications.

- Active liability: Failure to initiate PQC migration converts future technology risk into present solvency liability. Boards are accountable now.

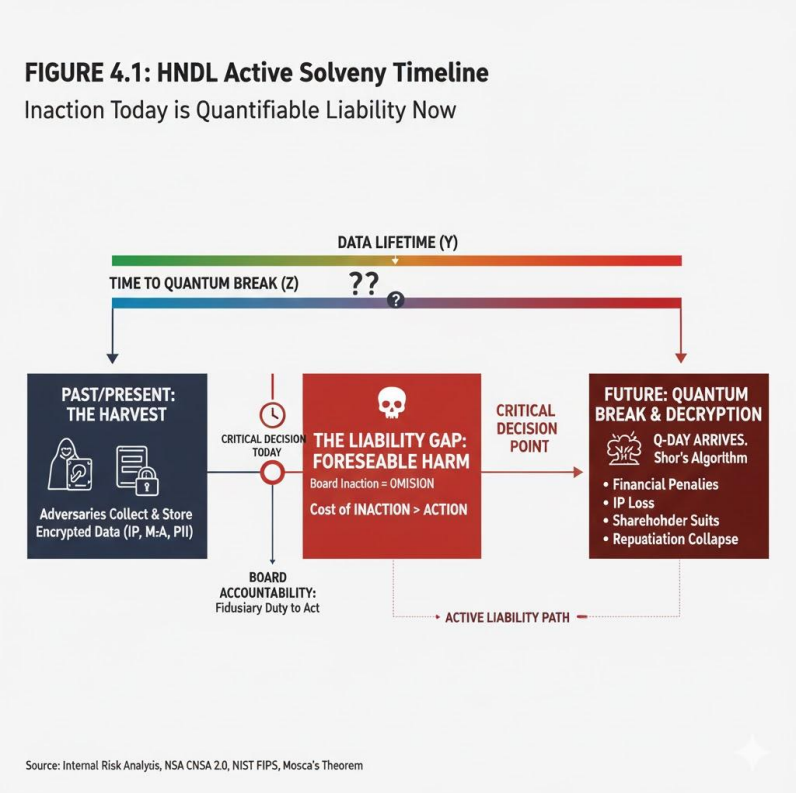

Figure 10-Active Solvency Timeline.

Harvested data becomes board liability. Delay triggers foreseeable harm.

4.4 Q-Day: The ultimate solvency event

Q-Day ((NIST) N. I., Getting Ready for Post-Quantum Cryptography (NIST Cybersecurity White Paper), 2021) is the moment a CRQC is confirmed to exist and is widely credible confirmation of a CRQC capable of breaking deployed RSA/ECC key sizes.

- Immediate impact: RSA and ECC lose secrecy and integrity. Secure boot, VPNs, TLS, identities, and certificate authorities fail.
- Compliance abyss: Organisations with long-term data face lawsuits and regulatory penalties for foreseeable and preventable loss.
- Strategic mandate: The objective is quantum readiness, with $X \approx 0$ before Q-Day.

4.5 Mandate

Boards should recognise the Doomsday Algorithm as a solvency threat. Survival requires immediate enforcement of PQC migration ((NIST) N. S., 2022–2023), CBOM completion, and quarterly reporting of survival KPIs. Delay may be indefensible.

5. Post-Quantum Cryptography (PQC) Solutions Overview

The risk defined by the Doomsday Algorithm requires immediate mitigation. The solution is adoption of Post-Quantum Cryptography. This is not a single product. It is a family of mathematical schemes with different strengths, weaknesses, and performance implications. Selection must be strategic.

5.1 Algorithm Families

NIST has finalised standards based on problems believed to be intractable for a Cryptographically Relevant Quantum Computer.

5.1.1 Lattice Based Cryptography

Dominant solution for key establishment and digital signatures. Based on the difficulty of finding the shortest vector in a lattice.

Key Standards: ML-KEM (CRYSTALS-Kyber) for key encapsulation (FIPS 203) ((NIST) N. I., Federal Information Processing Standard (FIPS) 203: ML-KEM — Key Encapsulation Mechanism (CRYSTALS-Kyber), 2024) and ML-DSA (CRYSTALS-Dilithium) for digital signatures (FIPS 204) ((NIST) N. I., Federal Information Processing Standard (FIPS) 204: ML-DSA — Digital Signature Algorithm (CRYSTALS-Dilithium), 2024).

Trade-offs: Strong performance and resistance to classical attacks. Weaknesses include larger key and signature sizes compared to ECC and exposure to side channel attacks if implemented poorly.

5.1.2 Hash Based Cryptography

Schemes such as XMSS and LMS rely on hash functions. Grover's Algorithm requires key size doubling but does not collapse them.

Key Standard: SLH DSA (SPHINCS+) for digital signatures (FIPS 205) ((NIST) N. I., Federal Information Processing Standard (FIPS) 205: SLH-DSA — Digital Signature Algorithm (SPHINCS+), 2024).

Trade-offs: Strong theoretical security. Less efficient. Stateful and stateless requirements add complexity.

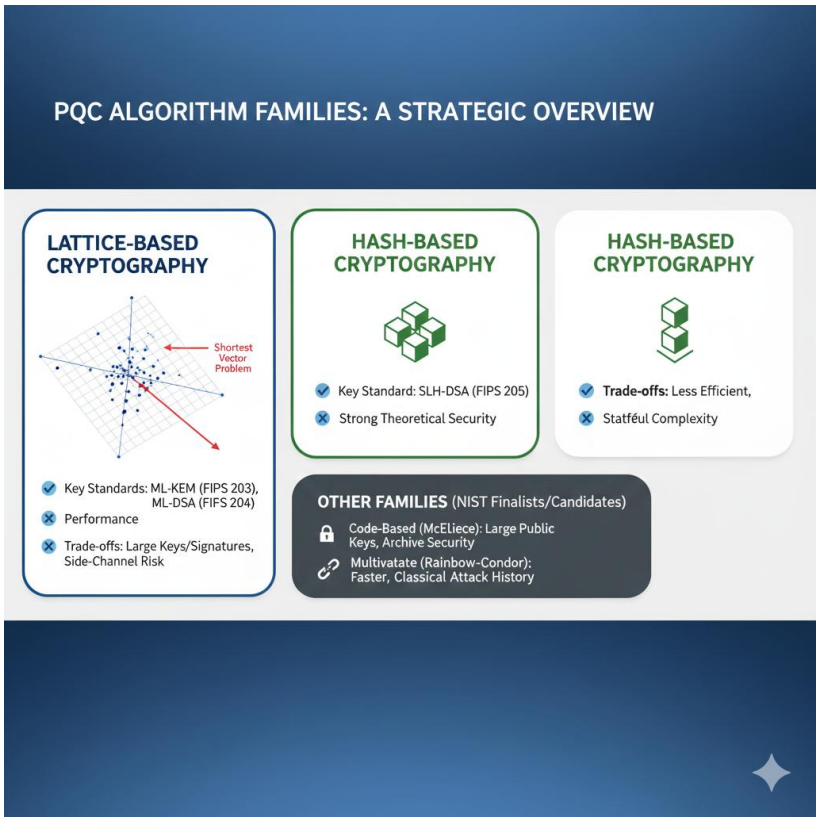

Figure 11-PQC Algorithm Families.

Lattice, hash, and code based. Each with trade-offs, all with quantum resilience.

5.1.3 Other Families

Code Based: McEliece. Strong security. Extremely large public keys.

Multivariate: Polynomial equations. Faster but complex. Several classical attacks have succeeded. ((NIST) N. I., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NIST IR 8413), 2022)

5.2 Security and Performance Trade-offs

No algorithm offers the balance of security and efficiency that RSA and ECC once did. Migration requires compromise ((NIST) N. I., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NIST IR 8413), 2022).

Size vs Speed: Some schemes produce large keys and signatures but compute quickly. Others are smaller but slower.

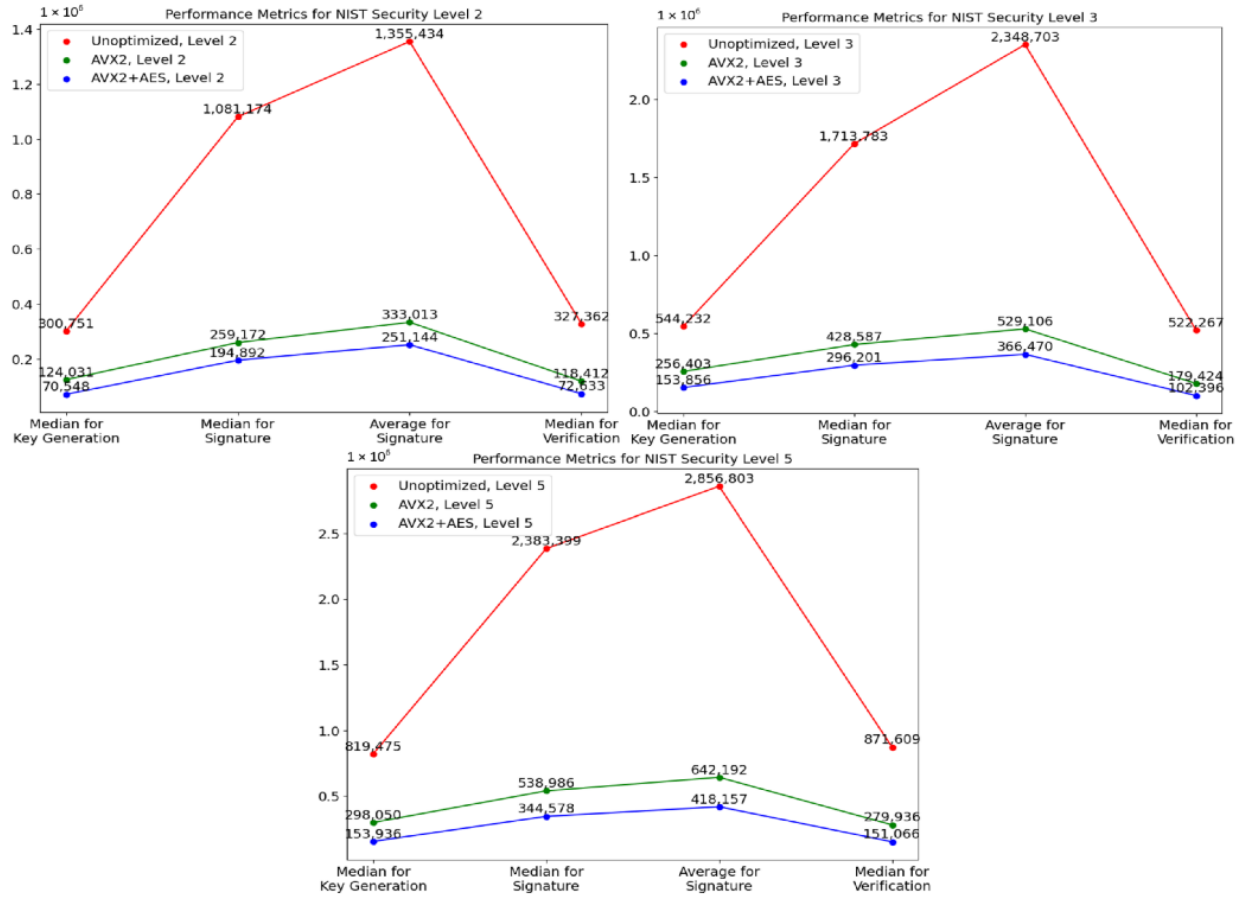

Figure 12-PQC Performance Metrics.

Speed matters. Boards must benchmark cryptographic performance before committing to migration.

Implementation Risk: Security depends on implementation quality. Side channel attacks remain a major threat.
Future Assurance: The field is young. Collapse of a family remains possible. Layered defence is required.

5.3 Cryptographic Agility

Organisations should build the capability to change algorithms, key lengths, protocols, and standards without redesign or downtime.

5.3.1 Definition

Cryptographic Agility is the ability to replace cryptographic implementations rapidly across infrastructure ((ETSI), 2020).

5.3.2 Hybrid Modes

Hybrid mode uses two primitives concurrently. Classical RSA or ECC paired with a quantum-resistant algorithm such as CRYSTALS-Kyber. A connection is accepted only if both succeed ((NIST) N. I., Recommendation for Pairing Post-Quantum Cryptography with Classical Algorithms in Hybrid Modes, 2023).

Benefit: Continuity if the new algorithm fails. Quantum security because both must be broken.
Governance: Systems must allow switching between algorithms or removal of classical components without interruption.

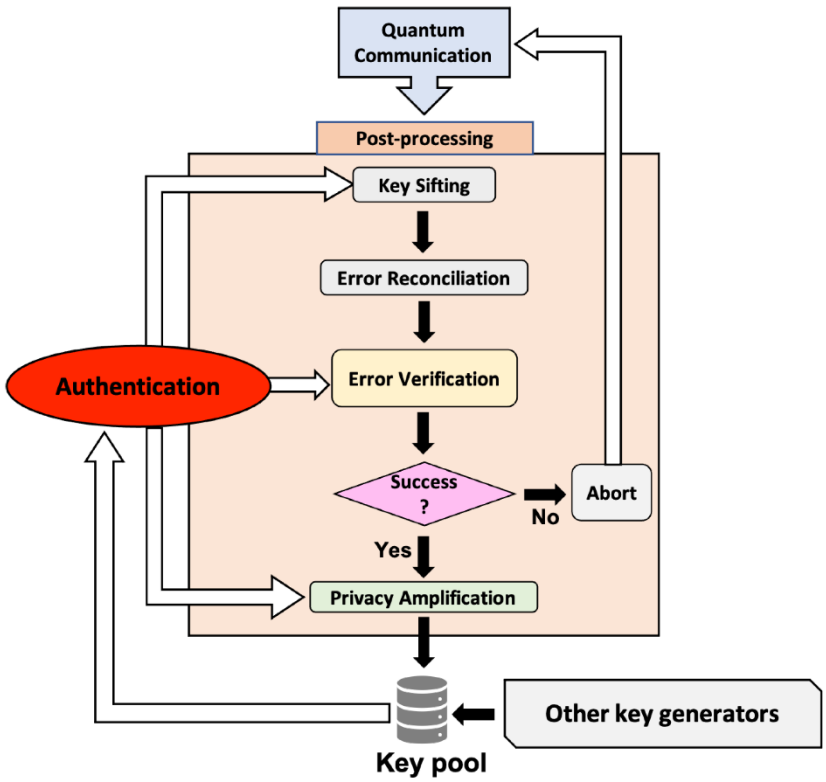

Figure 13-Quantum Key Distribution.

Secure key generation via quantum communication. Post-processing ensures integrity and privacy.

5.4 Mandate

Boards should mandate transition using Hybrid Agility. Governance must embed flexibility to swap primitives in the future. This prevents recurrence of rigid infrastructure crises ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022).

6. Quantum Risk Assessment and Inventory

The transition to Post Quantum Cryptography requires quantifying the scope of the problem. This quantification involves establishing a unified, auditable inventory of all cryptographic assets. The Cryptographic Bill of Materials (CBOM) is the mandatory metric for board accountability and quantum readiness.

