QUANTUM RISK · 2026 GLOBAL DOCTRINE

QUANTUM RISK

A 2026 Global Doctrine for Post-Quantum Cryptography Migration,

Board Accountability and Cryptographic Solvency

Forensic. Cross-jurisdictional. Standards-aligned.

GLOBAL FRAMING

EU · United Kingdom · United States · Canada · GCC · ASEAN · Australia & New Zealand · Africa · Latin America

STANDARDS BENCHMARK

NIST FIPS 203/204/205 · NSA CNSA 2.1 · ETSI TR 103 619 · ISO/IEC 27001 · ENISA Quantum-Safe Guidance · NIS2 · DORA

Edition 2026.1

Prepared by SITG-Consulting – Brian Couzens

CHAPTER

Executive Briefing: The Quantum Solvency Threat

The solvency threat that has already begun

Key Indictment: Harvest Now, Decrypt Later

Quantum computing will break RSA and elliptic-curve cryptography. The mathematical basis is settled: Shor's polynomial-time factoring and discrete-logarithm algorithm renders every widely deployed asymmetric primitive obsolete once a cryptographically relevant quantum computer (CRQC) exists[1].

Post-quantum cryptography (PQC) migration is not an algorithm swap. It requires a full cryptographic modernisation transformation: a governed, gated, evidence-driven programme that spans board mandate, enterprise-wide discovery, architecture redesign, wave-based transition, vendor assurance and continuous operational governance.

The active threat is Harvest Now, Decrypt Later (HNDL): the silent, sustained exfiltration of encrypted long-lived data for future retroactive decryption. NSA, NIST, ENISA, the UK NCSC, Canada's CCCS, Australia's ASD, Hong Kong's HKMA and the G7 Cyber Expert Group now treat HNDL as a present operational risk rather than a future hypothesis[2]. Organisations holding regulated, intellectual-property, treaty-bound, contractual, health, identity, or sovereign data face foreseeable and quantifiable liability the moment they fail to act.

Mathematical proof: the deadline is Day One

Q-Day is not the deadline. Migration time is the deadline. Mosca's inequality, $X + Y > Z$, defines the failure horizon: where X is migration time, Y is the confidentiality lifetime of protected data, and Z is the time remaining to a CRQC. For any enterprise holding decade-scale data, the inequality is already true today[3]. The Global Risk Institute's Quantum Threat Timeline Report, produced annually with evolutionQ, records a consistent narrowing of expert estimates: surveyed specialists treat a CRQC within a ten to twenty year horizon as a credible scenario rather than a remote one[4].

Fiduciary and governance mandate

This is a board-level solvency issue, not an IT upgrade. The defensive posture available to directors and officers is no longer a question of capability but of evidence: documented inventory, documented migration plan, documented funding, documented vendor coordination. The instruments are global and converging; some are binding in force, others are draft or advisory, and the distinction is set out below.

- **Standards and compliance:** NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) were finalised on 13 August 2024. FIPS 206 (FN-DSA / FALCON) is in development. HQC was

selected as a code-based backup KEM on 11 March 2025; the draft standard is expected in 2026 with finalisation in 2027. The initial public draft of NIST IR 8547 sets out an expected transition approach under which quantum-vulnerable algorithms are deprecated from 2030 and disallowed from 2035; the report is a draft at the date of writing, and the 2030/2035 horizons are also reflected in NIST SP 800-131A and US National Security Memorandum 10[5].

- **National security baselines:** NSA CNSA 2.0 (updated December 2024) mandates AES-256, ML-KEM-1024, ML-DSA-87 and SHA-384/512 for all US National Security Systems and their vendor ecosystem[6].
- **EU legal track:** COM(2026) 13 final, published 20 January 2026, is a proposed directive amending NIS2. If adopted, it would add a new Article 7(2)(k) requiring Member States to adopt post-quantum transition policies within their national cybersecurity strategies. At the date of writing, it remains in the ordinary legislative procedure and is not yet binding. The coordinated EU PQC roadmap, issued by the NIS Cooperation Group following the Commission's April 2024 Recommendation and published in June 2025, sets non-binding milestones: Member States to begin transition by end-2026, critical infrastructure to be transitioned by end-2030, and the wider transition completed for as many systems as practicable by 2035. DORA Article 6 RTS already obliges financial entities to monitor quantum-relevant cryptographic threats[7].
- **Allied and APAC posture:** UK NCSC three-phase roadmap (discover by 2028, prioritise/pilot 2028–2031, complete 2031–2035); Canada CCCS (April 2026 departmental plans, 2031 high-risk, 2035 complete); ASD ISM (asymmetric out by end-2030); HKMA Quantum Preparedness Index (2026); Singapore CSA quantum-readiness advisory; India’s National Quantum Mission Quantum-Safe Ecosystem programme[8].
- **Liability:** Failure to act increases the risk of regulatory enforcement, investor claims, securities-disclosure exposure (SEC Reg S-K cybersecurity rules; UK FCA TR-style supervisory expectations; equivalent supervisor expectations across BIS, EBA, MAS, HKMA, ASIC), and personal D&O liability. Boards should seek jurisdiction-specific legal advice[9].

Operational reality and Survival KPIs

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

- **The migration time problem (X):** The visibility gap is the first and most basic governance failure: an enterprise that cannot see its cryptographic estate cannot evidence a defensible response. Few enterprises maintain an accurate inventory of cryptographic assets. Shadow crypto, hard-coded primitives, embedded firmware, vendor dependencies, container images and long-lived datasets guarantee a multi-year transition. Security depends on a chain of trust; every dependent system, API and supplier must complete the transition before final security is achieved[10].
- **Survival KPIs:** Visibility → Mitigation → Governance. The board controls the only variable that prevents failure: starting now. The first act of governance is a Cryptographic Bill of Materials (CBOM) to establish visibility and auditability.

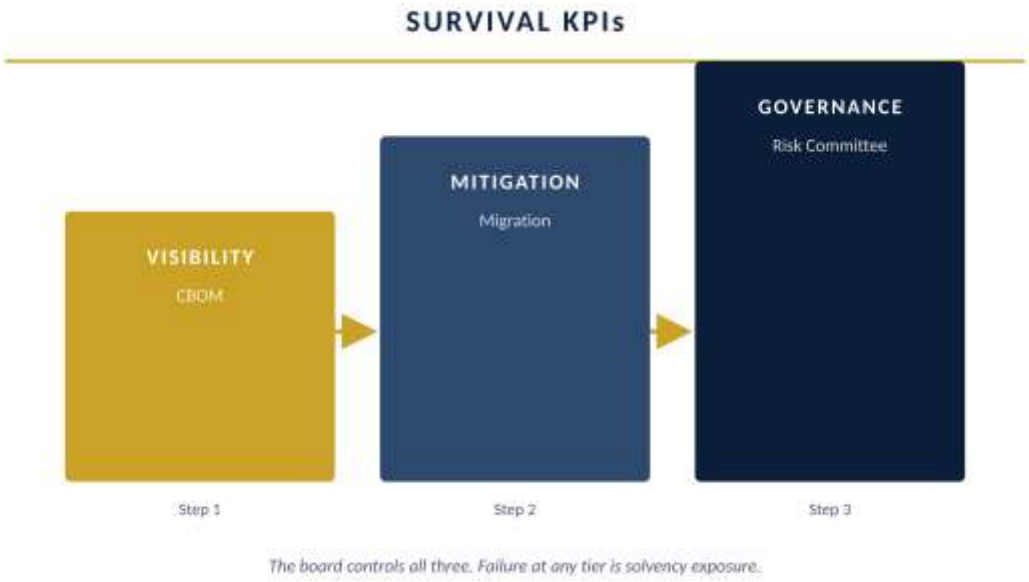

Figure 1. Survival KPIs. The board controls all three.

Corroborated and evidenced risk

Quantum-vulnerable encryption is not a future problem. Standards bodies, national-security authorities, financial-stability regulators, academic cryptographers, and public cryptographic incidents jointly confirm that long-lived encrypted data is already exposed to retroactive decryption. The threat is demonstrable and auditable and is increasingly reflected in regulation and supervisory expectation. Technical inertia creates board-level liability. Boards that delay may face regulatory enforcement, investor litigation, sovereignty challenges and personal exposure for directors and officers. The appropriate response is prompt, evidenced and governed action.

Societal and wellbeing impacts

Quantum-vulnerable data is a societal threat. Retroactive decryption will cause durable 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. As a director or officer, can you evidence to customers, investors, regulators, auditors, supervisors, and your D&O underwriter that your organisation has a governed post-quantum transition under way, with cryptographic migration latency reduced to a defensible level? If you cannot, your systems remain exposed, your compliance position is

incomplete, and your exposure may extend to individual directors and officers. Migration latency is the variable the board controls. The action required is immediate: begin the governed transition now or carry the consequences of an undocumented and unmanaged exposure.

Statements about liability, fiduciary duty and enforceable obligations are jurisdiction-specific. Consult counsel for binding interpretation.

References on this page • [1] Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE. • [2] G7 Cyber Expert Group (2025). Roadmap for the Financial Sector's Transition to Post-Quantum Cryptography; ENISA NIS2 Implementation Guidance (June 2025). • [3] Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers. IEEE Security & Privacy 16(5), 38–41. • [4] Mosca, M. & Piani, M. (2025). 2024 Quantum Threat Timeline Report. Global Risk Institute / evolutionQ. • [5] NIST (2024). FIPS 203, 204, 205. NIST (2025). NIST IR 8545 (HQC selection). NIST (2025, draft). NIST IR 8547 (transition to PQC). • [6] NSA (2024). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). • [7] European Commission (2024) Recommendation (EU) 2024/1101; NIS Cooperation Group (June 2025) Coordinated Implementation Roadmap; European Commission COM(2026) 13 final (20 January 2026); Commission Delegated Regulation (EU) 2024/1774 (DORA ICT RTS). • [8] UK NCSC (2025) Timelines for migration to post-quantum cryptography; CCCS (2025) Canadian Government PQC Roadmap; ASD Information Security Manual (2025); HKMA Quantum Preparedness Index (2026); Singapore CSA Quantum-Safe Cryptography Advisory (2025); India NQM Quantum-Safe Ecosystem (2025). • [9] SEC 17 CFR 229.106 (Reg S-K, Item 106); FCA SYSC 13; ESMA/EBA/EIOPA joint statement on DORA; FSB Cyber Lexicon (2023). • [10] ENISA (2024) Post-Quantum Cryptography – Integration Study; Trusted Computing Group (2025) State of PQC Readiness Survey.

CHAPTER

Table of Contents

Executive Briefing: The Quantum Solvency Threat 1
The solvency threat that has already begun 1
Key Indictment: Harvest Now, Decrypt Later 1
Mathematical proof: the deadline is Day One 1
Fiduciary and governance mandate 1
Operational reality and Survival KPIs 2
Corroborated and evidenced risk 3
Societal and wellbeing impacts 3
Table of Contents 5
Index of Figures 11
1. Purpose and Scope 12
1.1 Purpose 12
1.2 Scope 12
1.3 Target Audience 13
1.4 Visuals Note 13
1.5 Acronym Quick Reference 14
2. Executive Summary 16
2.1 The Quantum Imperative 16
2.2 Mathematical Proof of Failure 16
2.3 The Core Findings 17
2.3.1 Technical reality 17
2.3.2 Geopolitical race 17
2.3.3 Doomsday algorithms 17
2.3.4 HNDL exposure 18
2.4 Strategic and Operational Challenge 18
2.4.1 Inventory and assessment 18
2.4.2 Resource and talent gap 18
2.4.3 Legal and compliance failure 18
2.5 Immediate Board Actions: The Cryptographic Transformation Imperative 18
2.6 Mandate 20
3. Technical Reality Check 21

3.1 Fault Tolerance Barriers: The Scale of the Challenge 21
3.1.1 Quantum error correction 21
3.1.2 Conversion overhead 21
3.1.3 Scaling progress 21
3.2 Cryptanalytic Advances 22
3.2.1 Doomsday algorithms 22
3.2.2 Implementation vulnerabilities 22
3.2.3 Accelerated timelines 22
3.3 PQC Standardisation Status 23
3.3.1 Standards finalised 23
3.3.2 Uneven global adoption 23
3.3.3 Regional convergence 24
3.4 Infrastructure and Key Management 24
3.4.1 Hard-coded crypto 24
3.4.2 Key management sprawl 24
3.4.3 CBOM necessity 24
3.5 Governance Failures 24
3.5.1 Delegation of solvency risk 24
3.5.2 Lack of C-suite ownership 25
3.5.3 Fiduciary exposure 25
3.6 Geopolitical Race for Cryptographic Dominance 25
3.6.1 Opaque state programmes 25
3.6.2 Unannounced weaponisation 26
3.6.3 Parallel modalities 26
3.7 Mandate 26
4. Doomsday Algorithms and Q-Day 27
4.1 The Doomsday Algorithms: Shor and Grover 27
4.1.1 Shor: existential threat 27
4.1.2 Grover: weakening threat 27
4.2 The Mathematical Deadline: Mosca's Inequality 28
4.3 The HNDL Finding: Active Present-Risk Liability 29
4.4 Q-Day: The Point of Confirmed Capability 30
4.5 Mandate 30
5. Post-Quantum Cryptography Solutions Overview 32
5.1 Algorithm Families 32