6.1 Identify Cryptographic Assets

Boards must know what is at risk. This includes all systems using cryptography for confidentiality, integrity, authentication, or trust.
Asset Categories:

- Transport: TLS, VPNs, SSH, public facing communication protocols
- Identity: Certificates, digital signatures, secure boot mechanisms, PKI components
- Data at Rest: Encrypted files, databases, backups, long term archives
- Data in Transit: Messaging platforms, APIs, inter service communication
- Code Integrity: Signed binaries, firmware, software update packages
- Shadow Crypto: Hard coded keys, undocumented libraries, legacy dependencies

Mandate: No asset can be protected if it is not inventoried and assessed for RSA or ECC dependency ((ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021).

6.2 Establish a Dynamic CBOM

The CBOM is the survival baseline. It must be complete, version controlled, and auditable.
Required Fields:

- Algorithm type and key length
- Protocol and cryptographic library dependency
- Endpoint and system location
- Expiry profile and critical data shelf life (Y variable from Mosca's Theorem)
- Migration status and organisational owner

Format and Governance:

- Centralised, version-controlled repository, not a static spreadsheet
- Automated quarterly board reporting
- Integration with vendor disclosures to track supply chain liability

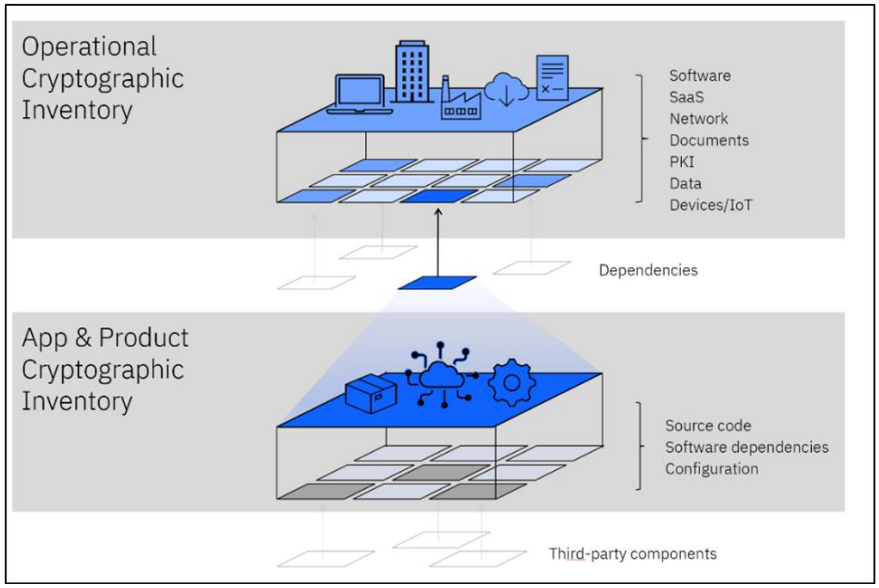

Figure 14-Cryptographic Inventory Layers.

Operational assets depend on app and product inventories. CBOM must capture all layers.

Mandate: CBOM completion is the first survival KPI. No migration can proceed without it ((NIST) N. I., Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, 2021).

6.3 Determine Risk Profile

Each asset must be classified by exposure and operational or legal impact. This profiling links the CBOM to fiduciary duty.
Risk Factors:

- Data Lifetime: Long lived data (high Y) is exposed to the Harvest Now, Decrypt Later threat
- System Criticality: Failure triggers operational outage or legal breach
- External Exposure: Internet facing systems are primary attack vectors
- Compliance Scope: Assets governed by GDPR, HIPAA, PCI DSS, federal contracts

Mandate: Boards must prioritise assets based on quantitative risk (Mosca, 2018).

6.4 Identify Shadow Crypto

Shadow Crypto is undocumented, legacy, or third-party cryptography outside governance.
Sources:

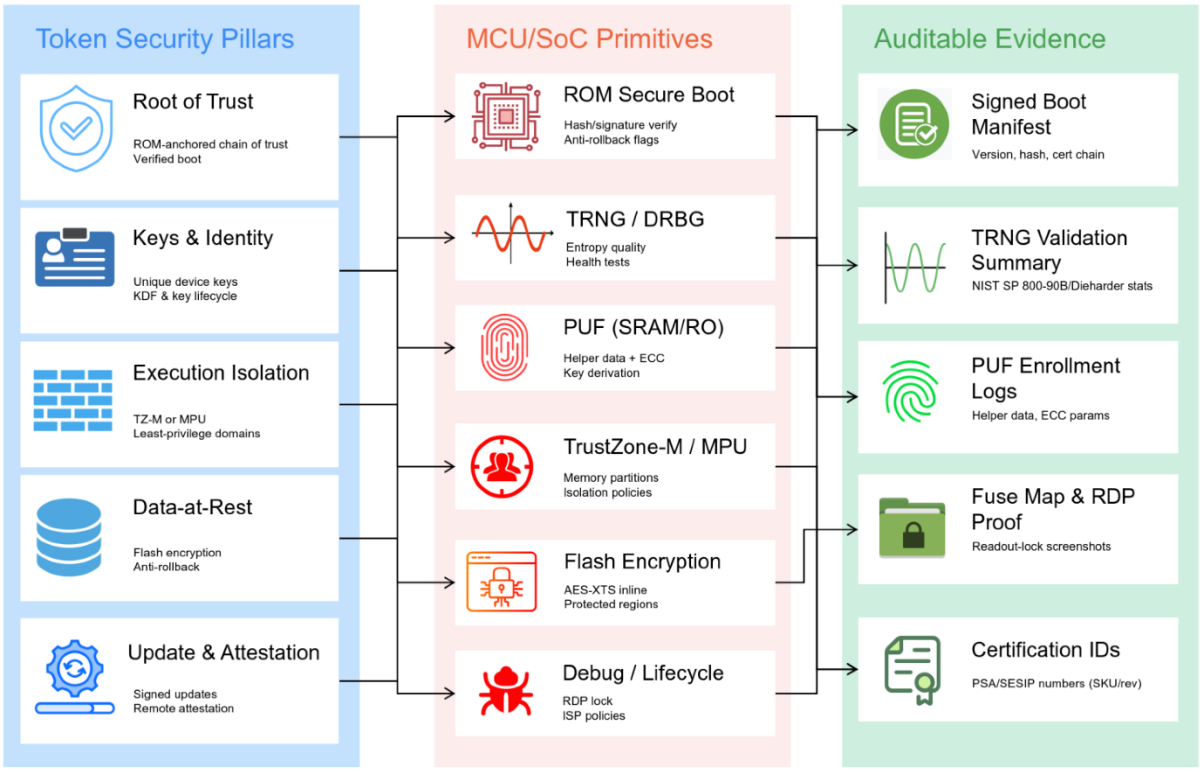

Figure 15-Shadow Crypto Exposure.

Risk starts in code and config. CBOM must trace every dependency to prevent liability.

- Embedded systems and IoT devices
- Proprietary vendor SDKs and libraries
- Legacy applications with undocumented cryptographic calls
- Hard coded keys or credentials in source code

Mandate: Shadow Crypto must be exposed and brought under CBOM control. Omission guarantees unmanaged liability. ((ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021)

6.5 Mandate

Boards should enforce full cryptographic inventory and mandate funding for the CBOM project. CBOM completion is non-negotiable. Survival requires visibility before migration. Delay may be indefensible. ((NIST) N. I., Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, 2021)

7. PQC Migration Roadmap & Budget

The shift from risk acknowledgement to mitigation requires a funded, phased, and governed roadmap. To protect long-lived data and ensure solvency, the enterprise must transition within three to five years. The only controllable variable in Mosca's Theorem (X + Y > Z) is migration time (X). Delay adds compounding liability and guarantees exposure to the Harvest Now, Decrypt Later threat. This roadmap defines the process, budget, and talent strategy required to execute the PQC transition.

7.1 Define Migration Phases

Migration is a multi-year transformation. It must be centrally managed and reported quarterly. The five-phase model provides governance granularity.
Phases:
Phase 1: Discovery and Inventory (Months 1–12). Completes the CBOM and establishes cryptographic policy.
Phase 2: Internet-facing Systems and Long-Lived Data (Months 10–24). Deploys hybrid PQC to public systems and re-encrypts critical data at rest.
Phase 3: Internal Systems and Compliance Exposure (Months 18–36). Secures internal APIs and regulated systems.
Phase 4: Vendor Dependencies and Supply Chain Cryptography (Months 24–48). Enforces vendor CBOM submissions and mandates PQC compliance.
Phase 5: Legacy Systems, Shadow Crypto, and Sunset (Months 36+). Retires hard-coded cryptography and decommissions classical algorithms.
Mandate: No phase proceeds without CBOM validation, documented risk reduction, and board sign-off. ((NIST) N. I., Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, 2021)

Figure 16-PQC Migration Roadmap.

Five-phase transformation with board milestones. Timeline defines urgency and sequencing.

7.2 Select PQC Algorithms

Algorithm selection is a governance decision. It must be based on risk, performance, and maturity.
Selection Criteria:

- NIST standardisation status (FIPS 203, 204, 205)
- Key and signature size impact
- Performance benchmarks for latency and throughput
- Known weaknesses including side-channel risks
- Hardware compatibility in HSMs, FPGAs, and embedded systems

Mandate: Boards should approve algorithm selection based on operational fit and risk analysis. Agility is the goal. ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024)

7.3 Replace Protocols and Libraries

Protocols must be upgraded to support PQC primitives.
Actions:

- Replace RSA and ECC with CRYSTALS-Kyber and CRYSTALS-Di lithium in hybrid modes
- Upgrade OpenSSL, BoringSSL, NSS to PQC-enabled versions
- Validate fallback and failure logic in hybrid modes
- Enforce downgrade prevention and version control

Mandate: Protocol replacement must be tested, versioned, and auditable. Downgrade risks are unacceptable ((IETF), 2018).

7.4 Coordinate Vendor Migration

Vendor exposure is external liability. Compliance is contractual.
Requirements:

- Vendor CBOM submission
- PQC readiness declaration
- Migration schedule linked to SLA
- Liability clauses for non-compliance

Mandate: Vendor migration is a governance obligation. Boards should enforce compliance through procurement leverage ((ENISA), Study on Cryptographic Agility and Migration, 2021).

7.5 Budget and Funding Logic

Migration requires dedicated funding. It is a solvency expenditure.
Budget Categories:

- CBOM tooling and automation
- Protocol and library upgrades
- Vendor audits and SLA enforcement
- Staff training and talent augmentation
- Legacy contingency for non-upgradeable systems

Mandate: Budget must be multi-year, board-approved, and tracked quarterly. Underfunding guarantees liability ((NIST) N. I., Getting Ready for Post-Quantum Cryptography: Exploring Challenges

Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, 2021).

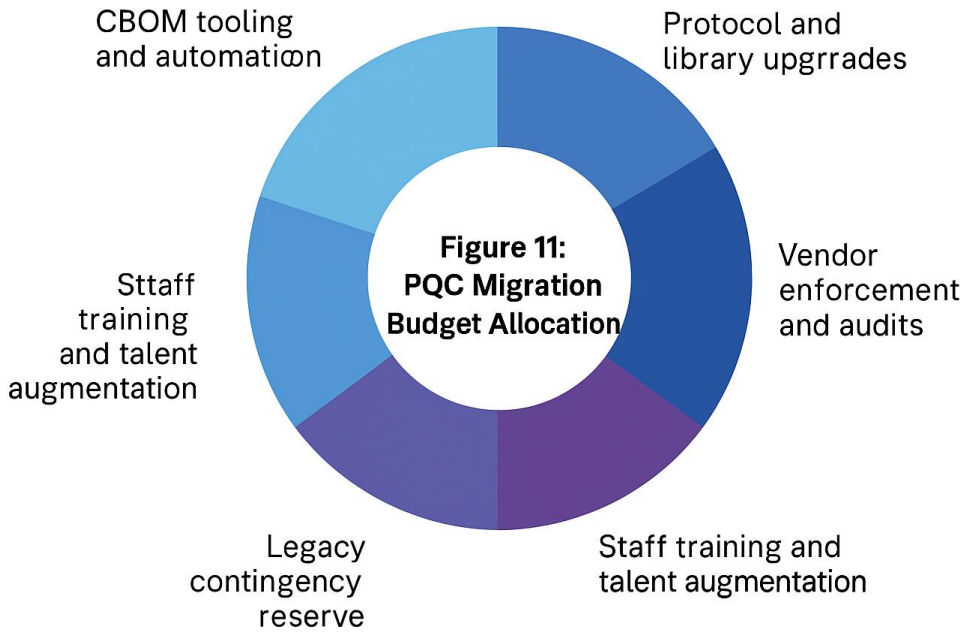

Figure 17-PQC Migration Budget Allocation.

Five solvency categories. CBOM, upgrades, audits, training, and legacy contingency

7.6 Mandate

The roadmap is the path to survival. Boards should enforce phased execution, algorithm selection, protocol replacement, vendor coordination, and budget allocation. Delay creates a high likelihood of failure. Underfunding creates a high likelihood of failure. Survival depends on immediate action ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022).

8. Governance Mandate and Strategic References

Quantum risk is a governance failure and an existential threat to corporate solvency. Boards should own the risk, enforce migration, and align with authoritative standards. This chapter consolidates governance architecture, compliance obligations, strategic benchmarks, and intelligence caveats into a single survival mandate.

8.1 Board Ownership and Governance Architecture

The time for delegation has passed. Only the board can mandate transformation and unlock solvency expenditure. Governance must be structured for enforcement, not reporting ((OECD), 2019).
Mandates:

- Board Resolution: Formal motion to initiate PQC migration, recorded in board minutes and tied to fiduciary duty.
- CEO Accountability: CEO should sign off on migration funding and execution. Delegation to CTO or CISO is operational only.
- Quantum Risk Committee (QRC): Sub-committee of the board with authority to enforce CBOM accuracy, vendor compliance, and budget allocation.
- Integration with ERM: PQC migration embedded into enterprise risk management frameworks, with quantum exposure listed as a top-tier systemic risk.
- Escalation Protocols: Vendor non-compliance or internal delays must trigger immediate escalation to the board.
- Reporting Cadence: PQC migration status should be a standing agenda item in quarterly board sessions.

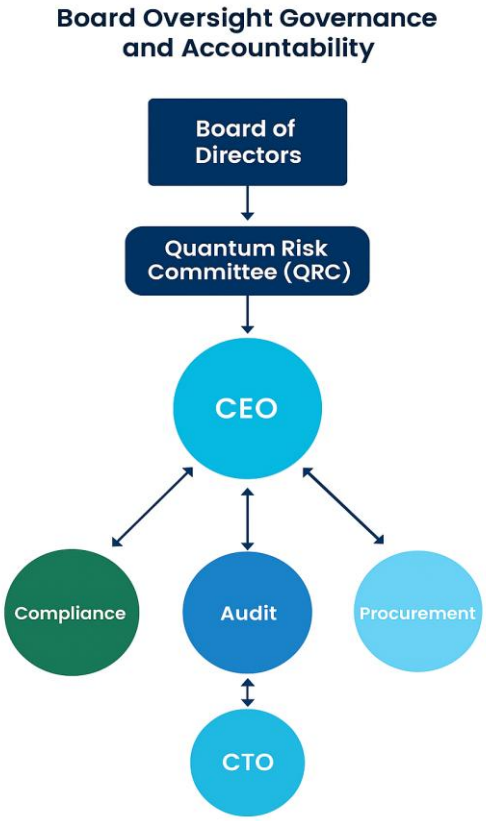

Figure 18-Governance Architecture Map.

Board owns the mandate. QRC enforces. Compliance, audit, procurement, and ERM form the escalation spine.

8.2 Regulatory and Strategic References

The urgency of PQC transition is dictated by authoritative global bodies and industry benchmarks. These documents set the standard for due diligence.
NIST:
Cybersecurity White Paper (CSWP): Defines the quantum threat and mandates cryptographic agility.
FIPS 203, 204, 205: Final standards for ML-KEM (CRYSTALS-Kyber) and ML-DSA (CRYSTALS-Dilithium).
NSA:
CNSA Suite 2.0: Explicit PQC transition timeline for national security systems.
ENISA:
Quantum-Safe Cryptography Guidance: Regulatory backing for European entities.
Industry Benchmarks:
TCG Survey: Hardware readiness, secure boot, PQC integration into supply chains.
EFR Financial Services Paper: Financial sector risks, data longevity, sovereignty penalties.
NIST FIPS Finalisation Timeline (August 2024): Draft to final standards in under two years. Delay is indefensible. ((NIST) N. I., Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, 2021)

8.3 Compliance Integration

Quantum risk is a compliance failure. PQC migration must be mapped directly to regulatory obligations.
Examples:
GDPR and HIPAA: Long-lived personal and health data must be re-encrypted with PQC. Current non-resilience is breach risk.
Financial Regulations: PQC mandates integrated into operational risk and IT audit frameworks.
ISO 27001, ENISA, NIST: PQC controls embedded into certification, monitoring, and audit cycles.
Mandate: Compliance teams must document quantum exposure and embed PQC controls into frameworks. Failure to act may be regulatory negligence. (Union, 2016)

8.4 Strategic Intelligence Caveat (SITG)

Boards should operate under a high-urgency caveat derived from strategic intelligence. The public timeline is not the real timeline.
Caveat:

- Nation-states are pursuing cryptographic dominance through undisclosed breakthroughs.
- Public timelines from commercial labs are irrelevant.
- Opaque state programmes accelerate the effective risk horizon.

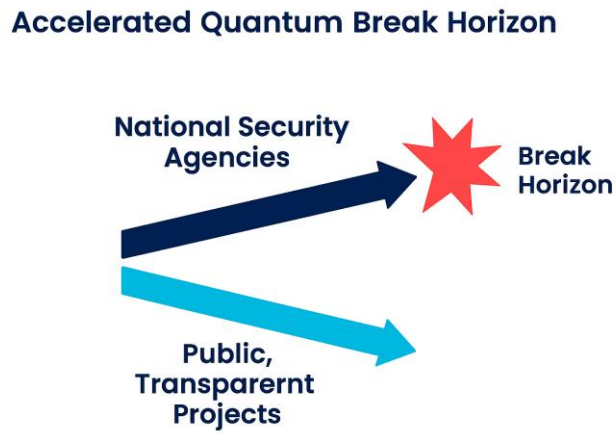

Figure 19-Accelerated Quantum Break Horizon.

Public projections lag behind classified timelines. Real risk is earlier, silent, and geopolitically driven.

Mandate: Treat NIST deadlines as the latest acceptable date for implementation testing. Budgets and migration timelines must be accelerated. Failure to factor opaque breakthroughs into planning may constitute breach of due diligence ((NIST) N. S., 2022–2023).

8.5 Audit and Enforcement

Audit is the independent validation of posture and progress. Liability may be personal.
Requirements:

- Quarterly CBOM Audits: Independent validation of CBOM accuracy and completeness.
- Vendor SLA Compliance Reports: PQC readiness declared, enforced contractually, and tracked.
- Independent Algorithm Review: External validation of PQC algorithm selection and implementation integrity, including side-channel resilience and downgrade prevention.
- Board Reporting Packs: PQC milestones and KPIs included in quarterly board materials.

Mandate: Audit must be forensic, independent, and board-facing. Underfunding or delay may be a breach of fiduciary duty ((IEC), 2013 (latest revision reaffirmed 2022)).

8.6 The Quantum Readiness Maturity Model (QRMM)

Quantum-resistant cryptography requires a multi-year migration program. It is not a single project. Boards should manage fiduciary duty using a diagnostic framework that measures progress against the timeline constraint.
The Quantum Readiness Maturity Model (QRMM) provides this framework. It maps the progression from denial to resilience. Most organisations are in the Unprepared or Aware stages. These stages carry unmanaged liability and exposure to the Harvest Now, Decrypt Later threat.
Boards should approve the budget and governance structure required to reach the Invested stage within the next fiscal year. This includes detailed CBOM remediation and multi-year funding.

Mandate: Approve budget and governance structure to reach the Invested stage within 12 months (Mosca, 2018).
KPI: Track quarterly the percentage of critical systems migrating from Aware to Mitigated.

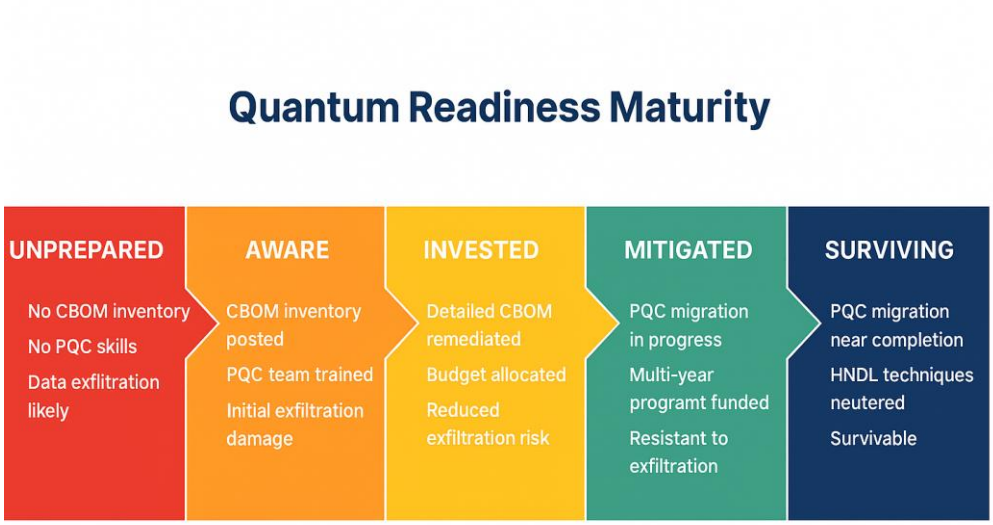

Figure 20-Quantum Readiness Maturity.

Five stages from unprepared to surviving. CBOM, budget, and migration define the path.

8.7 Vendor Dependencies and Supply Chain Cryptographic Risk

Quantum-resistant cryptography cannot be delegated. Vendor readiness does not equal organisational readiness. Vendors cannot reduce migration time (X) or data shelf life (Y) in Mosca's Theorem. These variables are internal. Waiting for vendors may be viewed as a breach of fiduciary duty.

8.7.1 Vendor Readiness ≠ Organisational Readiness

Security depends on a chain of trust. A vendor becoming PQC-ready only addresses the cryptographic primitives within their product. It does not address:

- Internal Inventory: Vendors cannot discover or remediate Shadow Crypto or hard-coded algorithms deployed years ago.
- Data Lifespan (Y): Vendors cannot reduce the mandated confidentiality period of regulated or long-lived data such as medical records or proprietary research.
- Migration Time (X): Vendors can only control their patch schedule, not the multi-year process required to deploy, test, and integrate patches across dependent internal systems and APIs.

8.7.2 Vendors Cannot Reduce Risk Variables

Mosca's Theorem $X+Y>Z$ governs solvency exposure. Vendors cannot solve this inequality:

- Vendors cannot reduce X (Migration Time). Deployment and integration across the enterprise ecosystem is a client responsibility.
- Vendors cannot reduce Y (Data Confidentiality Time). This is dictated by regulation, legal requirements, and business strategy.
- If is true, data loss is mathematically guaranteed regardless of vendor updates.

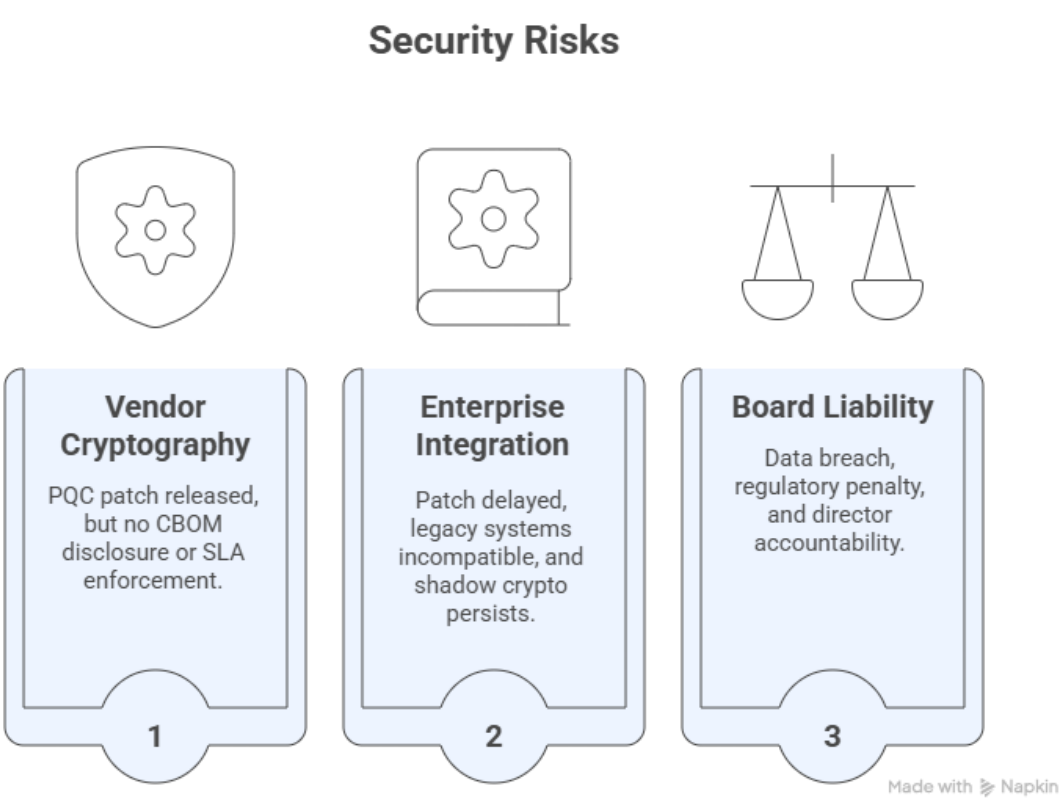

Figure 21-Security Risk Layers.

Vendor gaps, integration delays, and board liability. Each layer compounds quantum exposure.

8.7.3 Supply-Chain Crypto: The Blind Spot

Cryptographic security is embedded within APIs, dependencies, and external services. This supply-chain crypto is the largest blind spot:

- No Visibility: Without a CBOM that includes third-party dependencies, organisations have no visibility into quantum vulnerability of critical functions.

- Implied Liability: If a vendor component fails under quantum attack, their non-compliance becomes the organisation's regulatory liability. Waiting for vendors is fiduciary breach ((ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021).

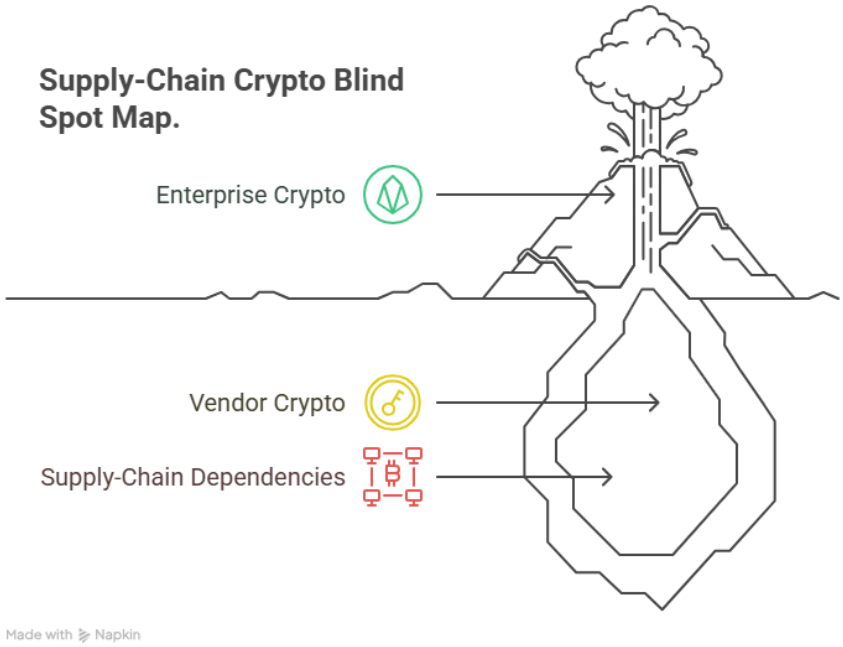

Figure 22-Supply-Chain Crypto Blind Spot Map.

Enterprise crypto is visible. Vendor and supply-chain layers remain buried. CBOM must surface all three.

8.7.4 Board Mandate: Crypto Disclosure Requirement

Boards should close this blind spot with a formal vendor requirement:

- Mandate: All critical technology vendors must provide cryptographic disclosure detailing their transition timeline, PQC algorithms selected, and a supply-chain CBOM for product dependencies.
- This positions the organisation to actively manage migration time (X) and moves it from Unprepared to Aware or Invested stages of the QRMM.
- It makes the Quantum Readiness Check essential for vendor due diligence and contract negotiation.

8.7.5 Strategic Imperative

Vendor cryptography is external liability. Boards should treat it as solvency exposure. Vendor readiness does not equal organisational survival. Delay guarantees failure.

8.8 Mandate

Governance is survival. Boards should own the risk, enforce migration, integrate compliance, and validate execution. Delegation may mean failure. Delay increases organisational liability exposure. Failure to act may be a breach of fiduciary duty with solvency consequences ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).

9. Rebuttal Section: Dismantling Organizational Inertia

This section addresses misconceptions used to justify delay, underfunding, or inaction. These arguments reflect a failure to differentiate between algorithm types and are mapped directly to board-level financial and legal exposure.

9.1 The Symmetric vs. Asymmetric Reality

The most common internal myth is that the problem is contained or already solved, creating a Quantum Decryption Chasm between perceived and actual risk.
Myth: AES-256 is quantum resilient, so migration is premature.
Rebuttal: AES-256 survives Grover's Algorithm with reduced security margin. The core danger is the asymmetric collapse of RSA and ECC under Shor's Algorithm. If the asymmetric key exchange fails, the symmetric session key is compromised. The Root of Trust (PKI) fails first.
Mandate: Boards should mandate the distinction between symmetric survivability and asymmetric collapse. PQC migration targets asymmetric cryptography. Symmetric upgrades alone are insufficient if the foundation has failed. (Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, 1994)

9.2 TLS and Protocol Vulnerabilities

Organizations often mistake protocol configuration changes for cryptographic agility, assuming TLS updates contain the threat.
Myth: TLS 1.3 ephemeral keys or routine TLS upgrades will solve quantum risk.
Rebuttal: TLS is a protocol wrapper, not a cryptographic solution. If the underlying key exchange or signature algorithm is quantum vulnerable, TLS offers no protection. Data captured today remains vulnerable. Hybrid TLS modes are a temporary bridge.
Mandate: Mandate: Protocol upgrades must include PQC primitives (ML-KEM, ML-DSA) in hybrid configuration. Relying on legacy TLS is a failure to meet the standard of care ((IETF), 2018).