5.1.1 Lattice-based cryptography 32
5.1.2 Hash-based cryptography 32
5.1.3 Code-based cryptography 33
5.1.4 Other families 33
5.2 Security and Performance Trade-offs 33
Implementation risk 35
Future assurance 35
5.3 Cryptographic Agility 35
5.3.1 Definition 35
5.3.2 Hybrid modes 35
5.4 Mandate 36
6. Quantum Risk Assessment and Inventory 38
6.1 Identify Cryptographic Assets 38
6.2 Establish a Dynamic CBOM 38
6.3 Determine Risk Profile 40
6.4 Identify Shadow Crypto 40
6.5 Mandate 41
7. Cryptographic Transformation Roadmap and Budget 42
7.1 The Six-Level Gated Transformation Model 42
7.2 Select PQC Algorithms 45
7.3 Replace Protocols and Libraries 46
7.4 Coordinate Vendor Migration 46
7.5 Budget and Funding Logic 47
7.6 Mandate 48
8. Global Governance Mandate and Regulatory References 49
8.1 Board Ownership and Governance Architecture 49
8.2 Regulatory and Strategic References by Jurisdiction 50
8.2.1 United States 50
8.2.2 European Union 51
8.2.3 United Kingdom 51
8.2.4 Canada 51
8.2.5 Australia and New Zealand 52
8.2.6 Gulf Cooperation Council (GCC) 52
8.2.7 ASEAN 52
8.2.8 East Asia 52

8.2.9 South Asia 53
8.2.10 Africa 53
8.2.11 Latin America 53
8.2.12 Industry benchmarks 53
8.3 Compliance Integration 53
8.4 Strategic Intelligence Caveat 54
8.5 Audit and Enforcement 55
8.6 The Quantum Readiness Maturity Model 55
8.7 Vendor Dependencies and Supply-Chain Cryptography 57
8.7.1 Vendor readiness is not organisational readiness 57
8.7.2 Vendors cannot reduce the risk variables 57
8.7.3 Supply-chain crypto: the blind spot 58
8.7.4 Board mandate: crypto disclosure requirement 58
8.7.5 Strategic imperative 59
8.8 Mandate 59
9. Rebuttal Section: Dismantling Organisational Inertia 60
9.1 The Symmetric versus Asymmetric Reality 60
9.2 TLS and Protocol Vulnerabilities 60
9.3 PQC Adoption Challenges 60
9.4 The Wait-and-See Fallacy 61
10. Legal and Compliance Implications: The Global Liability Bridge 62
10.1 Breach of Fiduciary Duty: Foreseeable Harm 62
10.2 Regulatory Enforcement and Penalties by Jurisdiction 62
10.3 The Emergence of Cyber Liability Law 63
10.4 Investor and Class-Action Liability 63
10.5 Strategic Legal Mandates 64
11. Strategic Survival KPIs: Measuring Solvency, Not Activity 65
11.1 Visibility and Auditability (CBOM Focus) 65
11.2 Mitigation and Deployment (Roadmap Focus) 66
11.3 Governance and Enforcement (Risk Committee Focus) 67
11.4 Board Directive: Accountability Mandate 67
12. Future-Proofing: The Next Cryptographic Generation 69
12.1 Cryptographic Agility Architecture 69
12.2 The Q-Resilience Mindset 69
12.3 Quantum Key Distribution Caveat 69

12.4 Quantum Incident Response Plan 70
12.5 Strategic Continuity Mandate 70
12.6 Anticipating the Emergent 71
12.7 Board Call to Action 71
13. Case Studies: Systemic Failure Pattern Overview 73
13.1 Case Study A: The Solvency Failure (Equifax, 2017) 74
13.2 Case Study B: The Harvest Now Reality (VENONA, 1943–1980) 75
13.3 Case Study C: The Cost of Readiness (Y2K, 1999) 76
13.4 Case Study D: The Cryptographic Agility Drag (SHA-1 to SHA-2, 2005–2017) 76
13.5 Mandate 76
14. Societal Wellbeing and ESG Risk Impacts 78
14.1 The Human Cost: Retroactive Harm 78
14.2 Post-Quantum Vulnerability as a Governance Failure 79
14.3 Priority Actions and Accountability 79
14.4 Operational Requirements and Metrics 80
14.4.1 Operational imperatives 80
14.4.2 Required metrics 80
14.5 Final Mandate: A Duty to Act 81
15. Conclusion and Board Call to Action 82
Board Directives: Mandatory and Time-Bound 82
15.1 Survival Framing: Inaction as Negligence Defined 82
15.2 Perpetual Q-Resilience: The Architectural Mandate 83
15.3 Final Call to Action: The Board's Decision 84
15.4 Measurable KPIs, Timelines and Evidence 85
15.5 Final Warning 85
Appendix 87
Lexicon for Quantum Risk 87
Bibliography and Sources 89
Foundational and Academic 89
Standards and Technical Guidance 89
European Union 90
United Kingdom 90
North America 91
Asia-Pacific 91
Gulf, Africa and Latin America 91

Global Multilateral and Industry 92
Historical and Case-Study Sources 92

CHAPTER

Index of Figures

Figure 1. *Survival KPIs. The board controls all three.*

Figure 2. *Survival Mandate Tiers. One solvency outcome.*

Figure 3. *Quantum Risk Dashboard. Time, threat level and cost.*

Figure 4. *Six-Level Cryptographic Transformation Model.*

Figure 5. *Qubit Conversion Challenge. Logical versus physical qubits.*

Figure 6. *Algorithm Impact Matrix. Shor and Grover effects.*

Figure 7. *Delegated Quantum Risk. The cost of board distance.*

Figure 8. *Quantum Algorithm Impact on Asymmetric and Symmetric Primitives.*

Figure 9. *Mosca's Inequality. X + Y > Z.*

Figure 10. *Harvest-to-Compromise Timeline. From data capture to exposure.*

Figure 11. *PQC Algorithm Families. Lattice, hash, code, multivariate, isogeny.*

Figure 12. *PQC Performance Metrics. Size, speed and footprint trade-offs.*

Figure 13. *Quantum Key Distribution. Optical exchange and post-processing.*

Figure 14. *Cryptographic Inventory Layers. CBOM coverage map.*

Figure 15. *Shadow Crypto Exposure. Sources and surface.*

Figure 16. *Cryptographic Transformation Roadmap. Six-gate governance with wave-based execution.*

Figure 17. *Cryptographic Transformation Budget Allocation. Solvency categories.*

Figure 18. *Governance Architecture Map. Board, QRC and the escalation spine.*

Figure 19. *Accelerated Quantum Break Horizon. Public versus classified curves.*

Figure 20. *Quantum Readiness Maturity. Five stages from Unprepared to Surviving.*

Figure 21. *Security Risk Layers. Vendor, integration and board exposure.*

Figure 22. *Supply-Chain Crypto Blind-Spot Map. Visibility gaps.*

Figure 23. *Strategic Survival KPIs Dashboard. CBOM, roadmap and governance.*

Figure 24. *PQC Solvency Pyramid. Visibility → Mitigation → Governance.*

Figure 25. *Perpetual Solvency Pyramid. Four layers including horizon intelligence.*

Figure 26. *Systemic Risk Iceberg. Visibility failure to retroactive exposure.*

Figure 27. *Quantum Risk Mapped to ESG Pillars and Governance Outcomes.*

Figure 28. *PQC Governance Check List. Directives, owners and RAG status.*

Figure 29. *The Board's Decision Point. Lead the transition or carry the exposure.*

CHAPTER

1. Purpose and Scope

1.1 Purpose

This paper provides a forensic, globally framed roadmap for surviving the quantum risk era. It is written for boards, regulators, supervisors, transformation leaders and general counsel operating in every major jurisdiction. Quantum computing poses an existential threat to current cryptographic foundations: RSA, Diffie-Hellman and the entire elliptic-curve family collapse under Shor's algorithm. Symmetric algorithms such as AES-256 and hash functions such as SHA-384 remain viable under Grover with adjusted parameters. Data encrypted today may be decrypted tomorrow under the Harvest Now, Decrypt Later threat.

This paper discharges two functions.

The strategic function sets out the technical reality with evidence, translates cryptographic advances into board accountability and director-level risk, and defines immediate survival KPIs.

The operational function provides CISOs, CIOs, CTOs, CDOs, architects and procurement leaders with a vendor-agnostic framework for PQC migration, budgeting and compliance with the converging family of global standards: NIST FIPS 203/204/205 (and forthcoming 206), NSA CNSA 2.0, ETSI TR 103 619, ISO/IEC 18033-3 and ISO/IEC SC 27 WG 2 work on quantum-safe cryptography, ENISA quantum-safe guidance, NIS2, DORA, the UK NCSC roadmap, Canada CCCS guidance, Australia's ASD ISM, Singapore CSA, HKMA, India's NQM, GCC digital-trust frameworks, and African Union and Latin American data-protection regimes that increasingly require state-of-the-art cryptography for long-lived personal data.

1.2 Scope

This paper covers the full lifecycle of quantum risk management, from initial assessment through to a sustained transition strategy. The frame is board-centric and cross-jurisdictional. It avoids theoretical physics while retaining forensic precision so that directors, supervisors and operational leaders understand both the urgency and the levers required for survival.

In scope

- Technical reality: fault tolerance barriers, cryptanalytic advances, PQC standardisation status, governance failures, the geopolitical race.
- Doomsday algorithms and Q-Day: Shor, Grover, Mosca, HNDL.
- PQC solutions overview: lattice, hash-based, code-based, multivariate, isogeny; security and performance trade-offs; hybrid agility.

- Risk assessment and inventory: CBOM as the auditable baseline; asset prioritisation; shadow crypto.
- Cryptographic transformation roadmap and budget: six-level gated model; talent gap; vendor dependencies; cost of delay.
- Legal and compliance landscape across EU, UK, US, GCC, ASEAN, Australia and New Zealand, Africa, Latin America: data sovereignty, fiduciary duty, supervisory expectations, civil liability.
- Strategic KPIs, future-proofing, cryptographic agility, the Q-Resilience mindset, the Quantum Incident Response Plan.

Out of scope

- Theoretical physics such as superposition or entanglement.
- Quantum computing for commercial optimisation such as drug discovery, materials science or machine learning.
- Proprietary vendor product reviews. The paper is vendor-agnostic and standards-anchored.

1.3 Target Audience

- Strategic layer: boards of directors, CEOs, CFOs, regulators and supervisors, legal counsel, risk and audit committees.
- Operational layer: transformation leaders, CISOs, CIOs, CTOs, CDOs, enterprise and security architects, compliance officers, vendor and supply-chain managers, procurement leads, internal audit.
- Public and policy layer: ministries, central banks, financial-stability bodies, critical-infrastructure operators, sectoral regulators across telecoms, energy, healthcare, transport, defence and public administration.

1.4 Visuals Note

The paper retains the diagrams, timelines and architecture maps of the original edition. These are governance instruments: Mosca's inequality, the HNDL timeline, the CBOM coverage map, the transformation roadmap and the resilience cycle exist to make abstract cryptographic exposure visible and defensible at board level.

Figure 2. Survival Mandate Tiers. A cascading hierarchy from fiduciary duty to technical execution.

References on this page • NIST (2024) FIPS 203/204/205; NIST (2025) IR 8545 (HQC); NIST (draft) IR 8547. • NSA (2024) CNSA 2.0. • European Commission (2024/2025/2026) PQC Recommendation, Roadmap, COM(2026) 13. • ETSI TR 103 619 (Migration strategies and recommendations to quantum-safe schemes). • ISO/IEC JTC 1/SC 27 WG 2 work programme on quantum-safe cryptography. • UK NCSC (2025); Canada CCCS (2025); ASD ISM (2025); Singapore CSA (2025); HKMA (2026); India NQM Quantum-Safe Ecosystem (2025).

1.5 Acronym Quick Reference

This quick reference defines the acronyms used most frequently in this paper. A fuller lexicon for board, supervisory and operational audiences is provided in the Appendix.