9.3 PQC Adoption Challenges

Arguments about instability or cost attempt to subordinate solvency risk to budgetary convenience.
Myth: PQC is too new, unstable, or untested. We should wait for vendor maturity.
Rebuttal: Technical maturity is proven. NIST has finalized FIPS 203, 204, 205. NSA has published CNSA 2.0. ENISA has issued governance guidance. TCG and EFR have benchmarked readiness. The "waiting for standards" excuse is eliminated.
Mandate: Boards should treat PQC as production ready. Migration delays are strategic negligence and a decision to prioritize short-term cost savings over long-term data solvency ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).

9.4 The "Wait and See" Fallacy

Inertia is the greatest multiplier of quantum liability.
Myth: We can wait for clearer timelines, market adoption, or for the CRQC to be closer.
Rebuttal: This posture may be a breach of fiduciary duty. Nation states are accelerating opaque quantum programmes. Every day of delay increases the X factor in Mosca's Theorem (X + Y > Z) and maximizes exposure to the HNDL threat. The cost of delay compounds exponentially.

Mandate: Migration must begin now, led by the CEO and Board. Inaction based on the “Wait and See” fallacy may be used as evidence of negligence and recklessness in future litigation (Mosca, 2018).

10. Legal and Compliance Implications: The Liability Bridge

In the quantum era the gap between cryptographic failure and legal liability is eliminated. The Board should recognize that failure to initiate mandated PQC migration may constitute a breach of fiduciary duty, exposes the organization to punitive regulatory penalties, and triggers personal liability for directors and officers.

10.1 Breach of Fiduciary Duty: Foreseeable Harm

The central legal risk is the foreseeability of the quantum threat. Directors are required to act with the care that an ordinarily prudent person would exercise. Given public guidance from NIST, NSA, and ENISA, PQC failure is no longer a Black Swan event; may become a predictable outcome of inaction ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022).
Fiduciary Failure Triggers:

- Failure of Oversight: Not establishing the Quantum Risk Committee (QRC) and neglecting its mandates (see Chapter 8).
- Information Ignorance: Dismissing or downplaying the findings of this White Paper or the timelines set by NSA CNSA 2.0.
- Misallocation of Capital: Treating PQC migration as a discretionary IT cost instead of a mandatory solvency expenditure.
- Documented Inaction: If the Board receives evidence of the HNDL threat and fails to initiate the CBOM project within six months it may establish a record of negligence and recklessness.
- Board Minutes: Failure to record PQC migration as a standing agenda item in board minutes may constitute evidence of negligence.

10.2 Regulatory Enforcement and Penalties

Global data protection laws require state of the art security. Since PQC standards are finalized (FIPS 203, 204, 205), classical cryptography no longer meets this requirement for long lived data, potentially creating regulatory penalty exposure ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).
Key Regulatory Intersections:

- GDPR: Long lived personal data encrypted with RSA or ECC is at risk of future unauthorized decryption. This may violate GDPR's mandate to secure data against unauthorized processing and exposure.
- HIPAA and HITECH: Health data in transit and at rest should be quantum resilient to avoid penalties for exposure of Protected Health Information.
- Data Sovereignty Laws: Failure to secure data against capture by foreign state actors undermines national security and regulatory control over data residency.
- Financial Regulators: Basel Committee (BCBS239), EBA Operational Resilience Guidelines, and SEC mandates require operational resilience. PQC migration is a reasonable measure to meet evolving operational resilience expectations under current regulatory frameworks.

10.3 The Emergence of Cyber Liability Law

Legal consensus points to the Board's role in cybersecurity governance as non-delegable. This reinforces the governance model defined in Chapter 8.
Key Legal Precedents and Trends:

- SEC Cybersecurity Disclosure Rules (U.S.): Mandate timely, accurate disclosure of material cybersecurity incidents. A quantum breach involving HNDL decryption would be material and require immediate disclosure.
- Director and Officer Liability: Claims against D&O insurance increasingly cover negligent oversight related to cyber preparedness. Inaction on PQC may provide plaintiffs with a clear path to proving negligence ((SEC), Cybersecurity Disclosure Rules, 2023).
- Contractual Enforcement: Legal should enforce PQC compliance clauses in all vendor and supply chain contracts. Failure to do so makes the company liable for vendor negligence.
- Insurance Exclusions: Cyber insurance exclusions increasingly omit quantum risk. Boards cannot rely on insurance as mitigation.

10.4 Investor and Class Action Liability

Beyond regulatory fines a quantum breach creates immediate litigation exposure and shareholder risk.

Litigation Gaps:

- Shareholder Derivative Suits: Failure to protect corporate assets against a standardized threat provides grounds for shareholders to sue the Board directly for mismanagement.
- Class Action Risk: The HNDL threat, the mass decryption of captured PII, will trigger class action lawsuits worldwide due to the scale of exposure.
- Stock Exchange Liability: Investor reporting mandates require disclosure of material risks. Under the SITG Caveat, failure to act on PQC risk could lead to enforcement actions by exchanges or regulators.
- Securities Fraud Exposure: Failure to disclose PQC risk in investor filings may constitute securities fraud under SEC and exchange rules ((SEC), Regulation S-K: Disclosure of Material Cybersecurity Risks, 2023).

10.5 Strategic Legal Mandates

General counsel should convert technical risk into legal preparedness.

- Formal Risk Assessment: Legal should assess exposure of all data sets classified as having long term secrecy requirements (high Y factor in Mosca's Theorem).
- Contractual Hardening: All new contracts must include PQC compliance clauses referencing NIST FIPS 203, 204, 205 and NSA CNSA 2.0.
- Personal Liability Review: Conduct confidential review of director and officer liability concerning PQC inaction, using this White Paper as the documented standard of care.
- Regulator Engagement: General counsel should proactively brief regulators, demonstrating PQC migration plans to mitigate enforcement risk.
- Audit Linkage: Legal mandates must be integrated into CBOM audits and board reporting packs to ensure enforceability.

Mandate: Legal and Compliance should integrate PQC into control frameworks and audit cycles ((ENISA), Study on Cryptographic Agility and Migration, 2021). The cost of migration is minimal compared to punitive fines and personal liability arising from a quantum breach.

11. Strategic Survival KPIs: Measuring Solvency, Not Activity

These are Solvency KPIs. They measure whether the Board has discharged fiduciary duty in the face of existential risk. They are auditable, binary, and escalation ready. Quarterly review by the Quantum Risk Committee (QRC) is mandatory.

Figure 23-Strategic Survival KPIs – Dashboard.

CBOM, roadmap, and governance define solvency. Red zone breaches trigger QRC escalation under Section 11.4.

11.1 Visibility and Audibility (CBOM Focus)

Visibility is the prerequisite for solvency. If the Board cannot see cryptographic exposure, it cannot survive it ((TCG), 2021).

- CBOM Completion Score

Definition: Percentage of Tier 1 systems with a Cryptographic Bill of Materials that is 100% accurate and dynamically updated.
Target: 95% within 12 months.
Audit Evidence: Weekly CBOM scan reports, date stamped inventories, audit logs proving no manual overrides.
Red Flag: Score below 80% for two consecutive quarters.

- Shadow Crypto Discovery Rate

Definition: Number of undocumented cryptographic instances discovered and remediated per quarter.
Target: Continuous discovery and remediation.
Audit Evidence: Inventory of self-signed certificates, hardcoded keys, custom crypto libraries.
Red Flag: Discovery rate drops to zero.

- Risk Prioritization Accuracy

Definition: Percentage of vulnerable assets correctly ranked by Mosca's Theorem (Y factor).

Target: 99% accuracy.
Audit Evidence: Third party validation of classification lifecycle.
Red Flag: Misclassification of any high value IP or PII with Y > 10 years.

11.2 Mitigation and Deployment (Roadmap Focus)

Execution against the migration roadmap is the measure of solvency. Delay is liability ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).

- HNDL Remediation Rate

Definition: Percentage of high value, long lived data sets re encrypted using PQC hybrid algorithms.
Target: 90% within 24 months.
Audit Evidence: Database records showing dual encryption status, Y factor reduction reports.
Red Flag: Remediation rate falls below roadmap trajectory.

- PKI Agility Score

Definition: Percentage of PKI components migrated to PQC hybrid.
Target: 100% within 18 months.
Audit Evidence: Certificate Transparency logs, internal CA adoption reports.
Red Flag: Any critical service still using RSA or ECC after 12 months.

- Test Lab Readiness

Definition: PQC test environment fully operational and simulating PQC load and latency.
Target: 100% within 6 months.
Audit Evidence: Load testing reports, hardware sign offs, latency metrics.
Red Flag: Test environment unavailable after 6 months.

11.3 Governance and Enforcement (QRC Focus)

Governance is survival architecture. Funding and compliance are non-negotiable ((ENISA), Study on Cryptographic Agility and Migration, 2021).

- Funding Adherence Index

Definition: Actual spending versus mandated Solvency Expenditure.
Target: 100% adherence.
Audit Evidence: Independent financial audit of PQC budget line item, CFO variance reports.
Red Flag: Any executive decision to cut, pause, or reallocate PQC expenditure.

- Vendor Compliance Rate

Definition: Percentage of Tier 1 vendor contracts with enforceable PQC clauses referencing NIST FIPS standards.
Target: 95% within 18 months.
Audit Evidence: Legal review of contracts, QRC sign off on vendor roadmaps.
Red Flag: Refusal by any critical vendor to provide a PQC compliance roadmap.

- Fiduciary Mandate Compliance

Definition: Quarterly rating (Green, Yellow, Red) by QRC on Board adherence to PQC resolutions.
Target: Continuous Green.
Audit Evidence: Board minutes recording QRC approvals, audit logs of board action.
Red Flag: Yellow or Red for two consecutive quarters.

11.4 Board Directive: Accountability Mandate

Failure to meet the targets defined in Sections 11.1 through 11.3 is not a technical delay. It may be a failure of governance (Mosca, 2018). These KPIs are the Board's final line of defence.
The Quantum Risk Committee (QRC) is mandated to:

- Report Escalations: Any Red Flag condition must be reported directly to the CEO and Chairperson.
- Trigger Intervention: Escalation triggers immediate executive intervention, with corrective action logged in board minutes.
- Leadership Accountability: Chronic non-performance against solvency KPIs may constitute grounds for leadership replacement.
- Fiduciary Enforcement: The QRC should document all escalations as evidence of fiduciary compliance, ensuring liability transfer is explicit and defensible.

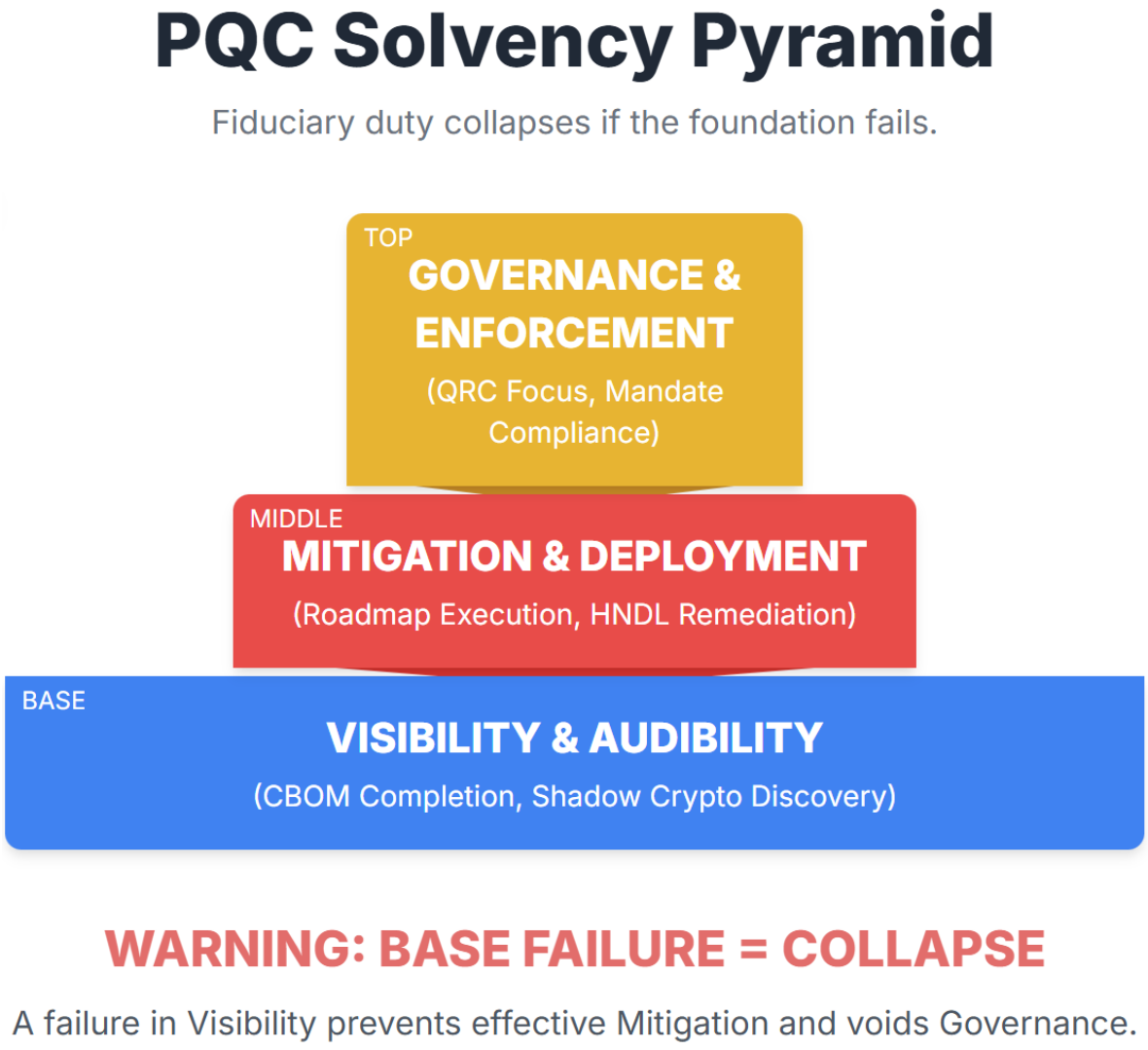

Figure 24-PQC Solvency Pyramid.

Visibility enables mitigation. Mitigation enables governance. Board duty collapses if the base fails.

12. Future-Proofing: The Next Cryptographic Generation

The PQC transition is the first mandatory step toward permanent Q-Resilience. Boards should shift from fixing a single failure (RSA/ECC) to building an architecture that anticipates and survives future cryptographic failure.

12.1 Cryptographic Agility Architecture

Cryptographic agility is the ability to replace and adapt cryptographic algorithms across protocols, applications, hardware, and infrastructures without disruption ((ENISA), Study on Cryptographic Agility and Migration, 2021).
Core Principles:

- Abstraction Layers: Encapsulate cryptographic calls within dedicated modules or services, isolating them from business logic.
- Centralized Policy: Enforce algorithm selection from a single control plane.
- Metadata Integration: Generate algorithm and key metadata for CBOM inclusion and audit traceability.

12.2 The Q-Resilience Mindset

Quantum resilience is a strategic mindset embedded in corporate culture.
Elements:

- Assume Failure: All cryptography is temporary.
- Minimize Data Lifetime: Reduce the Y variable in Mosca's Theorem through strict retention policies.
- Mandate Agility: Systems without cryptographic agility are security debt requiring remediation (Mosca, 2018).

12.3 Quantum Key Distribution (QKD) Caveat

QKD is an optical key exchange technology with limited scope.
Assessment:

- Limited Scope: Photon loss restricts reliable operation and requires specialized fibre or satellite links.
- No General Solution: QKD does not secure data at rest or support common protocols such as TLS.
- Strategic Research: QKD may support high-value transmission but cannot delay PQC migration ((NIST) N. I., Quantum Key Distribution (QKD) and Post-Quantum Cryptography, 2020).

12.4 Quantum Incident Response Plan (Q-IRP)

The PQC migration must conclude with a formal Q-IRP anticipating an unannounced quantum break.
Components:

- Decryption Contingency: Identify and protect data decrypted post-breach.
- PKI Revocation: Predefined procedures for global certificate revocation and re-issuance.
- Forensic Protocol: Analyse logs and metadata to determine breach scope.

Mandate: The Q-IRP must be drafted and tested by the end of the Five-Phase Migration Roadmap ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022).

12.5 Strategic Continuity Mandate

Cryptographic agility is a permanent governance function ((ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021).
Requirements:

- Horizon Watchlist: Monitor lattice cryptanalysis, side-channel risks, AI-accelerated cryptanalysis, and next-generation primitives.
- Strategic Intelligence Integration: Feed horizon data into board briefings and vendor contracts.
- Survival Architecture Extension: Extend the PQC Solvency Pyramid to include Cryptographic Horizon Intelligence.
- Funding Mandate: Allocate budget for cryptographic R&D and maintain test environments for emerging standards.

12.6 Anticipating the Emergent

Boards should prepare for primitives not yet conceived (Mosca, 2018).
Domains:

- Post-Lattice Breakthroughs: Prepare for code-based, multivariate, isogeny-based, or new constructs.
- AI and Quantum Hybrid Attacks: Anticipate adversaries combining quantum computing with AI.
- Entropy Collapse: Diversify entropy pools and mandate continuous audits.
- Blockchain Risks: Address PQC migration for smart contracts, Layer 2 protocols, and dormant assets.

12.7 Board Call to Action

- Approve QRC mandate to track post-PQC threats quarterly.
- Enforce future-proofing clauses in vendor contracts.
- Fund cryptographic R&D and sandboxing of unstandardized primitives.
- Treat cryptographic obsolescence, including what is not yet invented, as potential fiduciary risk ((NIST) N. I., Post-Quantum Cryptography Standardization Project — Round 4 and Beyond, 2024).

The Perpetual Solvency Pyramid

A resilient architecture against threats known and unknown.

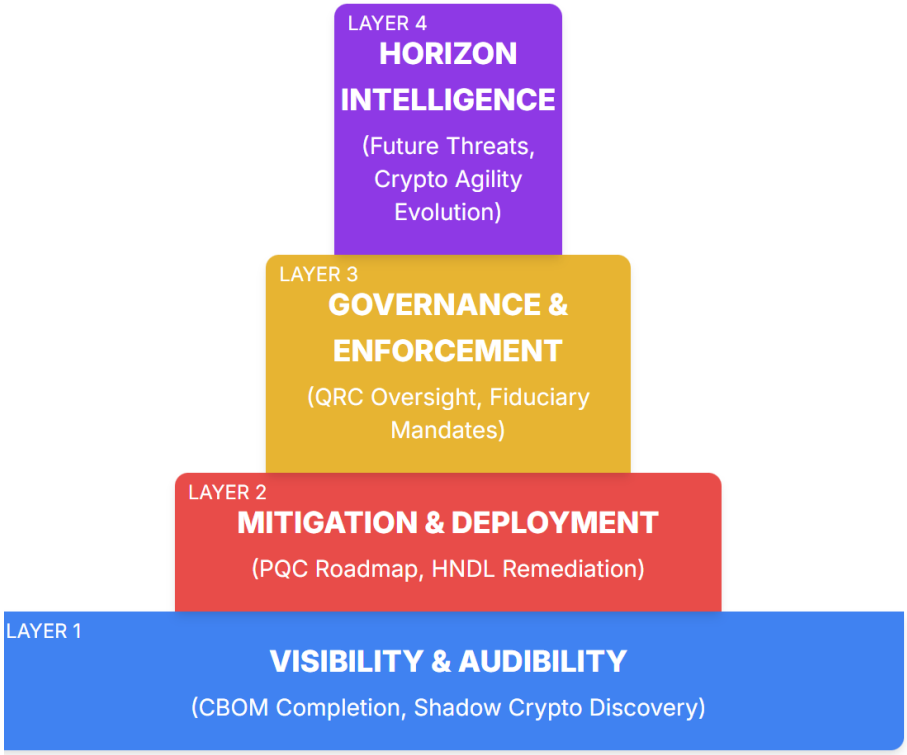

Figure 25-Perpetual Solvency Pyramid.

Visibility, mitigation, governance, and horizon intelligence. Resilience demands all four—continuously.

13. Case Studies: Systemic Failure Pattern Overview

Boards often dismiss quantum risk as speculative physics. History shows it is a recurring governance failure. The pattern is documented, predictable, and forensic: visibility failures, delayed decryption, solvency expenditures, and migration inertia. Across industries and decades, delayed action repeatedly converts a technical issue into a solvency liability.

These case studies follow the structure **Context → Failure → Impact → Board Lesson**, and the iceberg model below visualises the systemic risks they share.

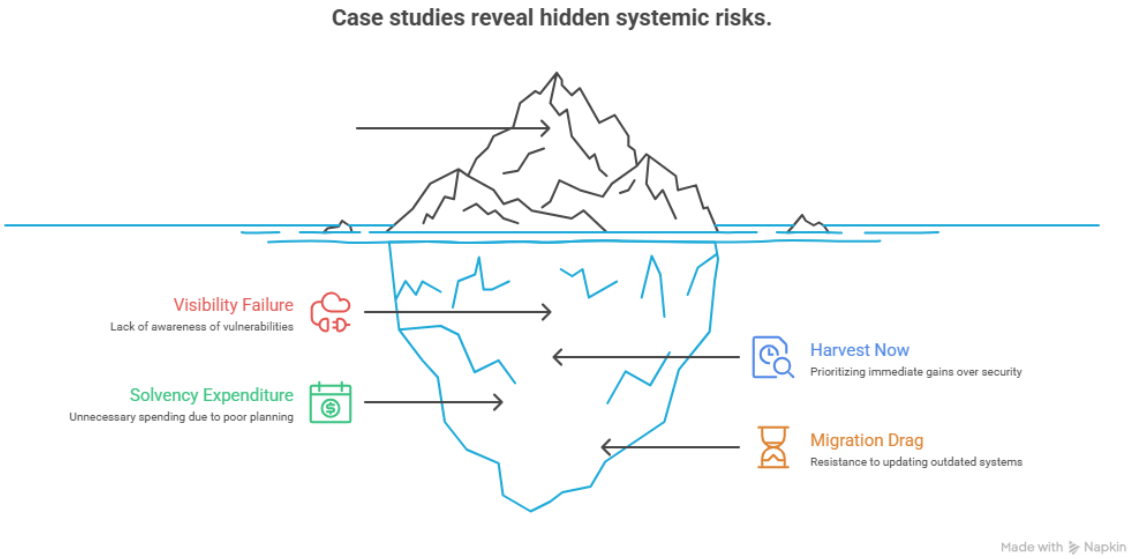

Figure 26-Systemic Risk Iceberg.

Case studies expose hidden risks: visibility failure, solvency waste, migration drag, and HNDL exposure.

The four elements of the iceberg map directly to the historical precedents examined in this chapter:

Visibility Failure (Equifax)
Context: Lack of cryptographic visibility.
Failure: Blind inventory and expired inspection certificate.
Impact: $1.38B solvency loss and 76 days of undetected exfiltration.
Board Lesson: You cannot govern what you cannot see.

Harvest Now (VENONA)
Context: Encrypted data harvested during geopolitical conflict.
Failure: Implementation weakness in one-time pads.
Impact: Retroactive decryption of decades-old secrets.
Board Lesson: Stored ciphertext is always at risk of future decryption.

Solvency Expenditure (Y2K)
Context: Legacy architecture with date dependencies.
Failure: Late remediation leading to a global scramble.
Impact: $300B+ emergency spend to avert systemic collapse.
Board Lesson: Early expenditure is solvency protection; delay multiplies cost.

Migration Drag (SHA-1)
Context: Deprecation warning issued years before exploit.

Failure: Industry-wide inertia and hard-coded dependencies.
Impact: 12-year delay culminating in real collision attacks.
Board Lesson: Migration always takes longer than predicted; delay guarantees exposure.

Together, these precedents reveal that cryptographic failures are not technology failures they are governance failures. Each one demonstrates the same pattern: delayed action converts predictable technical degradation into solvency damage.

The next sections provide detailed analysis of each precedent and its direct analogue to quantum-era risk.

13.1 Case Study A: The Solvency Failure (Equifax, 2017)

Analog: Failure of Visibility (CBOM) and Fiduciary Duty
Event: In 2017, a digital certificate on a network traffic inspection device expired. For 76 days, encrypted traffic left the network uninspected because the tool could not decrypt it.
Cost: $1.38 billion in remediation, fines, and settlements
Forensic Link to Quantum Risk: Equifax suffered from certificate blindness, the same state most enterprises face today with PQC inventory. The breach was not caused by a quantum computer but by a lack of visibility.
Forced Expiration Parallel: Just as the Equifax certificate expired unnoticed, quantum computing will cause the invalidation of security guarantees upon CRQC availability. Without a CBOM, boards will be blind to this expiration until after data is exfiltrated.
Mosca's Theorem Application: The time to discover the failure (X) was 76 days. The data required secrecy (Y) for a lifetime. The vulnerability (Z) was immediate. Because X > Z, solvency was impacted.
Lesson: You cannot secure what you cannot see ((GAO) U. G., 2018). A missing CBOM is a solvency risk today, not only in the quantum future.

13.2 Case Study B: The "Harvest Now" Reality (Project VENONA, 1943–1980)

Analog: Proof that Harvest Now, Decrypt Later (HNDL) is standard tradecraft
Event: During WWII, U.S. and British intelligence harvested thousands of encrypted Soviet diplomatic cables. At the time, they were secured by one-time pads, considered mathematically unbreakable.
Decryption Event: The cables were captured in the 1940s and stored. Years later, cryptanalysts discovered a flaw in pad generation. Over 37 years, the NSA decrypted these messages, exposing atomic spies and espionage networks.
Warning for Boards: HNDL is not theory, it is history.
Retroactive Decryption: Data encrypted today with RSA-2048 is being harvested. When Shor's Algorithm is applied, decryption will be retroactive, as it was with VENONA ((NSA), VENONA: Soviet Espionage and the American Response 1939–1957, 1996).
Implementation Risk: VENONA failed due to implementation, not mathematics. PQC adoption faces the same risk through side-channel attacks. This validates the need for crypto-agility, the ability to swap algorithms instantly if a flaw is discovered.
Strategic Implication: The shelf-life of your data (Y) defines your risk. If you hold data for more than ten years, it is likely already compromised if you are not using PQC.

13.3 Case Study C: The Cost of Readiness (Y2K, 1999)

Analog: The solvency expenditure model versus the hoax myth

Event: The Year 2000 bug threatened to crash global financial and infrastructure systems due to a legacy code formatting error.
Spend: Global organisations spent Hundreds of billions globally (commonly cited in the $300–600B range) on remediation.
Solvency Lesson: Critics cite Y2K as a hoax because planes did not fall out of the sky. This is survivor bias. Systems survived because boards unlocked billions in funding to remediate code before the deadline.
10x Premium Reality: Y2K had a fixed deadline (Z). Quantum has an unknown deadline. Banks that funded remediation in 1996 paid standard rates. Organisations that waited scrambled in late 1999, paying ten times the premium for contractors.
Lesson: The cost of migration is high, but the cost of panic is higher. PQC migration is the Y2K of the 21st century, but with no fixed date to force action. Spending now is solvency insurance. Spending later is a distress purchase ((GAO) U. G., 1999).

13.4 Case Study D: The "Crypto-Agility" Drag (SHA-1 to SHA-2, 2005–2017)

Analog: The reality of how long migration (X) takes
Event: In 2005, the SHA-1 hashing algorithm was theoretically broken. NIST deprecated it in 2011.
Inertia: Despite warnings, industry delayed. In 2017, Google demonstrated the SHAttered collision attack, forcing emergency migration.
Operational Reality: Migration took 12 years from theoretical risk to active exploit. Vendors, legacy hardware, and hard-coded dependencies stalled the transition.
Quantum Parallels: If PQC migration takes 12 years, and a CRQC arrives in 10, the math of survival ($X + Y < Z$) is impossible.
Lesson: Migration always takes longer than predicted ((NIST) N. I., Transitioning the Use of Cryptographic Algorithms and Key Lengths (SP 800-131A Rev. 2), 2019). Starting now is the only way to compress the timeline (X) to fit inside the risk horizon (Z).

13.5 Mandate

These precedents prove that cryptographic obsolescence and governance delay are documented solvency failures. Equifax shows the cost of missing inventory. VENONA proves HNDL is historical fact and highlights implementation risk. Y2K demonstrates that early solvency expenditure prevents catastrophe, while delay incurs a panic premium. SHA-1 proves that migration inertia is the norm. The board lesson is clear: delay may convert technical risk into fiduciary liability. PQC migration must be treated as a solvency expenditure, enforced through CBOM completion, roadmap funding, and governance mandates now ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).

14 Societal Wellbeing and ESG Risk Impacts

Retroactive decryption is an immediate ESG risk that destroys privacy and trust. Post-Quantum Cryptography migration is a fundamental fiduciary duty required to prevent long-term human harm and to preserve corporate legitimacy.

The threat of post-quantum decryption is an ESG failure with immediate social consequences. Retroactive compromise of cryptographic integrity produces direct human harm, systemic disruption, and irreversible reputational damage. Organisations that retain long-lived, sensitive encrypted data without an active, funded, and measurable Post-Quantum Cryptography migration plan are governance deficient and create material liability for shareholders and the public.

ESG Pillar	Core Quantum Risk Factor	Material Impact & Governance Outcome
Social (S)	**Mass Privacy Erosion**	The "Harvest Now, Decrypt Later" (HNDL) threat enables **irreversible privacy destruction** (health, identity, financial data). This breaches the social contract, erodes public trust, and causes widespread human harm and persistent fraud for decades.
Governance (G)	**Fiduciary Negligence**	Failure to fund and mandate Post-Quantum Cryptography (PQC) migration against a known, existential cyber threat is a fundamental **breach of fiduciary duty**. It signals **governance deficiency**, creating immense liability and inviting shareholder and regulatory action.
Environmental (E)	**Critical Infrastructure Compromise**	Retroactive exposure of secrets for complex systems (e.g., smart grids, resource management) can lead to **catastrophic physical service outages**. This may trigger localized environmental disasters or widespread disruptions to essential societal functions.

Figure 27-Quantum risk mapped to ESG pillars and material governance outcomes.

14.1 The human cost: retroactive harm

14.1.1 Harvest now, decrypt later. Adversaries can capture encrypted data today and decrypt it when quantum capability arrives. Archived data becomes a source of future irreversible harm.