ACRONYM	EXPANSION
PQC	Post-Quantum Cryptography
CRQC	Cryptographically Relevant Quantum Computer
HNDL	Harvest Now, Decrypt Later
CBOM	Cryptographic Bill of Materials
RSA	Rivest-Shamir-Adleman (asymmetric algorithm)

ACRONYM	EXPANSION
ECC	Elliptic-Curve Cryptography
AES	Advanced Encryption Standard (symmetric algorithm)
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism (FIPS 203)
ML-DSA	Module-Lattice-Based Digital Signature Algorithm (FIPS 204)
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (FIPS 205)
FN-DSA	FFT over NTRU-Lattice Digital Signature Algorithm (FIPS 206, in development)
FIPS	Federal Information Processing Standard (NIST)
CNSA 2.0	Commercial National Security Algorithm Suite 2.0 (NSA)
NIST	National Institute of Standards and Technology (US)
NCSC	National Cyber Security Centre (UK)
ENISA	European Union Agency for Cybersecurity
NIS2	Network and Information Security Directive 2 (EU)
DORA	Digital Operational Resilience Act (EU)
TOM	Target Operating Model
BAU	Business as Usual
Q-IRP	Quantum Incident Response Plan
D&O	Directors and Officers (liability)
HSM	Hardware Security Module
PKI	Public Key Infrastructure

CHAPTER

2. Executive Summary

Quantum-vulnerable encryption is not a future problem. It is a material societal risk that is present today. Standards bodies, national-security authorities, financial-stability regulators, academic cryptographers and public cryptographic incidents jointly confirm that long-lived encrypted data is already exposed to retroactive decryption. Real human harms follow: identity theft, irreversible privacy loss, compromised medical and identity records, disruption of critical services and the corrosion of public trust. Technical delay converts into social harm, regulatory liability and material loss. Prompt and evidenced action is required across every jurisdiction.

2.1 The Quantum Imperative

The threat posed by a cryptographically relevant quantum computer is a foreseeable enterprise risk requiring immediate board governance. RSA and ECC fail under Shor. AES-256 survives Grover with adjusted key sizes and remains the symmetric workhorse mandated by CNSA 2.0[1]. The deadline for corrective action is not Q-Day. The deadline is today, by virtue of Mosca's inequality. Inaction maps to potential solvency liability and personal exposure for directors and officers across SEC Reg S-K, UK FCA SYSC, DORA, NIS2, MAS TRM, HKMA SA-2, APRA CPS 234, FINMA, and equivalent supervisory regimes[2].

2.2 Mathematical Proof of Failure

Data security is already compromised. Mosca's inequality $X + Y > Z$ provides the mathematical basis for immediate action: any data with confidentiality lifetime Y which, when added to migration time X, exceeds the time to a CRQC (Z), is on the wrong side of the inequality. HNDL compounds this reality, with adversaries exfiltrating encrypted high-value data now to decrypt later, and opaque nation-state programmes add further uncertainty[3].

Inaction may, depending on jurisdiction, constitute a breach of duty of care and a failure to meet supervisory expectations of state-of-the-art cryptography under instruments such as GDPR Article 32, UK ICO guidance, NIS2 Article 21, DORA, the US HIPAA Security Rule, Singapore PDPA, the Australia Privacy Act, Canada PIPEDA, Brazil LGPD, South Africa POPIA, UAE PDPL, KSA PDPL and India DPDP Act[4].

Figure 3. Quantum Risk Dashboard. Critical time window, HNDL threat impact and agility cost.

2.3 The Core Findings

2.3.1 Technical reality

Fault-tolerance barriers remain but cryptanalytic advances are closing. PQC standardisation has crossed from theory to deployable specification with FIPS 203/204/205 final, FIPS 206 in development and HQC selected for code-based diversity. Implementation gaps, side-channel risk and entropy governance remain the largest commercial weaknesses.

2.3.2 Geopolitical race

The race for cryptographic dominance involves opaque state-sponsored programmes alongside commercial leaders. The United States (IBM, Google, IonQ, Quantinuum, Atom Computing, PsiQuantum), the United Kingdom (Oxford Quantum Circuits, Riverlane), China (USTC, Baidu, Origin Quantum, Pan Jianwei's satellite programme), the EU (Pasqal, IQM, Quantum Flagship), Japan (Fujitsu, RIKEN), South Korea, Singapore, India's NQM, the UAE (TII), Saudi Arabia (Aramco quantum sponsorship) and Australia (Diraq, Silicon Quantum Computing, PsiQuantum Brisbane) are pursuing parallel modalities. A material breakthrough in any single modality could shorten Z; the magnitude and timing of any such effect are uncertain.

2.3.3 Doomsday algorithms

Shor ends public-key encryption. Grover's algorithm reduces the effective security margin of symmetric primitives and motivates the use of larger key and hash sizes. Both are mathematically settled.

2.3.4 HNDL exposure

Any long-lived data exfiltrated today including intellectual property, M&A files, trade-secret algorithms, sovereign cables, treaty data, customer records and identity attributes becomes decryptable once a CRQC exists. Data with a confidentiality lifetime extending past the CRQC horizon is exposed from the moment it is harvested.

2.4 Strategic and Operational Challenge

The transition to PQC is not a software patch. It is a multi-year, multi-departmental, cross-border transformation requiring cryptographic agility. The roadmap addresses three forensic gaps.

2.4.1 Inventory and assessment

Establish a Cryptographic Bill of Materials as an auditable inventory to expose shadow crypto, vendor cryptography and supply-chain primitives, and to profile risk by Mosca’s Y factor.

2.4.2 Resource and talent gap

Allocate budget for a phased roadmap from discovery through pilot to deployment, retirement and post-deployment agility. Address the cryptography talent gap through workforce strategy, certified upskilling and selective vendor reliance with contractual guarantees.

2.4.3 Legal and compliance failure

Failure to initiate PQC migration may increase regulatory exposure under regimes such as GDPR Article 32, UK Data Protection Act 2018, NIS2, DORA, HIPAA, HITECH, PCI DSS v4.0.1, CCPA/CPRA, LGPD, PDPA Singapore, Australia Privacy Act 1988, Canada PIPEDA, POPIA, India DPDP, UAE PDPL, KSA PDPL, and sectoral mandates issued by central banks and prudential supervisors. Boards should obtain counsel on specific obligations.

2.5 Immediate Board Actions: The Cryptographic Transformation Imperative

PQC migration is a full cryptographic modernisation transformation. It cannot be delivered as a technical refresh, a vendor-led upgrade or a phased algorithm swap. It requires a gated, evidence-driven programme that spans board mandate through to continuous operational assurance.

The transformation operates across six levels. Level 0 (Executive Board) establishes mandate, funding and accountability. Level 1 (Programme) sequences four execution phases: Discover, Control, Transform, Sustain. Level 2 (Governance Gates) enforces six binary checkpoints: Business Case and Mandate Sign-Off;

CBOM and Risk Triage Approval; Architecture and TOM Approval; Vendor and Supply Chain Readiness; Go-Live and Interoperability Sign-Off; BAU Handover and Audit Sign-Off. No gate is advisory; all gates are mandatory.

Level 3 (Engineering) delivers across six concurrent workstreams. Level 4 (Operating Model) establishes six permanent operational functions. Level 5 (Evidence) produces eight artefact categories that prove what was done, not what was planned.

Organisations enter the programme through one of four tiers. Tier 1: current regulatory breach, requiring compressed Gate 1 delivery within 45 days. Tier 2: inventory complete but architecture pending, entering at Gate 3 with CBOM re-validation. Tier 3: mid-transition under an inadequate governance structure, requiring formal re-baselining. Tier 4: standard entry from a standing start. Tier selection is a board decision at Gate 1 and determines the compression, sequencing and parallelism of the early phases.

The transformation roadmap aligns to four time horizons: Months 0–3 (Business Case, Mandate and Mobilisation), Months 3–9 (Discovery, Automation and Architecture), Months 9–24 (End-to-End Wave-Based Transition) and Months 24–36 (BAU and Continuous Assurance). The 36-month arc is illustrative, not prescriptive. Real programmes run from eighteen months to ten years depending on estate scale, jurisdictional complexity, vendor readiness and organisational change capacity.

Transition execution is wave-based and risk-driven. The first wave addresses the highest-risk assets. Each wave has defined success criteria, rollback procedures and evidence requirements. No wave progresses to production without Gate 5 sign-off. Gate reversion machinery ensures that previously passed gates can be formally reopened when triggering events occur: algorithm vulnerability disclosure, regulatory change, vendor failure or new standards publication.

For organisations seeking an accelerated entry point, a Quantum-Cryptographic Discovery Sprint (20–30 days) establishes cryptographic visibility, quantifies quantum exposure and produces a defensible migration pathway and board-ready business case.

Executive leadership should act now to secure enterprise longevity and meet the standards set by NIST FIPS 203/204/205, NSA CNSA 2.0, ENISA, the EU coordinated roadmap, the UK NCSC, Canada CCCS, ASD, MAS, HKMA, the G7 Cyber Expert Group and equivalent national bodies.

- Mandate the CBOM project. Authorise and fund a centralised, auditable, dynamic CBOM as the first Survival KPI for visibility.
- Approve the gated transformation programme. Constitute the governance structure, fund the multi-year programme envelope and establish the six-gate decision framework. Delay is the costliest option.
- Embed Q-Resilience governance. Incorporate Survival KPIs into board reporting and the Cryptographic Risk Committee agenda, reviewed quarterly. Mandate a Quantum Incident Response Plan.

Figure 4. Six-Level Cryptographic Transformation Model. Board mandate through to continuous operational assurance, governed by six binary gates.

2.6 Mandate

Boards should lead this transition. The decision in front of the board is clear: secure long-lived data and discharge the duty of care now, or carry a compounding exposure across security, compliance and corporate resilience.

References on this page • [1] NSA (2024) CNSA 2.0; Grover, L. K. (1996) STOC; NIST IR 8547 (deprecation 2030, removal 2035). • [2] FSB Cyber Lexicon (2023); BCBS (2021) Principles for operational resilience; MAS TRM Guidelines (2021); APRA CPS 234. • [3] Mosca (2018) IEEE S&P; ENISA (2024) Post-Quantum Cryptography – Integration Study; ENISA NIS2 Implementation Guidance (June 2025). • [4] EU Reg 2016/679 (GDPR) Art. 32; EU Reg 2022/2554 (DORA) and Commission Delegated Reg 2024/1774; HIPAA Security Rule 45 CFR §164.312; PCI DSS v4.0.1 (2024).

CHAPTER

3. Technical Reality Check

The quantum threat is often dismissed on the basis of raw qubit counts reported by public laboratories. This is a category error. The benchmark is a cryptographically relevant quantum computer (CRQC): a machine with enough stable, error-corrected logical qubits to execute Shor at deployed key sizes within a useful run time. This chapter sets out the non-negotiable scientific and geopolitical realities.

3.1 Fault Tolerance Barriers: The Scale of the Challenge

3.1.1 Quantum error correction

Quantum computers require quantum error correction (QEC) to achieve fault tolerance. Physical qubits are highly susceptible to decoherence and gate noise. Surface-code and concatenated-code constructions trade many physical qubits for one error-protected logical qubit[1].

3.1.2 Conversion overhead

Current research demands thousands to tens of thousands of noisy physical qubits per stable logical qubit at the error rates needed for cryptographic Shor instances. Recent estimates for breaking RSA-2048 range broadly from roughly a million physical qubits in conservative models down to recent low-overhead estimates by Gidney and others suggesting under a million, depending on architecture and improvements in lattice surgery, magic-state distillation and code design[2]. The trajectory is downward.

3.1.3 Scaling progress

Scaling barriers are being reduced through coherence and coupling improvements. IBM (Heron, Condor, the 2024 quantum-centric supercomputing programme), Google (Willow, December 2024, below-threshold logical-qubit demonstration), Quantinuum (H-series trapped-ion), Atom Computing (neutral-atom arrays), PsiQuantum (photonic), Diraq (silicon spin), IonQ, Riverlane, Pasqal and others have reported results that were until recently considered theoretical[3].

Where viability has been demonstrated, scaling becomes principally an engineering and capital problem rather than a question of physical possibility. It does not follow that scaling is rapid, certain or uniform across modalities, and the planning horizon should account for that uncertainty in both directions.

Figure 5. Qubit Conversion Challenge. Thousands of unstable qubits stabilise a single logical qubit.

3.2 Cryptanalytic Advances

3.2.1 Doomsday algorithms

Shor is the definitive end of RSA, finite-field Diffie-Hellman and elliptic-curve cryptography (including Curve25519, P-256, P-384 and brainpool curves). Grover's algorithm provides a quadratic speed-up for unstructured search, reducing the effective brute-force security of a symmetric key from n bits towards n/2 bits as an upper bound on the speed-up. In practice the realisable advantage is lower because Grover's search does not parallelise efficiently and a full attack carries substantial circuit-depth and runtime costs. The working planning assumption is that AES-128 should be treated as offering a reduced margin and AES-256 retained as the symmetric baseline; hash output lengths should be sized so that collision and pre-image resistance remain adequate against both classical and quantum search.