14.1.2 Privacy and wellbeing. Health records, intimate medical histories, and identity data decrypted years after capture enable persistent fraud, extortion and privacy violations that cannot be undone.

14.1.3 Public safety and resilience. Retroactive exposure of infrastructure secrets, including smart grid controls and critical blueprints, can cascade into service outages, supply chain failures, and public safety incidents.

14.1.4 Equity and vulnerability. Remediation is costly and slow. People with limited resources, low digital literacy or weak legal protections will suffer disproportionately.

Key point 14.1

- Retroactive decryption converts archived data into long-term personal and public harm; prioritise health, identity, and infrastructure data now.

14.2 Post-Quantum vulnerability as a governance failure

14.2.1 Fiduciary duty. Boards should treat Post-Quantum Cryptography migration as a core fiduciary obligation. Failing to secure long-lived, sensitive encrypted data against a known quantifiable threat may be categorised as a governance failure.

14.2.2 Materiality. The social and governance impacts are material now. Organisations must classify post-quantum vulnerability as an ESG risk in risk registers and in public disclosures. The threat maps directly to the Social pillar through irreparable privacy destruction and to the Governance pillar through fiduciary negligence and lack of risk oversight.

14.2.3 Legal and financial exposure. Lack of funded migration, missing cryptographic inventories and absent executive accountability create exposure to regulatory enforcement, mandatory remediation orders, investor litigation, and personal fiduciary liability for board members.

Key point 14.2

- Post-Quantum Cryptography vulnerability is a material ESG and fiduciary risk; record it in risk registers and treat migration as non-delegable board oversight.

14.3 Priority actions and accountability

Boards should mandate and resource the following immediately.

14.3.1 Protect people first. Prioritise migration for health records, identity systems, financial data, and critical infrastructure control systems.

14.3.2 Assign executive accountability. Require Post-Quantum Cryptography resilience key performance indicators in executive performance metrics and tie non-performance to measurable consequences. Name responsible officers such as Chief Information Security Officer, Chief Information Officer, Chief Risk Officer and General Counsel.

14.3.3 Mandate transparency. Require public reporting of cryptographic inventories, migration milestones, and remediation plans so stakeholders can verify progress.

14.3.4 Embed equity. Include an equity assessment in data triage to identify and mitigate disproportionate impacts on vulnerable groups.

14.3.5 Targeted deadlines. Set board-approved deadlines: complete cryptographic inventory within 90 days; approve funded migration roadmap within 180 days; migrate top-tier high-impact data within 24 months; complete critical migrations within 48 months.

Key point 14.3

- Boards should set owners, deadlines, and funding now and require public accountability.

14.4 Operational requirements and metrics

14.4.1 Operational imperatives

- Data triage. Classify and accelerate work on data with the highest human impact.
- Auditability. Ensure cryptographic inventories and migration evidence are auditable and retained to establish a clear defence posture for regulators and stakeholders.
- Stakeholder communications. Prepare tested disclosure templates and remediation playbooks.
- Remediation planning. Design support programmes for affected individuals including identity protection and fraud remediation.

14.4.2 Required metrics

- Technical progress. Percentage of high-impact data inventories completed; percentage migrated to Post-Quantum Cryptography protections. Target: 100 percent inventory in 90 days; 60 percent migration of top-tier data in 24 months.
- Social impact. Number of remediation plans published; number of individuals or data points covered by remediation programmes. Target: remediation plans published within 30 days of confirmed exposure.
- Governance oversight. Quarterly executive scorecard on Post-Quantum Cryptography resilience KPIs, including budget, staffing and schedule adherence, with board review and executive sign-off.

Key point 14.4

- Require auditable controls and combined technical and social KPIs with quarterly signed executive reporting.

14.5 Final mandate: a duty to act.

The emergence of a cryptographically relevant quantum computer is a foreseeable governance risk with irreversible social consequences. Post-Quantum Cryptography migration should be considered a core fiduciary duty to prevent long-term human harm and to preserve organisational legitimacy. The cost of inaction is likely to exceed the cost of preparation. Boards should act now.

Board checklist

- Complete cryptographic inventory within 90 days.
- Approve funded migration roadmap within 180 days.
- Migrate top-tier high-impact data within 24 months.
- Publish remediation plans within 30 days of confirmed exposure.
- Require quarterly board review with executive sign-off.
- Publish an annual ESG disclosure on post-quantum risk and progress.

15. Conclusion and board call to action

The Quantum Security Gap is a present solvency and governance crisis. Shor's algorithm establishes the mathematical threat. First-wave NIST standards are finalised, and enterprise solutions exist. The Harvest Now, Decrypt Later attack and fragmented global harmonisation make delay may be considered negligent.
This is an ESG failure. Unchecked quantum vulnerability destroys privacy and trust and may constitute a non-delegable breach of fiduciary duty.

Board directives - mandatory and time bound.

Directive	⏳ Requirement / Deadline	👑 Owner	🚦 RAG Status
Complete Cryptographic Bill of Materials (CBOM)	Must be finalized within 90 days.	CISO	🟠
Approve PQC Migration Roadmap	Funded roadmap approval required within 180 days.	CEO & CFO	🟠
Migrate High-Impact Data	Execute migration of top-tier data within 24 months.	CIO	🔴
Publish Auditable Quarterly Progress	Require auditable evidence and quarterly progress publication.	CRO	🟢
Mandate PQC Resilience KPIs	Attach measurable financial consequences for non-performance.	Remuneration Committee	🟢
Embed Equity & Remediation Plan	Publish templates within 30 days of any confirmed exposure.	General Counsel (GC)	🟠
Integrate PQC Risk into ESG Disclosure	Include risk and progress in the organization's annual ESG disclosure.	Head of Sustainability	🟢

Figure 28-PQC Governance Check List

15.1 Survival framing: inaction as negligence defined.

This White Paper establishes the PQC transition as fundamental corporate survival. Any decision to delay, underfund, or delegate responsibility converts a technical risk into legal and financial liability.

- Fiduciary duty breach: Documented ignorance or non-adoption of established PQC standards and guidance may create foreseeable harm and personal liability exposure for Directors and Officers.
- Solvency collapse:

$$X + Y > Z$$

- When the time data must remain secure plus the time to migrate exceeds the time to a cryptographically relevant quantum computer, long-lived data loss is guaranteed under Harvest Now, Decrypt Later.
- Regulatory exposure: Reliance on quantum-vulnerable algorithms for long-lived PII may violate state-of-the-art security expectations and triggers punitive enforcement.
- Governance failure: Chronic underfunding and lack of QRC oversight prevents accurate tracking of Survival KPIs and masks unmanaged, material risk.
- Irrefutable negligence threshold:
- CBOM initiation: Failure to authorize and begin the Cryptographic Bill of Materials project within six months of this report may constitute reckless disregard ((NSA), Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022)in the event of a quantum cryptographic breach.

15.2 Perpetual Q-Resilience: the mandate for architecture

The immediate PQC migration is Phase 5 within a larger strategic transformation. The objective is a Perpetual Q-Resilience architecture that eliminates cryptographic lock-in and survives future, unknown breakthroughs. The Four-Layer Solvency Pyramid defines this model. Horizon Intelligence feeds Governance. Governance enforces Mitigation. Mitigation depends on Visibility.

- Solvency expenditure imperative: PQC migration funding is a solvency expenditure, not an IT cost. It is non-discretionary, multi-year, and protected from cuts to maintain 100 percent adherence to the Funding Adherence Index. Any pause or cut accepts existential liability.
- Global standards reality: First-wave NIST standards are finalized and ready for immediate use. ML-KEM is standardized in FIPS 203. ML-DSA is standardized in FIPS 204. SLH-DSA is standardized in FIPS 205. Additional algorithms and regional profiles are in motion. CNSA 2.0 guidance continues to update adoption details. Boards should adopt now and maintain crypto-agility for second-wave additions and jurisdictional variations ((NIST) N. I., FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme, 2024).
- Architectural mandates (Phase 6+):
- Mandate cryptographic abstraction: Enforce Abstraction Layers across all system development to isolate algorithms from business logic and enable rapid replacement.
- Institutionalize the Q-Resilience mindset: Treat current cryptography as temporary. Require Cryptographic Agility in all application development and procurement.
- Finalize the Q-IRP: Draft and test the Quantum Incident Response Plan by the conclusion of the migration roadmap. Include mass PKI revocation, certificate re-issuance, archival decryption containment, and forensic protocols.
- Adopt secure code signing now: Implement hash-based signatures per NIST SP 800-208 for software and firmware signing, consistent with CNSA 2.0 posture.

15.3 Final call to action: the board’s ultimatum

Executive leadership must act now to secure enterprise longevity, meet regulatory standards, and mitigate personal liability.
((SEC), Cybersecurity Disclosure Rules, 2023) ((SEC), Regulation S-K: Disclosure of Material Cybersecurity Risks, 2023)

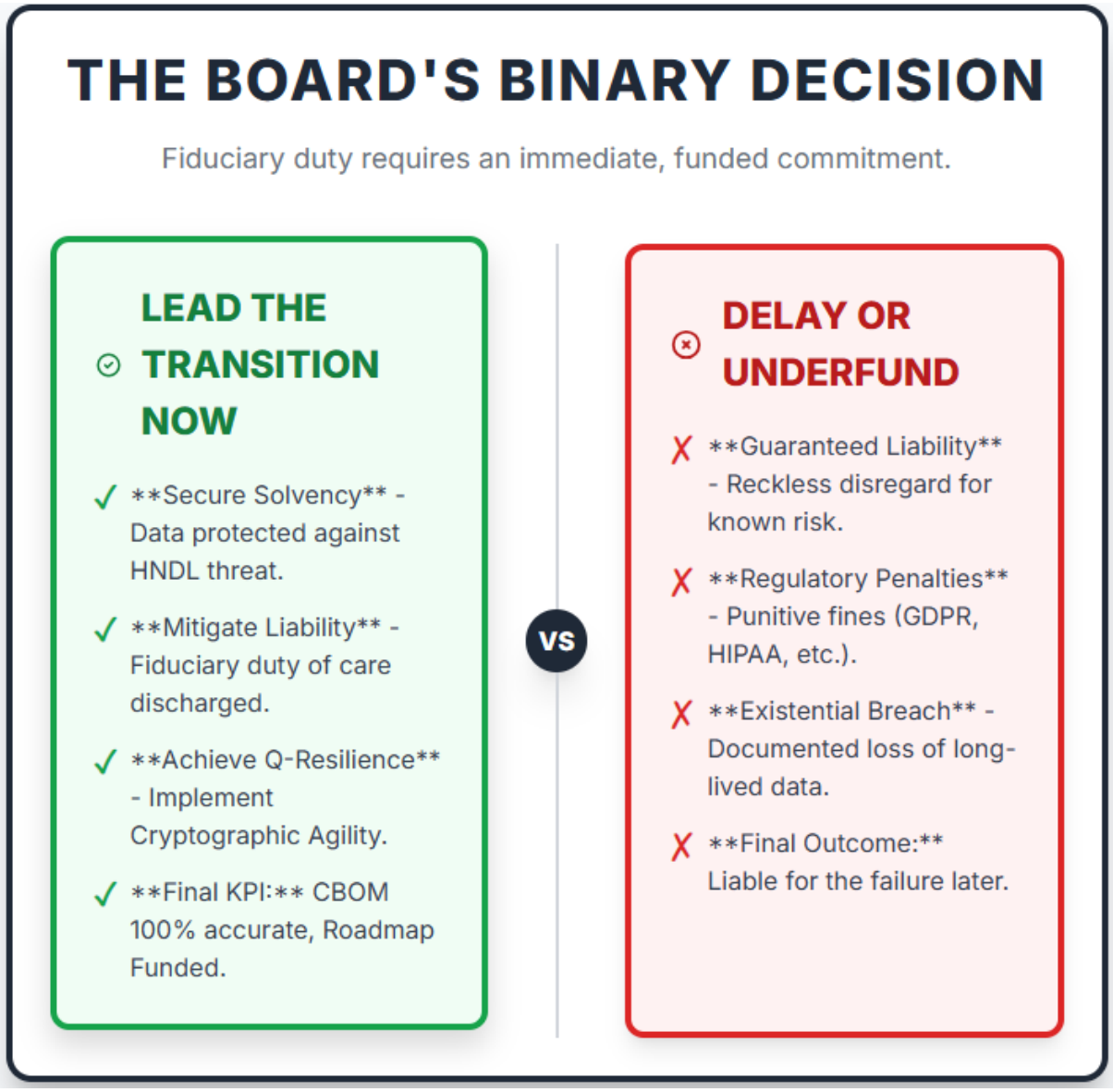

Figure 29-The Boards Binary Decision.

Lead now or delay and fail. Solvency, resilience, and fiduciary duty hinge on immediate, funded action.

- Immediate CBOM authorization: Authorize and fully fund the dynamic CBOM project immediately. CBOM completion is the binary first KPI for Visibility.
- Non-negotiable funding: Approve the dedicated, multi-year budget for the Five-Phase Migration Roadmap and forbid cuts to Solvency Expenditure.
- Empower QRC governance: Formalize and empower the Quantum Risk Committee with direct board reporting to enforce Survival KPIs and mandate aggressive vendor PQC compliance aligned to NIST FIPS and CNSA 2.0 guidance.
- Enforce architectural agility: Mandate immediate integration of Cryptographic Agility Architecture into all new and refactored systems.
- Global watch and briefings: Require quarterly board briefings on NIST PQC updates, CNSA 2.0 guidance, and international standardization status, with documented impacts on vendors, contracts, and controls.
- Vendor contract clauses: Insert obligations for crypto-agility, timelines for adopting second-wave algorithms, FIPS validation requirements, and remedies for non-compliance to avoid lock-in when regional standards diverge.

15.4 Measurable KPIs, timelines, and evidence

- CBOM coverage: 100 percent systems in scope by 30 June 2026. Shadow crypto sweeps remediated by 30 September 2026.
- PQC pilot to production: Pilot by 31 March 2026. Production rollout for high-value systems by 31 December 2026 using FIPS-approved primitives and parameter sets.
- Agility enforcement: New systems compliant immediately. Legacy refactor completed by 30 June 2027, evidenced by policy registry and metadata integration.
- Code signing posture: SP 800-208 signatures enforced for software and firmware by 31 March 2026 with audit proof.
- Q-IRP test: Full exercise completed before migration end. Evidence pack includes revocation scripts, reissue logs, decrypted-archive containment, and breach forensics.
- External alignment: KPIs aligned to recognized deprecation and migration targets through 2030 to 2035. Quarterly horizon briefings minuted with owners and actions.
- Audit artefacts required:
- Evidence packs: CBOM export, crypto policy registry, algorithm selection logs, parameter and key lifecycle records, exception register.
- Control tests: PQC performance baselines, side-channel resilience checks, entropy audits, rollback procedures.
- Q-IRP artefacts: Revocation playbooks, certificate reissue scripts, forensic workflows, breach classification criteria.
- Board reporting: KPI dashboard, Solvency Pyramid reference, risk heatmaps, action closure tracking, and attestation.

15.5 Final warning

Failure to authorize the CBOM and fund the Roadmap within six months may create a documented record of reckless disregard for a known risk. The choice is binary. Lead the transition now to secure solvency or potentially become liable for the failure later.

APPENDIX

Lexicon for Quantum Risk

Term	Definition for the Board
PQC	**Post-Quantum Cryptography.** New, quantum-resistant algorithms (e.g., Dilithium, Kyber) standardized by NIST to replace vulnerable RSA and ECC encryption.
RSA / ECC	**Rivest–Shamir–Adleman / Elliptic Curve Cryptography.** The algorithms forming the foundation of all modern digital security (PKI, TLS, VPNs). They are mathematically proven to be broken by quantum computers.
HNDL	**Harvest Now, Decrypt Later.** The current, immediate threat where encrypted data is being stolen and stored today, awaiting a cryptographically relevant quantum computer for future decryption.
Q-Day (Z)	The estimated point in time when a **Cryptographically Relevant Quantum Computer** becomes operational, capable of running Shor's Algorithm to break RSA/ECC.
Mosca's Theorem ($X + Y > Z$)	The mathematical proof that determines the true security deadline. If the time to migrate (X) plus the time data must remain confidential (Y) exceeds Q-Day (Z), data loss is guaranteed. **The deadline is $Day\ 1$ of X.**
CBOM	**Cryptographic Bill of Materials.** A comprehensive, audited inventory of every cryptographic primitive, algorithm, key, and dependency used across the enterprise, including vendor components. The first survival KPI.
Cryptographic Agility	The architectural mandate to abstract cryptographic algorithms from applications and infrastructure, allowing rapid switching (or "tuning") to new, safer algorithms in response to future threats.
Shadow Crypto	Unauthorized or unmanaged cryptographic implementations (e.g., hard-coded keys, non-standard algorithms) deployed within enterprise applications and systems, creating blind spots in the CBOM.

Bibliography

(ENISA), E. U. (2021). *Post-Quantum Cryptography: Current State and Quantum Mitigation*. Athens, Greece: ENISA. Retrieved from https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

(ENISA), E. U. (2021). *Study on Cryptographic Agility and Migration.* Athens, Greece: ENISA.

(ETSI), E. T. (2020). *Quantum-Safe Cryptography and Agility.* Sophia Antipolis, France: ETSI.

(GAO), U. G. (1999). *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*. Washington, DC: GAO. Retrieved from https://www.gao.gov/products/aimd-10.1.19

(GAO), U. G. (2018). *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. Washington, DC: GAO. Retrieved from https://www.gao.gov/products/gao-18-559

(IEC), I. O. (2013 (latest revision reaffirmed 2022)). *ISO/IEC 27001: Information Security Management Systems — Requirements.* Geneva, Switzerland: ISO/IEC. Retrieved from https://www.iso.org/standard/27001

(IETF), I. E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3.* RFC Editor.

(NIST), N. I. (2019). *Transitioning the Use of Cryptographic Algorithms and Key Lengths (SP 800-131A Rev. 2).* Gaithersburg, MD: NIST. Retrieved from https://csrc.nist.gov/pubs/sp/800/131/a/r2/final

(NIST), N. I. (2020). *Quantum Key Distribution (QKD) and Post-Quantum Cryptography.* Gaithersburg, MD: NIST. Retrieved from https://csrc.nist.gov/pubs/ir/8240/final

(NIST), N. I. (2021). *Getting Ready for Post-Quantum Cryptography (NIST Cybersecurity White Paper).* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

(NIST), N. I. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.* Gaithersburg, MD: U.S. Department of Commerce, NIST.

(NIST), N. I. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.* Gaithersburg, MD: U.S. Department of Commerce, NIST.

(NIST), N. I. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NIST IR 8413).* Gaithersburg, MD: U.S.

Department of Commerce, NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

(NIST), N. I. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NIST IR 8413).* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

(NIST), N. I. (2023). *Federal Information Processing Standards (FIPS) 203, 204, 205: Post-Quantum Cryptography Standards.* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography (official NIST PQC page)

(NIST), N. I. (2023). *Federal Information Processing Standards (FIPS) 203, 204, 205: Post-Quantum Cryptography Standards.* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

(NIST), N. I. (2023). *Recommendation for Pairing Post-Quantum Cryptography with Classical Algorithms in Hybrid Modes.* Gaithersburg, MD: U.S. Department of Commerce, NIST.

(NIST), N. I. (2024). *Federal Information Processing Standard (FIPS) 203: ML-KEM — Key Encapsulation Mechanism (CRYSTALS-Kyber).* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/pubs/fips/203/final

(NIST), N. I. (2024). *Federal Information Processing Standard (FIPS) 204: ML-DSA — Digital Signature Algorithm (CRYSTALS-Dilithium).* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/pubs/fips/204/final

(NIST), N. I. (2024). *Federal Information Processing Standard (FIPS) 205: SLH-DSA — Digital Signature Algorithm (SPHINCS+).* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/pubs/fips/205/final

(NIST), N. I. (2024). *FIPS 203: CRYSTALS-Kyber — Key Encapsulation Mechanism . FIPS 204: CRYSTALS-Dilithium — Digital Signature Scheme. FIPS 205: SPHINCS+ — Stateless Hash-Based Signature Scheme.* Gaithersburg, MD: U.S. Department of Commerce, NIST (Federal Information Processing Standards (FIPS)).

(NIST), N. I. (2024). *Post-Quantum Cryptography Standardization Project — Round 4 and Beyond.* Gaithersburg, MD: U.S. Department of Commerce, NIST. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

(NIST), N. S. (2022–2023). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) and NIST PQC Standards.* Fort Meade, MD / Gaithersburg, MD: NSA & NIST.

Retrieved from https://csrc.nist.gov/pubs/cswp/15/getting-ready-for-postquantum-cryptography/final

(NSA), N. S. (1996). *VENONA: Soviet Espionage and the American Response 1939–1957*. Fort Meade, MD: NSA.

(NSA), N. S. (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)*. Fort Meade, MD: National Security Agency. Retrieved from https://media.defense.gov/2022/Sept/CNSA-2.0.pdf (official NSA publication)

(NSA), N. S. (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)*. Fort Meade, MD: National Security Agency. Retrieved from https://media.defense.gov/2022/Sept/CNSA-2.0.pdf

(NSA), N. S. (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)*. Fort Meade, MD: National Security Agency. Retrieved from URL: https://media.defense.gov/2022/Sept/CNSA-2.0.pdf

(NSA), N. S. (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)*. Fort Meade, MD: National Security Agency.

(OECD), O. f.-o. (2019). *G20/OECD Principles of Corporate Governance*. Paris, France: OECD Publishing.

(SEC), U. S. (2023). *Cybersecurity Disclosure Rules*. Washington, DC: SEC. Retrieved from https://www.sec.gov/files/rules/final/2023/33-11216.pdf

(SEC), U. S. (2023). *Regulation S-K: Disclosure of Material Cybersecurity Risks*. Washington, DC: SEC. Retrieved from https://www.sec.gov/files/rules/final/2023/33-11216.pdf

(TCG), T. C. (2021). *TCG Guidance on Cryptographic Agility and Inventory (CBOM)*. Beaverton, OR: Trusted Computing Group.

Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)* (pp. 212–219). New York, NY: ACM.

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers. *IEEE Security & Privacy*, 38–41.

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *5th Annual Symposium on Foundations of Computer Science (FOCS)*, (pp. 124–134). Los Alamitos, CA.

Shor, P. W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. Santa Fe, NM: Proceedings of the 35th Annual Symposium on Foundations of Computer Science (IEEE). Retrieved from https://ieeexplore.ieee.org/document/365700

Union, E. (2016). *General Data Protection Regulation (GDPR)*. Brussels, Belgium: Official Journal of the European Union.

SOURCES AND REFERENCES

Standards and guidance

- NIST PQC standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA). Finalized August 13, 2024.
- NIST PQC program hub: Current PQC status, late-2025 updates, and IR 8545 on Round 4; HQC selected for further evaluation. (Mar 11, 2025).
- NSA CNSA 2.0: Migration guidance for national security systems; establishes minimum posture.
- ENISA guidance: Migration to post-quantum cryptography for European entities.
- OECD policymaker guide (2025): Government framing on risks, governance, workforce, and supply chains.

Regulatory, compliance, and governance

- SEC cybersecurity disclosure rules: Material incident and risk disclosure expectations; PQC readiness intersects governance and audit duty.
- GDPR: State-of-the-art security expectation applied to long-lived personal data at risk under quantum break.
- HIPAA/HITECH: Long-lived PHI must be protected against foreseeable decryption risk.
- BCBS239 & EBA operational resilience: Integrate PQC readiness with operational risk and reporting governance.
- ISO/IEC 27001, ISACA incident response: Controls and governance aligning PQC migration into audit cycles.
- CA/Browser Forum SC-081v3: Shrinking TLS certificate lifespans from today's 398-day maximum to 200 days in 2026, 100 days in 2027, and 47 days in 2029. This phased reduction is the operational signal that crypto agility must become routine practice.
- Cyber insurance exclusions: Emerging exclusions for known, unmitigated technical risks (market signals).
- Global policy signals: Canada/EU timelines and banking sector briefings showing regulatory pressure and shortened windows.
- Thailand market regulator and NCSA signals: Public calls to prepare for quantum risk and HNDL exposure (regional reinforcement).

Foundational and academic

- Shor (1994) and Grover (1996): Core algorithmic basis for asymmetric collapse and symmetric weakening.
- Mosca (2018): Theorem framing for failure timing.
- NISTIR 8105 (2016): HNDL threat model and migration implications.
- PQCrypto 2025 proceedings (Springer, LNCS 15577–15578): Current research across lattice, code-based, multivariate, isogeny, side-channel, and security notions.

- PQCrypto accepted papers index: Direct visibility into 2025 topics (AEAD notions, BKZ sampling, side channels, LWE qubit reductions).
- BKZ sieving and lattice cryptanalysis (2023–2025): Active lines of attack; informs parameter conservatism.
- Entropy and randomness audits (2024): Survey signals strengthening entropy governance in PQC deployments.
- QKD limitations (ETRI/KAIST): Scope boundaries: supports governance positioning vs. PQC migration.

Industry, market, and executive insight

- Trusted Computing Group: State of PQC Readiness 2025: 1,500-respondent survey; lack of roadmaps, HSM and library readiness gaps; budget realities.
- Utimaco PQC Readiness Report 2025: PKI urgency, legacy drag, low QKD viability, ownership patterns across CISO/CT leadership.
- Future Market Insights (2025): PQC migration market growth forecast to 2035; lattice dominance and sector adoption signals.
- AMI Aptio V UEFI firmware PQC implementation (Nov 2025): Early infrastructure-level adoption; signals supply-chain/firmware seriousness.
- CIO coverage on 47-day certificates: Operational crypto agility and lifecycle management imperative tying directly to PQC preparedness.
- Global Risk Institute (evolutionQ briefing, Aug 2025): Accelerating CRQC timeline signals from major players; urgency for migration planning.
- Microsoft Quantum Safe program strategy (2025): Enterprise roadmaps and vendor ecosystem positioning.
- Gartner PQC roadmap (2024): CIO planning guidance and cost controls via CryptoCOE.
- Financial sector briefings (GFMA/BoE references via media and analyst reports): Narrowing window and regulator nudges for resilience.
- SITG Consulting (2025): Board mandates and solvency framing aligned to current standards and governance practice.
- EFR Financial Services (2023): Banking exposures and sovereignty angles supporting board action framing.
- Blockchain PQC migration risks (2024–2025): Protocol exposure and dormant asset risks under asymmetric collapse.
- NARA VENONA archives: Historical precedent confirming HNDL retroactive decryption risk for long-lived data.

Reference Deployment Matrix

Standards and Guidance

- NIST PQC Standards (FIPS 203, 204, 205, 2024) → Board packs, Academic
- NSA CNSA 2.0 (2022) → Board packs, Legal compliance
- CA/Browser Forum proposed/phased reductions TLS certificates (2025) → Board packs, LinkedIn operational lever.
- OECD PQC Policy Guide (2025) → Academic, Regulatory

Regulatory and Compliance

- SEC Cybersecurity Disclosure Rules (2024) → Board packs, Liability framing
- GDPR, HIPAA, HITECH → Legal compliance, Academic
- BCBS239, EBA Resilience Guidelines → Board packs, Audit appendix
- Cyber Insurance Exclusions (2025) → Board packs, LinkedIn market signal

Academic and Foundational

- Shor (1994), Grover (1996) → Academic anchor
- Mosca (2018) → Board packs, Academic proof
- NISTIR 8105 (2016) → Academic precedent
- PQCrypto 2025 Proceedings → Academic publishing, Scholarly gravity
- Entropy and randomness audits (2024) → Academic, Technical assurance

Industry and Executive Insight

- Trusted Computing Group Survey (2025) → Board packs, LinkedIn industry inertia
- Utimaco PQC Readiness Report (2025) → Board packs, LinkedIn PKI urgency
- AMI Aptio V UEFI PQC Implementation (2025) → Board packs, Supply chain signal
- Future Market Insights (2025) → Investor packs, LinkedIn
- SITG Consulting (2025) → Board packs, Consultancy authority
- Global Risk Institute and evolutionQ (2025) → Board packs, Accelerated horizon
- Microsoft Quantum Safe Strategy (2025) → Board packs, Executive briefings
- Gartner PQC Roadmap (2024) → Board packs, CIO channel
- EFR Financial Services (2023) → Board packs, Sector specific
- Blockchain PQC migration risks (2024–2025) → LinkedIn, Emerging risk signal
- NARA VENONA archives → Academic, Historical precedent

Reference Horizon Scan

Geopolitical Programs

- China National Quantum Strategy → Global race signal
- Russia Quantum Information Science Progress Reports → State program reference
- India National Mission on Quantum Technologies → Regional program signal
- UK NCSC PQC Guidance (2024–2025) → National security posture

Sector Standards

- PCI DSS v4.0 (2024) → Financial services crypto agility
- FIPS 140-3 validation updates (2025) → Hardware crypto module compliance

Vendor Ecosystem

- OpenSSL PQC integration notes (2024–2025) → Library readiness
- AWS, Google Cloud, Azure PQC roadmaps → Cloud provider migration timelines
- Thales and Entrust HSM advisories (2024–2025) → Hardware vendor readiness

Risk and Insurance

- Actuarial Society briefings (2024–2025) → Quantum risk modelling for insurers
- Bank of England and BIS speeches → Financial stability references

Academic Depth

- Isogeny cryptography collapse papers (2022–2023) → Family failure precedent
- Hybrid PQC deployment studies (2024–2025) → RSA plus Kyber adoption evidence
- AI accelerated cryptanalysis surveys (2025) → Emerging attack vector

Regional Frameworks

- ASEAN cybersecurity frameworks → Regional governance signal
- Canadian Centre for Cyber Security PQC guidance (2024) → National readiness reference

References and Sources - Useful Web Links

Core Standards and Guidance

1. NIST announcement of PQC FIPS 203, 204, 205 (Kyber, Dilithium, SPHINCS+) — https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

2. Federal Register notice of FIPS 203/204/205 issuance — https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

3. NSA CNSA 2.0 official advisory — https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

4. ENISA report: Post-Quantum Cryptography – Current State and Quantum Mitigation — https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Regulatory and Legal Anchors

5. GDPR encryption and “state of the art” requirements — https://gdpr-info.eu/issues/encryption/

6. ENISA/TeleTrusT guidance on “state of the art” IT security — https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

7. UK ICO encryption guidance — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/encryption/

8. SEC Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (2023) — https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Case Studies and Precedents

9. Equifax 2017 breach settlement — https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

10. VENONA project archives — https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/

11. SHA-1 “SHAttered” collision paper — https://shattered.io/static/shattered.pdf

Recent Academic and Market Advances

12. SpringerLink collection of quantum computing articles — https://link.springer.com/subjects/quantum-computing

13. McKinsey Quantum Technology Monitor 2025 — https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

14. arXiv paper: Quantum Computing: Vision and Challenges — https://arxiv.org/abs/2403.02240
15. UK Cyber Coordination Group PQC migration guidance (April 2025) — https://www.cmorg.org.uk/sites/default/files/2025-06/CMORG%20-%20Guidance%20for%20Post-Quantum%20Cryptography%20-%20April%202025%20-%20TLP%20CLEAR%20%281%29.pdf
16. EU Commission PQC roadmap (targets 2030 for critical infrastructure) article NIS— https://postquantum.com/quantum-policy/eu-pqc-roadmap/
17. Trusted Computing Group State of PQC Readiness 2025 report — https://trustedcomputinggroup.org/wp-content/uploads/State-of-PQC-Readiness-2025-November-2025.pdf

SITG Consulting Authority Statement

Track Record of Risk and Resilience

We have followed the evolution of quantum risk since its earliest signals. Our collective experience spans systemic exposures across banks, insurers, governments, healthcare, and travel and tourism.