3.2.2 Implementation vulnerabilities

Lattice-based PQC schemes remain exposed to side-channel attack, fault injection, decryption-failure exploitation and parameter mis-selection if implementation discipline is poor. Algorithm strength alone is insufficient defence. The 2022 SIDH collapse, broken on a laptop in an afternoon by Castryck and Decru, is the canonical reminder that families can fall.

3.2.3 Accelerated timelines

Optimisations to Shor circuit construction, lattice-surgery techniques, magic-state distillation, AI-assisted cryptanalysis and undisclosed state-sponsored research could each reduce logical-qubit requirements and bring CRQC readiness forward, though the size of any such effect is not predictable in advance.

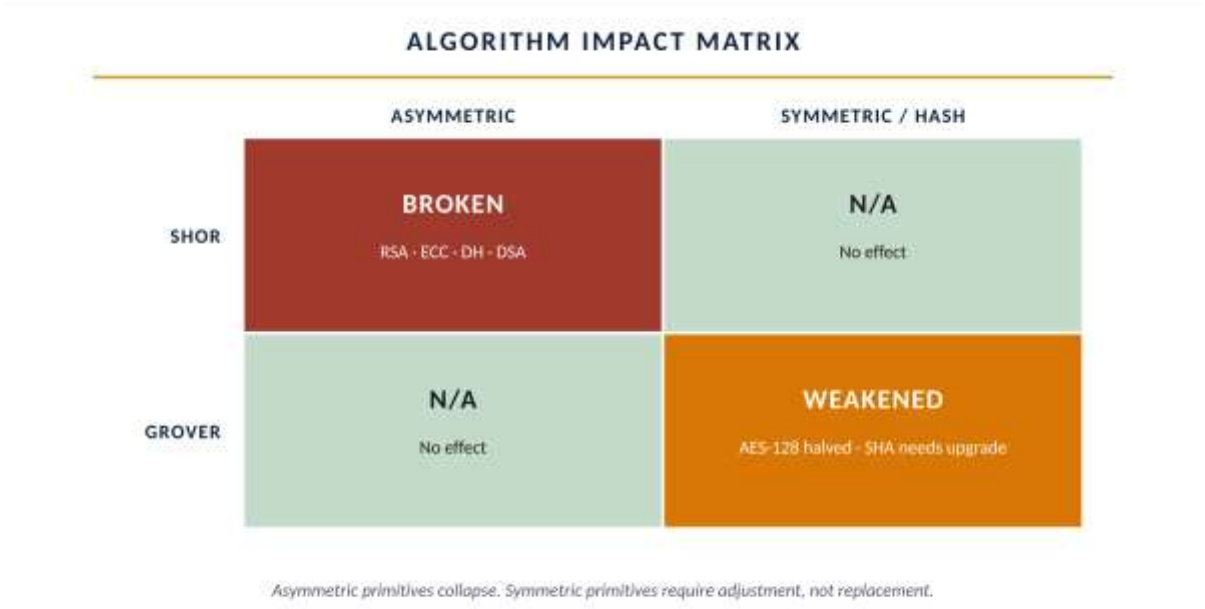

Figure 6. Algorithm Impact Matrix. Shor breaks RSA and ECC. Grover weakens AES-128. Action is mandatory.

3.3 PQC Standardisation Status

3.3.1 Standards finalised

NIST published FIPS 203 (ML-KEM, lattice-based key encapsulation), FIPS 204 (ML-DSA, lattice-based digital signature) and FIPS 205 (SLH-DSA, stateless hash-based signature) on 13 August 2024. FIPS 206 (FN-DSA / FALCON) is in development. HQC was selected as a code-based KEM backup on 11 March 2025 under NIST IR 8545; draft expected in 2026, final in 2027. CNSA 2.0 (NSA, December 2024) operationalises these for US National Security Systems.

3.3.2 Uneven global adoption

The 2025 Trusted Computing Group State of PQC Readiness survey of 1,500 respondents shows that fewer than one in three organisations maintain even a partial cryptographic inventory; fewer than one in five have a funded migration plan. The Utimaco PQC Readiness Report 2025 confirms PKI as the most exposed and least addressed layer. Vendor ecosystems are maturing rapidly (OpenSSL 3.5, BoringSSL, wolfSSL, Cloudflare deployments, AWS-LC, Microsoft Quantum Safe Program, Google Tink, Apple PQ3 for

iMessage, Signal PQXDH, AMI Aptio V UEFI PQC implementation November 2025) but enterprise consumption lags.

3.3.3 Regional convergence

CNSA 2.0, the EU coordinated roadmap, ENISA, the UK NCSC, Canada CCCS, ASD ISM, Singapore CSA, HKMA, India NQM, the GCC digital-trust authorities (UAE TDRA, KSA NCA), the African Union Cybersecurity Convention (Malabo Convention) implementation, and Latin American regulators are converging on NIST-aligned primitives with regional sequencing. Hybrid PQ/T deployments are explicitly encouraged in ENISA and CSWP 39.

3.4 Infrastructure and Key Management

3.4.1 Hard-coded crypto

Decades of embedded RSA and ECC in firmware, container images, IoT devices, vehicle ECUs, industrial control systems, medical devices, payment terminals and HSM-bound applications produce a vast latent migration debt that no patch cycle alone can resolve.

3.4.2 Key management sprawl

Key management is fragmented across thousands of keys spread between cloud KMS instances (AWS KMS, Azure Key Vault, GCP KMS), on-premise HSMs (Thales, Entrust, Utimaco, Crypto4A, Yubico, Marvell LiquidSecurity, AWS CloudHSM), legacy vaults and developer secrets stores. FIPS 140-3 validation matters: from 21 September 2026, all remaining FIPS 140-2 certificates move to the Historical list, constraining procurement and audit pathways.

3.4.3 CBOM necessity

Without a comprehensive, dynamic CBOM, accurate risk profiling and migration planning is impossible. Liability remains unaddressed. CSWP 48 (NIST, September 2025 draft) maps PQC capabilities to the NIST Cybersecurity Framework 2.0 and SP 800-53 Rev. 5, giving governance teams a structured method to express PQC migration as an auditable risk outcome.

3.5 Governance Failures

3.5.1 Delegation of solvency risk

Boards and supervisors have not yet uniformly mandated cryptographic inventories or migration timelines. PQC is too often funded under generic cybersecurity budgets, producing chronic under-resourcing.

This position is changing. EU NIS2, DORA, the proposed COM(2026) 13 amendment, the SEC cybersecurity disclosure rules and analogous instruments in Singapore (CSA Cyber Essentials, MAS Notice 655/657), Hong Kong (HKMA SA-2, Quantum Preparedness Index), Australia (SLACIP Act, ASD ISM) and the UAE (NCA and TDRA Information Assurance Standards) together make underinvestment increasingly difficult to justify to supervisors and investors.

3.5.2 Lack of C-suite ownership

Responsibility is delegated too far down the organisation chart. Shadow crypto, vendor primitives and supply-chain dependencies remain unaddressed, hiding liability that should sit on the executive and board risk register.

3.5.3 Fiduciary exposure

Technical inertia converts into financial and regulatory exposure once standards are final, supervisors articulate expectations and a public incident provides a comparator. All three conditions are now met.

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 state programmes

Commercial leadership is no longer the full picture. China's national quantum strategy (Hefei National Laboratory, the Pan Jianwei Micius satellite QKD programme, the Beijing-Shanghai metropolitan QKD

network and the Origin Wukong superconducting platform), Russia's federal quantum project, India's National Quantum Mission, the UAE Technology Innovation Institute Quantum Research Centre, Saudi Arabia's Aramco-sponsored quantum initiatives, Japan's Moonshot R&D Programme, South Korea's K-Quantum, and Singapore's NQ.SG all maintain elements that are not publicly disclosed.

3.6.2 Unannounced weaponisation

A CRQC breakthrough may not be announced. It may be used against intelligence and financial targets first. The operating principle for boards is the strategic-intelligence caveat: public timelines from commercial laboratories are not the operational risk horizon.

3.6.3 Parallel modalities

Multiple qubit modalities are being pursued simultaneously: superconducting, trapped ion, neutral atom, photonic, silicon spin, topological, NV-centre. Each additional independent line of research raises, rather than lowers, the aggregate probability of an unannounced breakthrough.

3.7 Mandate

Boards should formally acknowledge the technical reality. A defensible position requires governance enforcement of cryptographic inventories, PQC migration planning, vendor disclosure and quarterly reporting of Survival KPIs including CBOM completion, PKI migration and HNDL remediation. Each year of deferral leaves fewer options and a more expensive transition.

References on this page • [1] NIST SP 800-208 (Stateful Hash-Based Signatures); NIST IR 8413 (Round 3 status); Litinski (2019) A Game of Surface Codes. • [2] Gidney, C. & Ekerå, M. (2021) How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits, Quantum 5, 433; Gidney (2025) updates on lattice-surgery resource estimates. • [3] Google AI Quantum (2024) Quantum error correction below the surface-code threshold (Willow); IBM (2024) Quantum-centric supercomputing roadmap; Atom Computing (2024) 1,180-qubit neutral-atom array. • NIST CSWP 39 (December 2025) Considerations for Achieving Cryptographic Agility; NIST CSWP 48 (September 2025 draft) PQC Capability Mappings. • Trusted Computing Group (November 2025) State of PQC Readiness Survey; Utimaco PQC Readiness Report 2025; AMI (November 2025) Aptio V UEFI PQC implementation. • Castryck, W. & Decru, T. (2022) An Efficient Key Recovery Attack on SIDH; NIST IR 8545 (HQC selection, 2025).

CHAPTER

4. Doomsday Algorithms 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 inequality for timing risk, and a liability mechanism that is operational today: Harvest Now, Decrypt Later.

4.1 The Doomsday Algorithms: Shor and Grover

4.1.1 Shor: existential threat

Shor's algorithm reduces integer factorisation and discrete logarithm to polynomial time on a CRQC. RSA, finite-field Diffie-Hellman and elliptic-curve schemes collapse retroactively the moment CRQC capability is demonstrated[1].

- Impact: complete failure of asymmetric encryption, asymmetric authentication, key agreement, and the PKI trust chain.
- Mandate: mandatory replacement.

4.1.2 Grover: weakening threat

Grover's algorithm offers a quadratic speed-up for unstructured search. Against Grover's algorithm AES-256 retains a substantial security margin and is the recommended symmetric baseline; AES-128 offers a materially reduced margin and is not recommended for long-lived protection[2]. SHA-256 outputs need extension or pairing with longer hashes for long-lived signatures.

- Impact: symmetric systems require key-size and parameter adjustment.
- Mandate: mandatory adjustment under CNSA 2.0 and ENISA quantum-safe guidance.

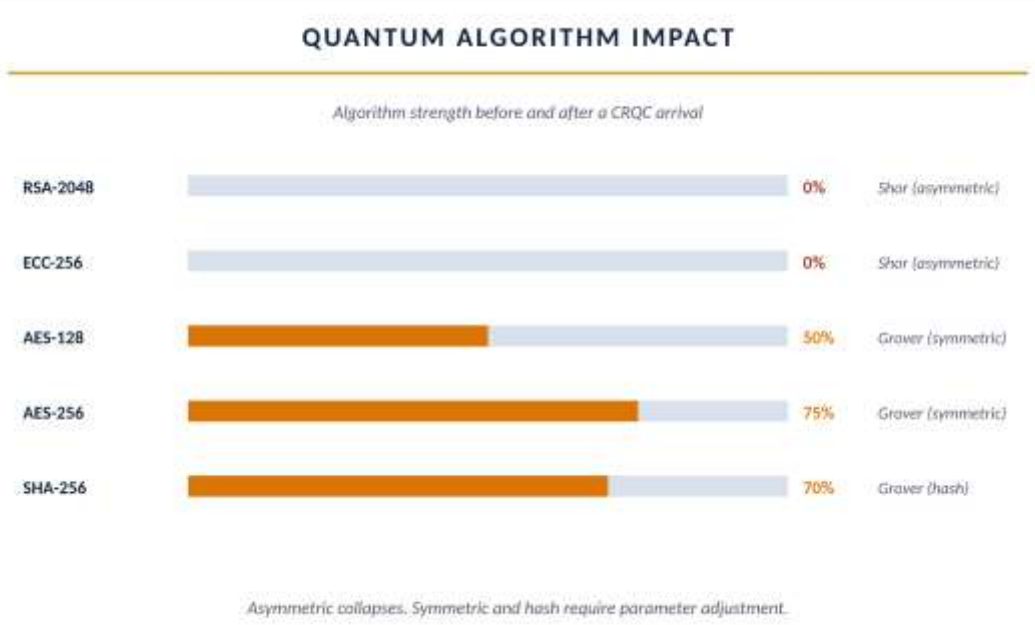

Figure 8. Quantum Algorithm Impact. Shor breaks asymmetric. Grover weakens symmetric. Mitigation is mandatory.

4.2 The Mathematical Deadline: Mosca's Inequality

Mosca's inequality defines the failure condition: X + Y > Z, where X is migration time across discovery, pilot and deployment; Y is the secrecy or integrity lifetime of protected data; Z is the time remaining to CRQC capability[3]. For long-lived data, the inequality is true today. Boards control X. Regulators, treaty obligations, contracts and business strategy define Y. Adversaries and physics define Z.

Figure 9. Mosca's Inequality. If X plus Y exceeds Z, failure is guaranteed.

4.3 The HNDL Finding: Active Present-Risk Liability

Adversaries are exfiltrating encrypted data now, storing it indefinitely, and waiting for CRQC capability. The Federal Reserve's 2025 working paper FEDS 2025-093 explicitly classifies HNDL as a present privacy risk in financial networks. The G7 Cyber Expert Group 2025 roadmap, the BIS Innovation Hub, the Bank of England, the European Systemic Risk Board, the OECD and intelligence-community white papers from Five Eyes partners adopt the same framing.

- Retroactive failure: today's encryption becomes tomorrow's breach.
- Target profile: intellectual property, M&A files, proprietary algorithms, treaty cables, long-term customer data, identity attributes, sovereign communications, defence procurement, healthcare records and genomic data.
- Present exposure: failure to initiate PQC migration converts a future technology risk into a present governance exposure that supervisors and courts can assess against the standard of care available today.

Figure 10. Harvest-to-Compromise Timeline. Harvested data becomes a board-level liability; delay extends the window of foreseeable harm.

4.4 Q-Day: The Point of Confirmed Capability

Q-Day is the moment a CRQC capable of breaking deployed asymmetric key sizes is confirmed to exist, whether by public disclosure, inferred by traffic analysis or signalled by intelligence sources. The operational implications are immediate.

- Immediate impact: RSA and ECC lose secrecy and integrity. Secure boot, code signing, TLS, IPsec, SSH, S/MIME, document signing, blockchain signature schemes, eIDAS-compliant identity, smart-card authentication and certificate authorities fail.
- Compliance exposure: organisations holding long-term data may face civil litigation, regulatory enforcement and supervisor-led remediation for loss that was foreseeable and preventable, with the severity varying by jurisdiction.
- Strategic mandate: the objective is quantum readiness, with X approximately equal to zero before Q-Day.

4.5 Mandate

Boards should recognise the doomsday algorithms as a solvency threat. Survival requires immediate enforcement of PQC migration, CBOM completion, vendor disclosure and quarterly reporting of Survival KPIs. Delay narrows the available options and raises the cost and risk of the eventual transition.

References on this page • [1] Shor (1994); Proös & Zalka (2003) Shor implementation for ECC. • [2] Grover (1996); NIST SP 800-131A Rev. 2 (2019). • [3] Mosca (2018); Mosca & Piani (2025) 2024 Quantum Threat Timeline Report. • Federal Reserve Board (2025) FEDS 2025-093 Quantum Risk in Financial Networks. • G7 Cyber Expert Group (2025) Roadmap for the financial sector's transition to PQC. • BIS Innovation Hub (2025) Project Leap: PQC for central-bank communications.

CHAPTER

5. Post-Quantum Cryptography Solutions Overview

The risk defined by the doomsday algorithms requires immediate mitigation. The solution is the adoption of post-quantum cryptography. PQC is not a single product. It is a family of mathematical constructions with distinct strengths, weaknesses and performance characteristics. Selection is a governance decision.

5.1 Algorithm Families

NIST, ETSI, ISO/IEC, ENISA, the UK NCSC and the GCC digital-trust authorities have converged on the same core families.

5.1.1 Lattice-based cryptography

The dominant solution for key establishment and digital signatures. Based on the hardness of learning-with-errors (LWE), module-LWE and structured-lattice short-vector problems. Standards: ML-KEM (FIPS 203, formerly CRYSTALS-Kyber) for key encapsulation; ML-DSA (FIPS 204, formerly CRYSTALS-Dilithium) for digital signatures; FN-DSA (FIPS 206, in development, formerly FALCON) for compact signatures.

Trade-offs: strong performance, resistance to classical and known quantum attacks. Weaknesses: larger keys and signatures than ECC, side-channel sensitivity in implementation, ongoing cryptanalytic monitoring of BKZ sieving and lattice-reduction improvements.

5.1.2 Hash-based cryptography

Stateful schemes (XMSS, LMS, per NIST SP 800-208) and stateless schemes (SLH-DSA / SPHINCS+, FIPS 205) rely only on the security of an underlying hash function. Grover requires hash-output doubling but does not collapse the families.

Trade-offs: extremely conservative security based on well-understood primitives. Larger signatures, slower signing, stateful variants impose strict key-management discipline (firmware signing is the canonical use case).

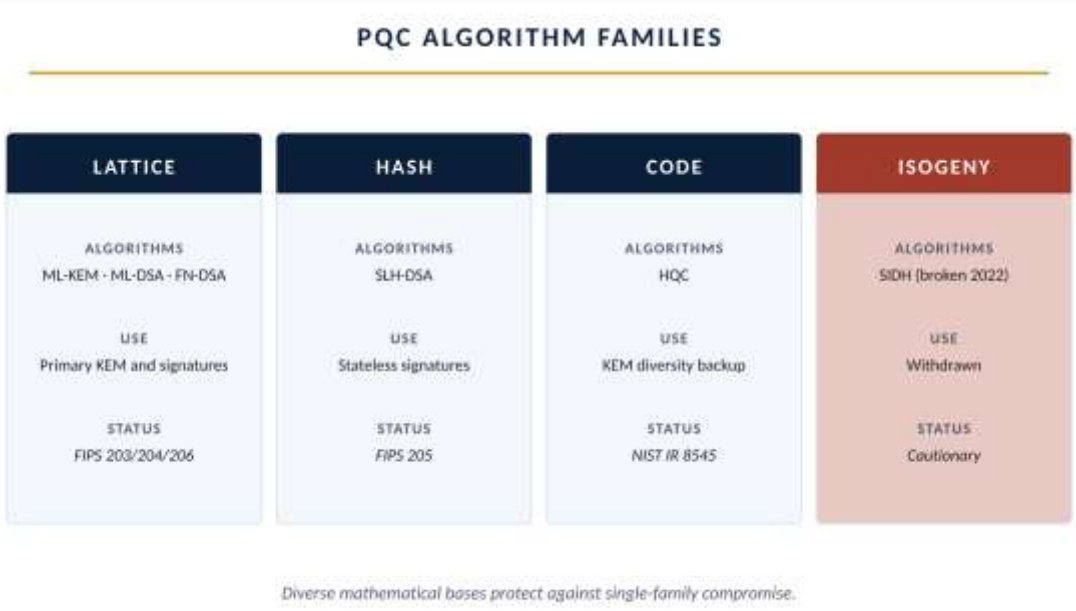

Figure 11. PQC Algorithm Families. Lattice, hash, code and isogeny. Each with trade-offs, all with quantum resilience.

5.1.3 Code-based cryptography

Based on the hardness of decoding random linear codes. Classic McEliece offers extreme conservatism with megabyte-scale public keys. HQC (selected March 2025 under NIST IR 8545; draft 2026, final 2027) provides a code-based KEM alternative with more manageable key sizes and a different hardness assumption to ML-KEM, supporting algorithmic diversity.

5.1.4 Other families

Multivariate quadratic schemes (Rainbow was broken in 2022; UOV variants under review in the NIST additional signatures call), isogeny-based schemes (SIDH/SIKE collapsed in 2022; CSIDH and SQIsign remain candidates with caution), and zero-knowledge or symmetric-only signature schemes (Picnic, FAEST) are active research lines. None should be deployed without standardisation and conservative cryptanalytic exposure.

5.2 Security and Performance Trade-offs

No PQC scheme replicates the size-speed balance once offered by RSA-2048 and ECC P-256. Migration requires trade-off discipline.

SCHEME	PUBLIC KEY (BYTES)	CIPHERTEXT / SIG (BYTES)	USE CASE	NOTES
RSA-2048 (legacy)	256	256	Reference baseline	Broken by Shor on CRQC
ECDSA P-256 (legacy)	64	64	Reference baseline	Broken by Shor on CRQC
ML-KEM-768 (FIPS 203)	1,184	1,088	General KEM	Lattice; current default
ML-KEM-1024 (FIPS 203)	1,568	1,568	CNSA 2.0 KEM	NSS baseline
ML-DSA-65 (FIPS 204)	1,952	3,309	General signature	Lattice; balanced
ML-DSA-87 (FIPS 204)	2,592	4,627	CNSA 2.0 signature	NSS baseline
SLH-DSA-128s (FIPS 205)	32	7,856	Long-term firmware	Hash-based; very conservative
FN-DSA-512 (FIPS 206 draft)	897	666	Compact signature	FALCON; constant-time discipline
HQC-128 (NIST IR 8545)	2,249	4,481	Backup KEM	Code-based; for diversity
Classic McEliece 348864	261,120	128	Sovereign archival KEM	Huge keys; very conservative

Indicative key and ciphertext sizes. Source: NIST FIPS 203, 204, 205 and IR 8545.

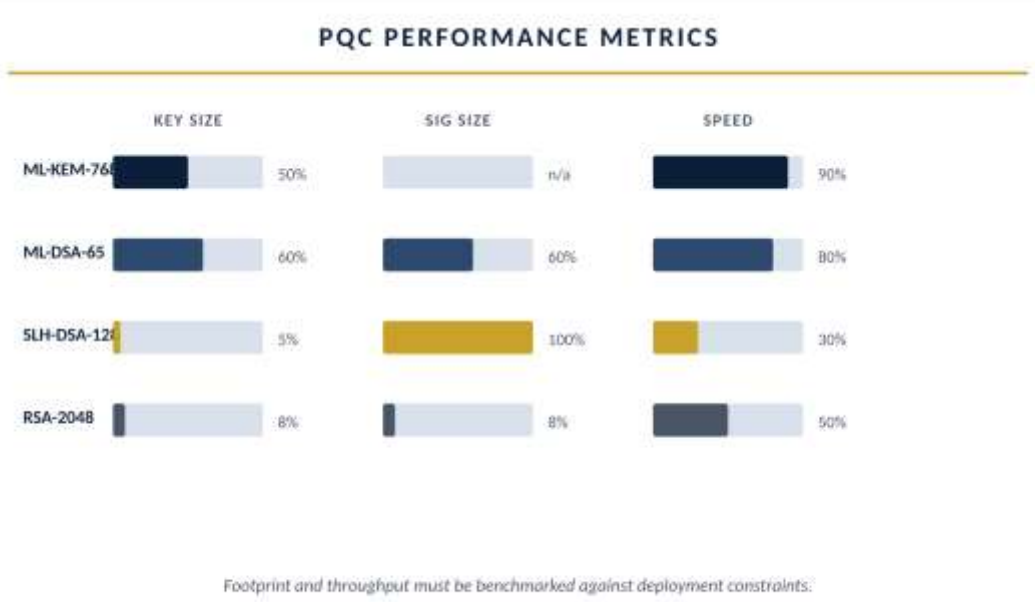

Figure 12. PQC Performance Metrics. Boards must benchmark cryptographic performance before committing to migration.

Implementation risk

Security depends on implementation quality. Side-channel resistance, constant-time execution, fault-injection countermeasures, secure random number generation and decryption-failure-rate analysis are non-negotiable. The 2022 Rainbow break and SIDH collapse are warnings that families can fail; layered defence and cryptographic agility are mandatory.

Future assurance

The field is young. Collapse of a family remains a non-trivial probability over a multi-decade horizon. This is why FIPS 205 (hash-based) and HQC (code-based) exist alongside the lattice-based primary stack. Hybrid PQ/T deployments are now standard ENISA, NCSC and CSWP 39 guidance for the migration period.

5.3 Cryptographic Agility

5.3.1 Definition

Cryptographic agility is the ability to replace algorithms, key sizes, protocols and parameters across the enterprise without redesign or downtime. NIST CSWP 39 (finalised 19 December 2025) defines agility as essential capability and introduces a maturity model used by supervisors and auditors.