- Y2K readiness → Global technology survival mandate
- Sarbanes-Oxley (SOX) → Governance and compliance enforcement
- Basel frameworks → Banking solvency and capital adequacy
- BCBS239 → Risk data aggregation and reporting discipline
- Solvency II → Insurance capital adequacy and resilience
- Financial Crime Compliance (FCC) → AML, sanctions, and fraud risk transformation
- Enterprise Risk Management (ERM) → Global banking frameworks and board accountability
- Government and healthcare programmes → NHS, pensions, and public sector resilience
- Travel and tourism audits → Risk exposure, regulatory fit, and survival strategies.

Each of these mandates carried the same lesson: boards should act before disruption becomes failure. Quantum risk is the next inevitability.

Why Boards Choose SITG Consulting

- Global reach with a pool of associates ready to engage across jurisdictions and sectors.
- Small enough to care, large enough to scale with forensic discipline and board-level impact.
- Proven authority in rescuing failing transformation programmes and architecting quantum risk diagnostics
- Audit-ready outputs designed for frictionless deployment in board packs, regulatory submissions, and investor briefing.

Engagement Options

- Initial Diagnostic Review → Rapid current-state assessment with survival recommendations
- Board Readiness Briefing → Tailored session mapping liability, regulation, and solvency risk.
- Full Forensic PQC Audit → Comprehensive review benchmarked against NIST, CNSA 2.0, ENISA, and sector standards.

Author & SITG Chief Strategist Profile

Brian Couzens

Brian Couzens is the author of this white paper and Chief Strategist at SITG Consulting. He has led enterprise-wide transformation programmes for over 25 years across banks, insurers, asset management, governments, healthcare, and energy.

- Rescued failing programmes in financial services, government, and healthcare, delivering forensic readiness and survival strategies.
- Architected regulatory frameworks spanning Basel, BCBS239, Solvency II, FCC, and ERM, embedding board accountability.
- Designed and deployed compliance methodologies, including authoring the SOX methodology for Shell International, which became a reference model for internal control and audit readiness.
- Defined early operational standards for risk reporting in the 1990s, creating templates that were later adopted by regulators as baseline practice.
- Directed cloud and data transformation across AWS, Azure, and GCP, embedding governance and risk control frameworks into enterprise architecture.
- Applied AI selectively to accelerate forensic diagnostics, automate compliance reporting, and benchmark operational performance, using it as a tool for efficiency rather than a headline.
- Led public sector programmes including NHS and pensions remediation, aligning governance mandates with operational continuity.
- Published technical commentary on quantum risk, cryptography, and systemic resilience, positioning SITG Consulting as the benchmark authority for board survival and regulatory transformation.

Contact Information

SITG Consulting

Global

📧 info@sitg-consulting.com

📞 Asia: +66 972176658

📞 Europe: +44 7418622620

For board enquiries, regulatory reviews, or consultancy engagements, SITG Consulting provides stripped, audit-ready outputs designed for immediate deployment.

SITG Consulting: Services Offered

Quantum Risk Diagnostics

Forensic readiness reviews and survival strategies, mapping exposures to Harvest-Now-Decrypt-Later threats and CRQC timelines.

Board Readiness Briefings

Tailored sessions for directors and executives, framing liability, solvency, and regulatory risk in board-ready language.

Regulatory Transformation Audits

Basel, BCBS239, Solvency II, FCC, ERM compliance reviews — exposing systemic gaps and aligning governance with survival mandates.

Programme Rescue & Turnaround

Recovery of failing transformation initiatives across banks, insurers, governments, healthcare, and travel/tourism, restoring credibility and resilience.

Cloud & Data Governance

Migration, remediation, and audit-ready frameworks for AWS, Azure, and GCP, embedding governance and risk control into digital infrastructure.

ESG Data & Analytics

Integration of climate, diversity, and sustainability metrics into board reporting, aligned with OECD, ISSB, and EU Taxonomy standards.

Digitization Mandates

Advisory on regulatory digitization requirements, covering cloud migration, open banking APIs, and digital operational resilience (DORA, MAS, etc.).

NIS2 Readiness

Forensic audits and compliance frameworks aligned to the EU NIS2 Directive, ensuring operational resilience and regulatory fit.

Strategic Publications & Advisory

White papers, rebuttals, and board-level communication assets designed for frictionless deployment in board packs, regulatory submissions, and investor briefings.

How SITG Consulting Helps with Quantum Risk

Implementation Pathway for Readiness

1. Current State Analysis

- Conduct forensic assessment of cryptographic assets.
- Identify RSA/ECC dependencies, shadow crypto, and vendor exposures.
- Establish baseline risk profile against Mosca's Theorem (X + Y > Z).

2. Cryptographic Bill of Materials (CBOM)

- Build a dynamic, auditable inventory of all cryptographic assets.

- Integrate vendor disclosures and supply chain dependencies.
- Automate quarterly board reporting for visibility and accountability.

3. Risk Profiling and Governance Alignment

- Classify assets by data lifetime, system criticality, and compliance scope.
- Map liabilities to fiduciary duty and regulatory mandates.
- Embed survival KPIs into board governance structures.

4. PQC Migration Roadmap

- Define phased migration: Discovery → Pilot → Deployment.
- Select NIST-approved PQC algorithms (Kyber, Dilithium, SPHINCS+).
- Replace protocols, libraries, and vendor integrations.
- Allocate solvency-based budget and enforce timelines.

5. Operational Integration

- Embed cryptographic agility into architecture.
- Align cloud platforms (AWS, Azure, GCP) with PQC standards.
- Deploy governance and risk control frameworks across enterprise systems.

6. Compliance and Regulatory Readiness

- Align with CNSA 2.0, ENISA guidance, GDPR “state of the art,” SEC disclosure rules.
- Prepare defensible evidence for regulators, auditors, and investors.
- Position board actions as proactive compliance, not reactive remediation.

7. Board and Executive Briefings

- Deliver stripped, forensic briefings tailored for directors and officers.
- Certify readiness against fiduciary liability and solvency risk.
- Provide survival framing: visibility, mitigation, governance.

8. Resources We Provide

- White Papers and Technical Guides: Board-ready publications on quantum risk, PQC migration, and governance mandates.
- Diagnostic Tools: Quantum Risk Dashboard, CBOM templates, and solvency KPIs for measurable readiness.
- Training and Workshops: Executive briefings, risk officer training, and compliance workshops tailored to sector needs.
- Regulatory Methodologies: Proven frameworks authored by SITG Consulting, including SOX methodology for Shell International, Basel/BCBS239 templates, and PQC compliance playbooks.
- Survival Benchmarks: Comparative analysis across industries, showing where boards stand against peers and regulators.

The SITG Bench: Expertise We Deploy

Board-Level Strategists

- Senior advisors framing fiduciary liability, solvency risk, and governance mandates.

Regulatory Architects

- Specialists who design and deploy compliance methodologies, including SOX for Shell International, Basel templates, and BCBS239 frameworks.

Quantum Computing Experts

- Researchers tracking fault tolerance, logical qubit scaling, and cryptanalytic breakthroughs.

Cryptography Engineers

- Focused on PQC standards (Kyber, Dilithium, SPHINCS+) and hybrid cryptographic agility, ensuring secure implementation.

Risk Analysts

- Responsible for cryptographic inventories, CBOM deployment, and survival KPI measurement.

Cloud and Systems Engineers

- Embedding PQC standards into enterprise architecture and vendor ecosystems across AWS, Azure, and GCP.

Sector Specialists

- Tailoring readiness for financial services, healthcare, pensions, and government programmes.

AI Analysts

- Applying AI selectively to accelerate diagnostics, automate compliance reporting, and benchmark operational performance.

Programme Managers

- Coordinating multi-year migration roadmaps, vendor dependencies, and budget enforcement.

Audit and Assurance Leads

- Validating CBOM accuracy, migration milestones, and board reporting for defensible compliance evidence.

Delivery Resources We Supply

Business Analysts

To capture requirements, map cryptographic inventories, and translate regulatory mandates into operational workflows.

Project Managers

To oversee migration timelines, vendor coordination, and budget enforcement, ensuring milestones are met.

Programme Managers

To direct multi-stream initiatives across enterprise systems, cloud platforms, and regulated sectors.

PMO (Project Management Office)

To provide governance, reporting, and portfolio oversight, ensuring board visibility and accountability.

Risk Analysts

To quantify exposures, track CBOM accuracy, and benchmark survival KPIs.

Compliance Analysts

To align deliverables with Basel, BCBS239, Solvency II, GDPR, SEC disclosure, and sector mandates.

Audit and Assurance Leads

To validate readiness evidence, confirm migration milestones, and prepare defensible board reporting.

Testing and Validation Engineers

To stress-test PQC implementations, verify cryptographic agility, and confirm operational resilience across systems and vendors.

SITG Consulting delivers complete Quantum Risk readiness. We design the pathway, supply the resources, and deploy the bench of strategists, engineers, and analysts required to achieve both compliance and assurance at board level. We can operate as the full delivery partner or integrate with your existing teams to strengthen capacity where it matters most. Whether building from the ground up or augmenting what is already in place, SITG ensures readiness is executed with speed, credibility, and survival certainty. Compliance you can evidence. Assurance you can trust.

Legal Notice

This white paper is for informational and commercial purposes only and does not constitute legal advice. The content is intended to inform boards, executives, and technical teams about post-quantum cryptography risks, mitigation approaches, and governance considerations. It is not a substitute for legal, regulatory, tax, insurance, or other professional advice tailored to your organisation's facts and applicable law.

Jurisdictional and fact-specific nature of legal statements

Statements in this document that refer to liability, fiduciary duty, regulatory obligations, enforceable requirements, or potential legal consequences are general observations based on publicly available standards, guidance, and technical literature. Such statements are jurisdictional and fact-specific: their applicability and legal effect depend on the law of the relevant jurisdiction, the organisation's contractual obligations, regulatory status, sectoral rules, and the specific facts and timing of any incident. Readers should not treat any statement in this paper as a definitive legal conclusion.

No warranties or guarantees

While the paper cites technical sources and standards to support its analysis, no representation or warranty is made regarding the completeness, accuracy, or suitability of the information for any particular purpose. Technical models and risk projections (including references to Mosca's Theorem, Shor's Algorithm, or the Harvest Now, Decrypt Later threat) are presented to illustrate risk scenarios and planning imperatives; they do not guarantee specific outcomes. Organisations should treat probabilistic and model-based statements as planning inputs, not as certainties.

Reliance and decision making

Decisions based on the content of this white paper are the sole responsibility of the reader. Before implementing any governance, technical, or disclosure action, organisations should obtain independent legal, regulatory, insurance, and technical advice appropriate to their circumstances. In particular, boards and officers should consult counsel and their D&O insurers regarding any public statements, certifications, or attestations about readiness, migration timelines, or compliance.

Limitations on liability

To the fullest extent permitted by applicable law, SITG Consulting and the author disclaim all liability for any direct, indirect, incidental, consequential, special, or punitive damages arising out of or relating to the use of, reliance on, or inability to use the information contained in this document. Nothing in this paper creates a contractual relationship, fiduciary duty, or professional engagement between the reader and SITG Consulting or the author.

References and evidence

Where the paper cites standards, guidance, or academic work, those references are provided for context and further reading. Readers should verify the current status of any standard, regulation, or technical publication cited, as standards and regulatory expectations evolve over time.

Recommended next steps

Organisations should: (1) treat the paper as a strategic briefing and sales-oriented advisory resource; (2) run any proposed board resolutions, public disclosures, or contractual commitments by qualified legal counsel; and (3) consult insurers and regulators as appropriate before making formal attestations or public statements.

Contact for legal review

For assistance coordinating legal review or to discuss how the observations in this paper apply to a specific organisation, contact your legal counsel or request a formal engagement with SITG Consulting's regulatory and legal advisory team.

Effective date

This Legal Notice applies to the version of the white paper dated November 2025. Legal and regulatory positions may change; consult counsel for the most current interpretation.

COPYRIGHT NOTICE

This white paper and all content contained herein, including text, figures, tables, graphics, and layout (the "Work"), are protected by copyright and other intellectual property laws. No part of the Work may be reproduced, distributed, transmitted, displayed, published, or broadcast in any form or by any means without the prior written permission of SITG Consulting, except where permitted by applicable law.

Permitted Uses

- You may download, print, and use extracts of the Work for internal, non-commercial, educational, or advisory purposes provided that you retain all copyright and other proprietary notices and do not alter the content.
- Any public distribution, commercial use, derivative works, or republication requires prior written permission from SITG Consulting.

Requests for Permission

To request permission for reproduction, distribution, or other uses not covered above, contact: info@sitg-consulting.com. Include the title of the Work, the requested use, the portion to be used, and the intended audience.

Trademarks and Third-Party Rights

All trademarks, service marks, trade names, logos, and product names appearing in the Work are the property of their respective owners. Reference to any third-party product, service, or standard does not constitute or imply endorsement by SITG Consulting.

No Legal or Professional Advice

The Work is provided for informational and commercial purposes only and does not constitute legal, regulatory, tax, insurance, or other professional advice. Readers should consult qualified professionals before acting on the basis of the Work.

DMCA and Copyright Infringement

SITG Consulting respects the intellectual property rights of others. If you believe that your copyrighted work has been used in a way that constitutes copyright infringement, please provide a written notice containing the following information:

- A physical or electronic signature of the copyright owner or a person authorized to act on their behalf;
- Identification of the copyrighted work claimed to have been infringed;
- Identification of the material that is claimed to be infringing and information reasonably sufficient to permit SITG Consulting to locate the material;
- Contact information for the complaining party (address, telephone number, and email);
- A statement that the complaining party has a good-faith belief that use of the material is not authorized by the copyright owner, its agent, or the law; and
- A statement, under penalty of perjury, that the information in the notice is accurate and that the complaining party is the copyright owner or authorized to act on the owner's behalf.

Send DMCA notices and inquiries to: info@sitg-consulting.com with subject line DMCA Notice — QUANTUM RISK White Paper.

Limitation of Liability

To the fullest extent permitted by law, SITG Consulting disclaims liability for any direct, indirect, incidental, consequential, or special damages arising out of the use of the Work.

Effective Date

This copyright notice applies to the version of the Work dated November 2025.