5.3.2 Hybrid modes

Hybrid PQ/T mode combines a classical primitive (RSA, ECDH or ECDSA) with a quantum-resistant primitive (ML-KEM, ML-DSA, FN-DSA, SLH-DSA or HQC). A connection is accepted only if both succeed. Major TLS, IPsec, SSH, MACsec and OpenPGP deployments now run hybrid in production: Cloudflare X25519MLKEM768, Google Chrome and Microsoft Edge hybrid TLS, AWS s2n-quic hybrid KEMs, Apple PQ3 for iMessage (PQ + ECDH), Signal PQXDH. ENISA, the NCSC, CCCS and the ECCG Agreed Cryptographic Algorithms v2 (May 2025) explicitly endorse hybrid PQ/T as the migration default.

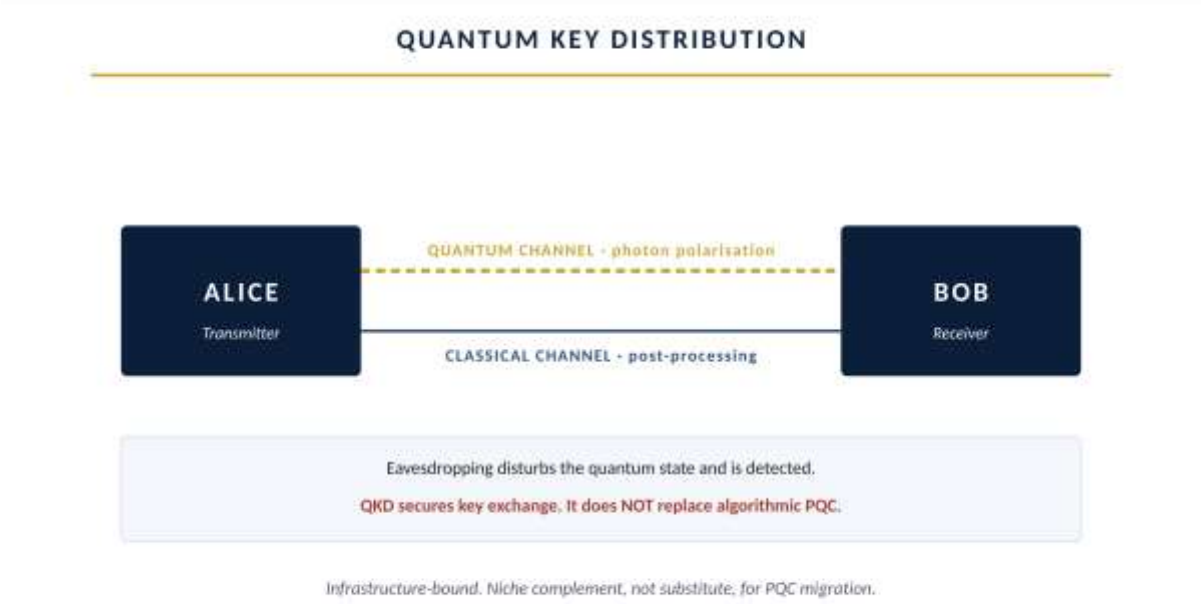

Figure 13. Quantum Key Distribution. Secure key generation via quantum communication. Post-processing ensures integrity.

Governance: systems must allow primitives to be swapped, parameter sets to be tuned and classical components to be removed without service interruption. This is now an audit-grade expectation under DORA, NIS2, MAS TRM and HKMA SA-2.

5.4 Mandate

Boards should mandate transition using hybrid agility as the default and pure-PQC as the destination. Governance must embed the flexibility to swap primitives in the future. This prevents recurrence of rigid infrastructure crises and aligns with CSWP 39 expectations.

References on this page • NIST (2024) FIPS 203 ML-KEM; FIPS 204 ML-DSA; FIPS 205 SLH-DSA. NIST (in development) FIPS 206 FN-DSA. NIST (2025) IR 8545 (HQC selection). • NIST CSWP 39 (19 December 2025) Considerations for Achieving Cryptographic Agility. • ENISA (2024) Post-Quantum Cryptography – Integration Study; ECCG (May 2025) Agreed Cryptographic Algorithms v2. • IETF RFC 8446 (TLS

1.3); IETF draft-ietf-tls-hybrid-design; IETF draft-ietf-ipsecme-ikev2-multiple-ke. • Cloudflare (2024–2025) X25519MLKEM768 deployment statistics; Apple (2024) iMessage PQ3; Signal (2023) PQXDH.

CHAPTER

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 every cryptographic asset across the enterprise and its supply chain. The Cryptographic Bill of Materials (CBOM) is the mandatory metric for board accountability and quantum readiness. The European Commission, US CISA, UK NCSC, Canada CCCS, Australia ASD, Singapore CSA, Japan METI, MAS, HKMA and the OECD all converge on this point.

6.1 Identify Cryptographic Assets

Boards must know what is at risk. The inventory covers every system using cryptography for confidentiality, integrity, authentication, non-repudiation or trust.

Asset categories

- Transport: TLS, mTLS, QUIC, IPsec, MACsec, VPN, SSH, SMTPS, IMAPS, public-facing communication.
- Identity: certificates, digital signatures, secure boot mechanisms, PKI components, eIDAS-compliant identity wallets, federated identity, OAuth/OIDC token signing, FIDO2, smart-card authentication.
- Data at rest: encrypted files, databases, backups, archives, sovereign cloud volumes, full-disk encryption, tape archives.
- Data in transit: messaging platforms, APIs, inter-service communication, ESB, MQ, Kafka with TLS, SFTP, secure file transfer.
- Code integrity: signed binaries, firmware, software update packages, container image signing (cosign, Notation), package signing (RPM, DEB, JAR, PEP-485).
- Sectoral primitives: SWIFT messaging, ISO 20022 payments, EMV chip-and-PIN, 3-D Secure, HSM-bound trade execution, smart-grid SCADA, telecom subscriber identity, healthcare DICOM, eHealth records, eIDAS wallet credentials.
- Shadow crypto: hard-coded keys, undocumented libraries, legacy dependencies, embedded firmware primitives, build-pipeline secrets.

Governance requirement: no asset can be protected if it is not inventoried and assessed for RSA, ECC or quantum-vulnerable dependency[1].

6.2 Establish a Dynamic CBOM

The CBOM is the survival baseline. It must be complete, version-controlled and continuously auditable. SBOM and CBOM should align under the same governance discipline.

Required fields

- Algorithm type, parameter set and key length.
- Protocol and cryptographic library dependency (with version, validation status and FIPS 140-3 certificate where applicable).
- Endpoint and system location, including cloud region for data-sovereignty triage.
- Expiry profile and confidentiality lifetime (Y) for the protected data.
- Migration status, organisational owner, last review date.
- Vendor and supply-chain disclosure linkage.

Format and governance

- Centralised, version-controlled repository, not a static spreadsheet.
- Machine-readable structure aligned with CycloneDX cryptographic asset extension, SPDX 3.0 cryptographic profile or equivalent.
- Automated quarterly board reporting with RAG status.
- Integration with vendor disclosures to track supply-chain liability, including PQC roadmap commitments and FIPS 140-3 module status.

Figure 14. Cryptographic Inventory Layers. Operational assets depend on application and product inventories. CBOM must capture all layers.

Mandate: CBOM completion is the first Survival KPI. No migration can proceed without it[2].

6.3 Determine Risk Profile

Each asset must be classified by exposure and by operational, legal and reputational impact. This profiling links the CBOM directly to fiduciary duty and to supervisory reporting.

Risk factors

- Data lifetime: long-lived data (high Y) is exposed to HNDL by default.
- System criticality: failure triggers operational outage, treaty breach or legal incident.
- External exposure: internet-facing systems and cross-border data flows are primary attack vectors.
- Compliance scope: assets governed by GDPR, UK DPA 2018, HIPAA, HITECH, PCI DSS v4.0.1, NIS2, DORA, MAS TRM, HKMA SA-2, APRA CPS 234, federal and defence contracts (US DFARS, UK MOD JSP 440, EU EDF), Trade-Control regimes (US ITAR/EAR, UK Strategic Export Controls, EU Dual-Use Regulation).
- Sovereignty: data subject to data-localisation laws (Russia FZ-152, China DSL/PIPL, Vietnam Decree 53, India DPDP, KSA PDPL) requires sovereign cryptographic primitive selection where mandated.

Board action: boards must prioritise assets based on quantitative risk modelled against Mosca's inequality.

6.4 Identify Shadow Crypto

Shadow crypto is undocumented, legacy or third-party cryptography outside governance. It is the single largest source of unmanaged liability.

Sources

- Embedded systems and IoT devices: industrial control systems, building management, telematics, medical devices, smart meters.
- Proprietary vendor SDKs and libraries with cryptographic call sites that are not surfaced in product documentation.
- Legacy applications with undocumented cryptographic calls, often binding to deprecated OpenSSL versions or local key stores.
- Hard-coded keys or credentials in source code, CI/CD secrets, build artefacts and container images.
- Crypto-mining contamination, malware persistence keys, abandoned developer credentials.

Figure 15. Shadow Crypto Exposure. Risk starts in code and configuration. CBOM must trace every dependency.

Mandate: shadow crypto must be exposed and brought under CBOM control. Omission leaves liability unmanaged and is increasingly difficult to defend to supervisors and auditors.

6.5 Mandate

Boards should enforce a full cryptographic inventory and fund the CBOM project. CBOM completion is the precondition for everything that follows: there is no defensible migration without prior visibility. Deferral compounds both cost and risk.

References on this page • [1] ENISA (2024) Post-Quantum Cryptography – Integration Study; CISA (2024) PQC Initiative; OWASP CBOM project. • [2] NIST IR 8413 (2022); NIST CSWP 48 (September 2025 draft) PQC Capability Mappings to NIST CSF 2.0 and SP 800-53 Rev. 5. • CycloneDX 1.6 Cryptographic Asset Extension; SPDX 3.0 Cryptographic Profile. • NCSC (2025) Migration to PQC: discover, plan, execute. • ASD ISM (2025) Information Security Manual – cryptography section. • EU Reg 2022/2554 (DORA) Art. 9 ICT security; Commission Delegated Reg 2024/1774 RTS.

CHAPTER

7. Cryptographic Transformation Roadmap and Budget

The shift from acknowledgement to mitigation requires a funded and governed transformation programme. PQC migration is not a technical refresh. It is a full cryptographic modernisation transformation: centrally mandated, visible to regulators and reported quarterly. To protect long-lived data and discharge fiduciary duty across every jurisdiction in which the enterprise operates, the transition must complete within the windows set by NIST IR 8547, NSA CNSA 2.0, the EU coordinated roadmap, the UK NCSC, Canada CCCS, ASD ISM, MAS, HKMA and the G7 Cyber Expert Group. The only controllable variable in Mosca's inequality is migration time (X). Delay compounds liability and guarantees HNDL exposure.

7.1 The Six-Level Gated Transformation Model

Cryptographic transformation operates across six levels, from executive mandate through engineering execution to continuous operational assurance. Each level is distinct in audience, function and evidence requirements. Each level feeds the next. None can be skipped. The model is gated, not phased: gates cannot be bypassed, and no gate is advisory.

Level 0: Executive Board View. The transformation begins and ends at board level. Level 0 defines the strategic shape of the programme in terms boards can mandate, fund and govern. The first board-level decision is tier entry: which of four entry tiers applies to the organisation, determining the compression, sequencing and parallelism of early phases.

- Tier 1 (Current Regulatory Breach): the organisation has passed one or more regulatory deadlines. Gate 1 evidence pack is compressed to 45 days. Examples include US NSS supply chain entities non-aligned with the CNSA 2.0 software and firmware date of January 2025; EU financial entities not DORA-aligned; NIS2-scoped entities in transposed jurisdictions.
- Tier 2 (Inventory Complete, Architecture Pending): validated CBOM exists but no target architecture, no approved hybrid strategy, no sanctioned migration plan. Entry at Gate 3 with CBOM re-validation.
- Tier 3 (Mid-Transition): executing migration waves under a prior governance structure that does not meet the required standard. Formal programme assessment and re-baselining required before further waves execute.
- Tier 4 (Standard Entry): no active regulatory breach, no prior programme work. The standard illustrative arc. The least common entry point in the current market.

Level 1: Programme View (Tactical). Four execution phases translate the board mandate into accountable delivery: Discover (pre-discovery and business case, executive mobilisation, automated discovery and CBOM generation); Control (stabilisation and risk prioritisation, target architecture and hybrid strategy); Transform (build and integration, wave-based transition execution); Sustain (interoperability and cryptographic agility, sovereign and regulatory alignment, BAU transition and continuous assurance).

Level 2: Governance Gates. Six mandatory binary gates span the programme lifecycle. Each requires validated evidence before the programme may proceed. Each is a formal SteerCo decision point.

- Gate 1: Business Case and Mandate Sign-Off. Board-approved business case, executive mandate, funding authorisation, programme governance constituted.
- Gate 2: CBOM and Risk Triage Approval. Complete CBOM validated against sampling audit, risk classification applied, wave sequence proposed. CBOM confidence tiers (High, Medium, Low, Attestation-only) documented per asset category.
- Gate 3: Architecture and TOM Approval. Target architecture, Target Operating Model, hybrid strategy, vendor selection framework, cryptographic agility design.
- Gate 4: Vendor and Supply Chain Readiness. The gate failed in practice with the greatest frequency and the severest downstream consequences. All critical vendors assessed for cryptographic supply chain integrity. Three outcomes where a vendor cannot pass: Replace (Outcome A), Conditional pass with remediation plan (Outcome B), Board escalation (Outcome C).
- Gate 5: Go-Live and Interoperability Sign-Off. Interoperability testing complete, staging validation, rollback procedures tested, classical material decommissioning evidence.
- Gate 6: BAU Handover and Audit Sign-Off. Operating model operational and evidenced, monitoring live, all evidence artefacts in continuous production, gate reversion machinery operational.

Gates are binary. A gate is either passed on the evidence or it is not passed. Programme momentum, executive commitment and budget cycle optics are not permitted inputs to gate decisions.

Level 3: Engineering and Operational Execution. Six concurrent workstreams deliver the transformed state: Automated Inventory and CBOM; Risk Assessment and Wave Prioritisation; Hybrid PQC and PKI Integration; Build, Integration and CI/CD Enforcement; Interoperability and Protocol Testing; Monitoring, Telemetry and Lifecycle Control.

Level 4: Operating Model. Six permanent operational functions constitute the cryptographic operating model, staffed, tooled and governed on a permanent basis. The operating model must be built and tested before the delivery programme closes.

Level 5: Evidence. Eight artefact categories prove what was done: Baseline CBOM, Migration CBOM, Target Architecture and Architecture Decision Records, Vendor Assessment Evidence, Wave Execution Evidence, Sovereign and Regulatory Alignment Confirmations, Cryptographic Agility Test Evidence,

Operating Model Handover and BAU Evidence. Evidence is a programme deliverable, not documentation produced for audit consumption.

The Transformation Roadmap. The model aligns to four time horizons: Months 0–3 (Business Case, Mandate and Mobilisation), Months 3–9 (Discovery, Automation and Architecture, passing Gates 2, 3 and 4), Months 9–24 (End-to-End Wave-Based Transition, passing Gate 5 per wave) and Months 24–36 (BAU and Continuous Assurance, passing Gate 6). The 36-month arc is illustrative, not prescriptive. Programme duration is a function of estate scale, jurisdictional complexity, entry tier, vendor readiness and organisational change capacity. Real programmes run from eighteen months to ten years.

Wave-Based Execution. Transition is risk-driven and wave-based. The first wave addresses the highest-risk assets. Waves are structured migration events with defined scope, success criteria, rollback procedures and evidence requirements. Wave failure is a governance event with three defined states: rollback successful, rollback partial, rollback failed. Each state has its own governance response. Non-atomic wave categories (database encryption hierarchies, distributed caching, hardware-bound keys) require explicit governance including compensating controls, containment procedures and a defined point of no return.

Gate Reversion. Gates are not one-way doors. Gate reversion is the formal reopening of a previously passed gate following a triggering event. Category A (immediate, five working days): algorithm vulnerability disclosure, hard deadline change, vendor commercial failure. Category B (scheduled, 30 days): new algorithm approvals, updated sector guidance, vendor roadmap changes. Category C (logged): theoretical vulnerabilities, early-stage legislative proposals. The Cryptographic Risk Committee owns gate reversion in BAU.

Discovery Sprint Entry Point. For organisations seeking an accelerated entry, a Quantum-Cryptographic Discovery Sprint (20–30 days) establishes cryptographic visibility, quantifies quantum exposure and produces four core deliverables: initial CBOM and asset view, quantum risk and stress heatmap, strategic PQC migration roadmap and a Level 1 business case proposal.

Governance requirement: no gate passes without validated evidence, documented risk reduction, regulator-ready artefacts and board sign-off. The transformation aligns with NCSC three-phase guidance, CCCS phasing, the EU 2026/2030/2035 milestones and CNSA 2.0 category schedules[1].

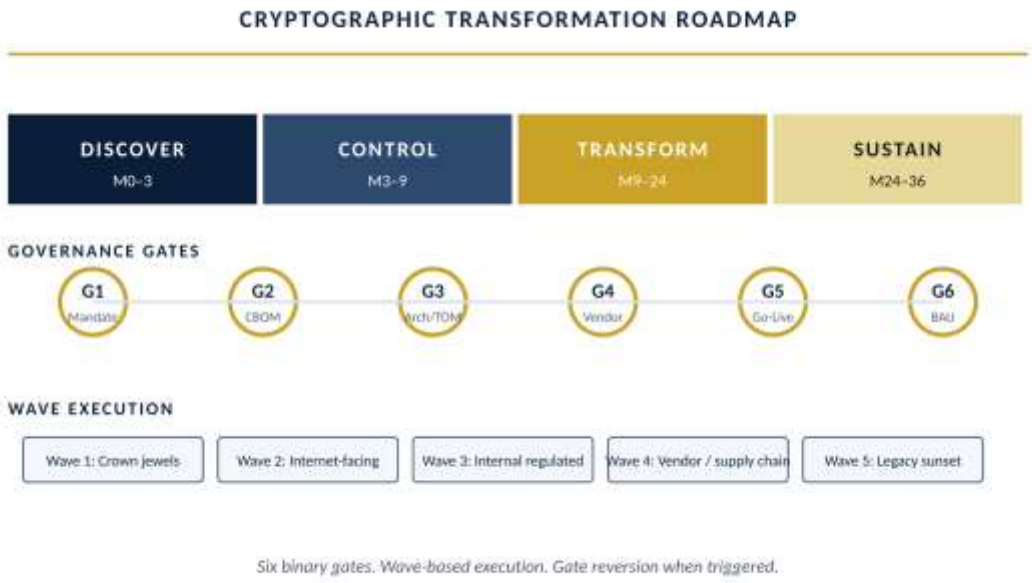

Figure 16. Cryptographic Transformation Roadmap. Six-level gated model with wave-based execution, aligned to NIST, EU, UK, Canada, ASD and CNSA 2.0 timelines.

7.2 Select PQC Algorithms

Algorithm selection is a governance decision. It must be based on risk, performance, validation status, sovereign acceptance and hardware compatibility.

- NIST standardisation status: FIPS 203/204/205 final (August 2024); FIPS 206 (FN-DSA) in development, with an initial public draft and final standard anticipated across 2026-2027; HQC selected March 2025 under NIST IR 8545, draft expected 2026 and finalisation expected 2027.
- Key and signature sizes, including impact on protocol message sizes (TLS handshake, X.509 certificate chains, code-signing artefacts).
- Performance benchmarks for latency, throughput, energy consumption and CPU/FPGA/ASIC footprint.
- Known weaknesses including side-channel risk, decryption-failure rate, and recent cryptanalytic literature (BKZ sieving, lattice-reduction improvements, GPU-accelerated attacks).
- Hardware compatibility in HSMs (Thales, Entrust, Utimaco, Crypto4A, Yubico, Marvell LiquidSecurity), TPMs (TCG TPM 2.0), FPGAs, secure enclaves (SGX, SEV-SNP, TDX, ARM CCA), smart cards and embedded MCUs.
- Sovereign acceptance: CNSA 2.0 mandates ML-KEM-1024 and ML-DSA-87 for US NSS; ENISA recommends parameter sets aligned to ECCG v2; GCC, ASEAN and Latin American regulators are converging on NIST-aligned profiles with selective sovereign extensions.

Board action: boards should approve algorithm selection based on operational fit, sovereign acceptance and risk analysis. Agility is the design goal.

7.3 Replace Protocols and Libraries

Protocols must be upgraded to support PQC primitives. This is now a procurement, audit and supervisory matter.

- Replace RSA and ECC with hybrid PQ/T (ML-KEM + X25519 / ECDH P-256/P-384) in TLS 1.3, IKEv2, SSH, MACsec, QUIC.
- Upgrade cryptographic libraries: OpenSSL 3.5+, BoringSSL, AWS-LC, wolfSSL, Bouncy Castle, mbedTLS, Microsoft SymCrypt, Apple corecrypto, Open Quantum Safe liboqs.
- Adopt IETF hybrid drafts: draft-ietf-tls-hybrid-design, draft-ietf-ipsecme-ikev2-multiple-ke, draft-ietf-openpgp-pqc, draft-ietf-cose-pqc.
- Validate fallback and failure logic in hybrid modes; enforce downgrade prevention; sign and timestamp version-control commits.
- Address the certificate-lifecycle squeeze: the CA/Browser Forum SC-081v3 reduction of TLS certificate lifespans (398 days today, 200 days in 2026, 100 days in 2027, 47 days in 2029) makes routine automated lifecycle a precondition for PQC operations.

Governance requirement: protocol replacement must be tested, versioned and auditable. Downgrade tolerance is unacceptable.

7.4 Coordinate Vendor Migration

Vendor exposure is external liability. Compliance is contractual, supervisory and increasingly statutory.

- Vendor CBOM submission aligned to CycloneDX cryptographic asset extension or equivalent.
- PQC readiness declaration covering algorithms, parameter sets, validation status (FIPS 140-3) and product roadmap.
- Migration schedule linked to SLA, with milestones and escalation triggers.
- Liability clauses for non-compliance, including indemnity for HNDL exposure and supervisor-imposed remediation.
- Flow-down to sub-suppliers consistent with DORA Chapter V (ICT third-party risk), NIS2 Article 21 supply-chain requirements, US Executive Order 14028 software-supply-chain attestation, UK Telecommunications Security Act 2021 supply-chain duties.

Governance requirement: vendor migration is a governance obligation. Boards should enforce compliance through procurement leverage and contractual instruments.

7.5 Budget and Funding Logic

Migration requires dedicated, multi-year, ring-fenced funding. It is a resilience investment, not a discretionary IT cost. Gartner, McKinsey, Forrester and IDC 2025 PQC migration cost benchmarks place median enterprise programmes in the tens of millions; sectoral or global tier-1 programmes (banks, telecoms, utilities, defence primes) regularly exceed nine figures over the migration horizon.

Budget categories

- CBOM tooling and automation: discovery, certificate inventory, runtime cryptographic telemetry.
- Protocol and library upgrades, including hybrid TLS, SSH, IPsec and PKI re-platforming.
- Hardware refresh: FIPS 140-3 HSMs, PQC-capable TPMs, secure enclaves, embedded MCUs with PQC offload.
- Vendor audits, attestation and SLA enforcement.
- Staff training, talent augmentation, certified cryptographic engineering, cross-jurisdictional legal advisory.
- Legacy contingency for non-upgradeable systems: ring-fenced replacement budget aligned to NIST IR 8547 deprecation and disallowance dates.

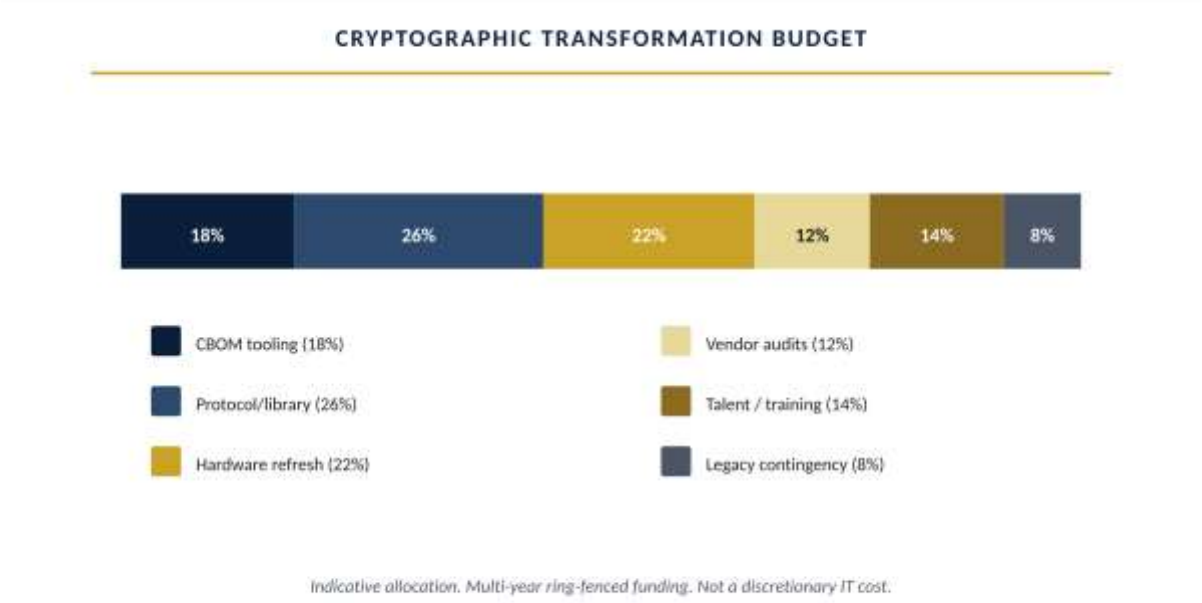

Figure 17. PQC Migration Budget Allocation. CBOM, upgrades, hardware, audits, training and legacy contingency.

Governance requirement: budget must be multi-year, board-approved, supervisor-visible and tracked quarterly. Under-funding guarantees liability[2].

7.6 Mandate

The roadmap is the path to survival. Boards should enforce gated transformation 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.

References on this page • [1] NIST IR 8547 (transition); NSA CNSA 2.0 (2024); EU coordinated PQC roadmap (June 2025). • [2] Gartner (2024) PQC roadmap and CryptoCOE guidance; McKinsey (2025) Quantum Technology Monitor; Forrester (2025) PQC migration benchmarks; IDC (2025) Worldwide Quantum Security Forecast. • IETF hybrid drafts: draft-ietf-tls-hybrid-design; draft-ietf-ipsecme-ikev2-multiple-ke. • CA/Browser Forum SC-081v3 (TLS certificate lifecycle reductions). • EU Reg 2022/2554 (DORA) Chapter V; EU Reg 2022/2555 (NIS2) Art. 21; US Executive Order 14028; UK Telecommunications Security Act 2021. • UK NCSC (2025) Migration to PQC; Canada CCCS (2025) PQC Roadmap; ASD ISM (2025) Cryptography section.

CHAPTER

8. Global Governance Mandate and Regulatory References

Quantum risk is a governance failure and a foreseeable threat to corporate resilience in every jurisdiction. Boards should own the risk, enforce migration and align with the converging family of authoritative standards. This chapter consolidates governance architecture, compliance obligations, intelligence caveats and global enforcement vectors into a single survival framework.

8.1 Board Ownership and Governance Architecture

The era of delegation has passed. Only the board can authorise the transformation, release multi-year resilience funding and certify a state-of-the-art cryptographic posture. Governance must be structured for enforcement, not reporting.

The OECD G20 Principles of Corporate Governance, the BIS Principles for Effective Cyber Resilience, the FSB Cyber Lexicon, and supervisory expectations under NIS2, DORA, SEC Reg S-K, FCA SYSC, MAS TRM, HKMA SA-2, APRA CPS 234 and equivalent regimes converge on board-level cyber accountability.

Mandates

- Board resolution: formal motion to initiate and fund PQC migration, recorded in board minutes and tied to fiduciary duty.
- CEO accountability: CEO signs off on migration funding and execution. Delegation to CTO or CISO is operational, not governance.
- Quantum Risk Committee or its equivalent: sub-committee of the board with authority to enforce CBOM accuracy, vendor compliance and budget allocation.
- Integration with enterprise risk management: PQC migration embedded into ERM frameworks; quantum exposure listed as a top-tier systemic risk.
- Escalation protocols: vendor non-compliance, internal delays or supervisory queries trigger immediate escalation.
- Reporting cadence: PQC migration is a standing agenda item in quarterly board sessions and in the annual ICT operational-resilience attestation.

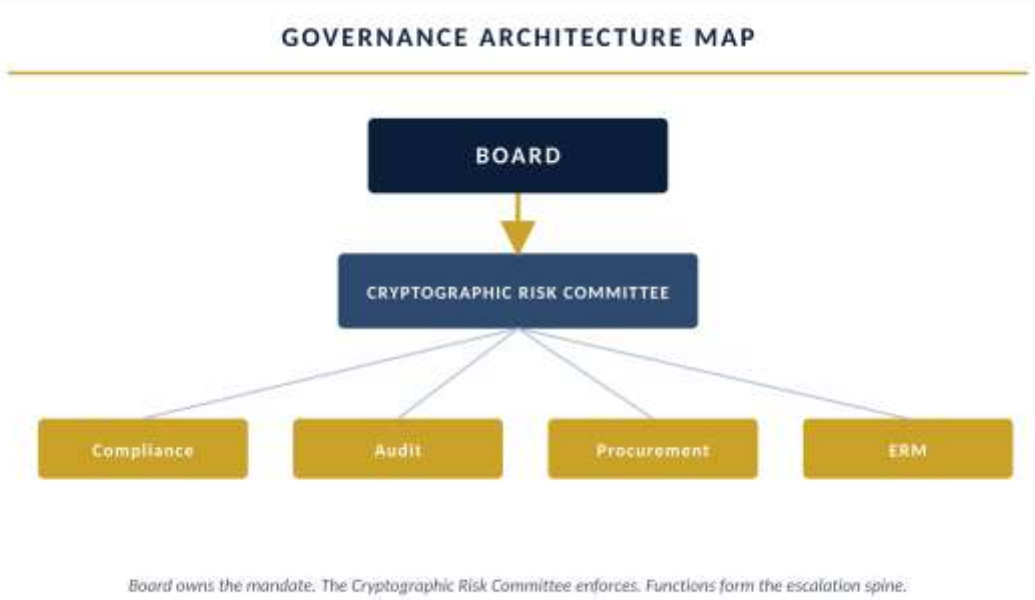

Figure 18. Governance Architecture Map. Board owns the mandate. The Risk Committee enforces. Compliance, audit, procurement and ERM form the escalation spine.

References on this page • OECD (2023) G20/OECD Principles of Corporate Governance. • BIS Committee on Payments and Market Infrastructures (2016, updated 2021) Guidance on cyber resilience for financial market infrastructures. • FSB (2023) Cyber Lexicon (revised). • EU Regulation 2022/2555 (NIS2) Art. 20 (management body accountability); EU Regulation 2022/2554 (DORA) Art. 5 (ICT risk management). • SEC 17 CFR 229.106 (Reg S-K, Item 106); FCA SYSC 13; APRA CPS 234.

8.2 Regulatory and Strategic References by Jurisdiction

The urgency of PQC transition is dictated by an interlocking family of global standards and supervisory instruments. Boards operating across borders must satisfy multiple regimes simultaneously.

8.2.1 United States

- NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), final 13 August 2024.
- FIPS 206 (FN-DSA / FALCON) in development; HQC selection (NIST IR 8545, 11 March 2025); draft 2026, final 2027.
- NIST IR 8547, Transition to Post-Quantum Cryptography Standards (initial public draft, November 2024): expected transition approach, with deprecation from 2030 and disallowance from 2035.

- NIST CSWP 39 (cryptographic agility, 19 December 2025); CSWP 48 (PQC capability mappings, September 2025 draft).
- NSA CNSA 2.0 (December 2024) for National Security Systems and the vendor ecosystem.
- CISA PQC Initiative and PQC product categories list; Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260, 2022); OMB M-23-02.
- SEC 17 CFR 229.106 (Reg S-K, Item 106) cybersecurity disclosure rules.
- FIPS 140-3 mandatory for new procurement from 21 September 2026 as FIPS 140-2 moves to Historical.

8.2.2 European Union

- European Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for PQC (11 April 2024).
- NIS Cooperation Group Coordinated Implementation Roadmap (June 2025): begin transition end-2026, high-risk infrastructure by 2030, complete 2035.
- European Commission COM(2026) 13 final (20 January 2026): a proposed directive which, if adopted, would insert Article 7(2)(k) into NIS2 requiring PQC transition policies in national cybersecurity strategies. In the legislative procedure at the date of writing; not yet binding.
- ECCG Agreed Cryptographic Algorithms v2 (May 2025).
- Regulation (EU) 2016/679 (GDPR) Article 32 state-of-the-art encryption requirement.
- Regulation (EU) 2022/2555 (NIS2) Article 21; Commission Implementing Regulation (EU) 2024/2690.
- Regulation (EU) 2022/2554 (DORA); Commission Delegated Regulation (EU) 2024/1774 (ICT risk RTS).
- eIDAS 2.0 (Regulation (EU) 2024/1183) and European Digital Identity Wallet requirements.
- ENISA Post-Quantum Cryptography integration studies (2024, 2025) and NIS2 Implementation Guidance (June 2025).

8.2.3 United Kingdom

- NCSC (2025) Timelines for migration to PQC: discover/plan to 2028, prioritise/pilot 2028–2031, complete 2031–2035.
- NCSC PQC migration guidance for critical infrastructure and public sector.
- UK GDPR and Data Protection Act 2018 (UK ICO encryption guidance).
- FCA SYSC 13; PRA SS1/21 Operational Resilience.
- Telecommunications Security Act 2021 and Code of Practice.
- Cyber Security and Resilience Bill (anticipated 2026).

8.2.4 Canada

- CCCS PQC Roadmap (June 2025): April 2026 departmental migration plans; 2031 high-risk migration complete; 2035 full transition.
- Treasury Board ITSG-33 controls; PIPEDA and provincial privacy statutes; Bill C-26 Critical Cyber Systems Protection Act.

8.2.5 Australia and New Zealand

- ASD Information Security Manual (2025): asymmetric cryptography not to be used beyond end-2030; refined plan end-2026; transition begin end-2028.
- SOCI Act (as amended by SLACIP); Cyber Security Strategy 2023–2030.
- APRA CPS 234; Privacy Act 1988 (Cth) and amendments.
- New Zealand NZISM cryptography standards.

8.2.6 Gulf Cooperation Council (GCC)

- UAE: TDRA Information Assurance Standards; UAE Cybersecurity Council Cyber Risk Management Framework; Federal Decree-Law 45/2021 PDPL; DESC Information Security Regulation; ADGM and DIFC data-protection regulations.
- Saudi Arabia: NCA Essential Cybersecurity Controls (ECC-1) and Critical Systems Cybersecurity Controls (CSCC); SAMA Cyber Security Framework; PDPL (2023).
- Qatar: NCSA National Information Assurance Framework; QFC Data Protection Regulations.
- Kuwait, Oman, Bahrain: NCAs aligned to GCC Cybersecurity Strategy; PDPL frameworks under reform.

8.2.7 ASEAN

- Singapore: CSA Cybersecurity Code of Practice for CII; MAS TRM Guidelines; PDPC PDPA; National Quantum Strategy.
- Malaysia: Cyber Security Act 2024; NACSA CII protection; PDPA 2010 (as amended 2024).
- Thailand: NCSA framework; PDPA 2019; Bank of Thailand technology-risk guidance.
- Indonesia: BSSN cyber-security; UU PDP 27/2022; OJK cyber-risk guidance.
- Philippines, Vietnam, Brunei, Cambodia, Lao PDR, Myanmar: ASEAN Cybersecurity Cooperation Strategy.

8.2.8 East Asia

- Japan: METI CRYPTREC PQC migration guidance; FSA TRM; APPI.
- South Korea: K-PQC initiative; KISA cryptographic guidance; PIPA.
- Taiwan: TWNIC and FSC cryptographic guidance; PDPA.
- Hong Kong: HKMA Supervisory Policy Manual SA-2; HKMA Quantum Preparedness Index (2026); PCPD PDPO.

8.2.9 South Asia

- India: National Quantum Mission Implementation of Quantum Safe Ecosystem (2025); CERT-In directions; RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023); DPDP Act 2023; SEBI cyber-security framework.
- Pakistan, Bangladesh, Sri Lanka: national CERTs, financial-sector cyber resilience frameworks.

8.2.10 Africa

- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, in force June 2023).
- South Africa: POPIA; SARB Cyber Resilience Standard; FSCA cyber-risk supervision.
- Kenya, Nigeria, Egypt, Morocco, Rwanda, Ghana: national cyber-security strategies and DPL statutes aligning to NIST and ENISA.

8.2.11 Latin America

- Brazil: LGPD; ANPD guidance; Banco Central do Brasil cyber-resilience requirements.
- Mexico: LFPDPPP; CNBV cyber-security circular.
- Argentina, Chile, Colombia, Peru, Uruguay: DPL authorities and financial supervisors aligning to ENISA and NIST.

8.2.12 Industry benchmarks

- Trusted Computing Group State of PQC Readiness 2025; Cloud Security Alliance PQC WG; PCI SSC PQC WG; SWIFT CSP PQC guidance.
- IFRS / ISSB sustainability disclosure standards where cyber-resilience intersects operational-resilience reporting.
- OECD (2025) Policy Brief on the Transition to Post-Quantum Cryptography.

References on this page • NIST FIPS 203/204/205 (2024); FIPS 206 (in development); NIST IR 8545 (2025); NIST IR 8547 (draft); CSWP 39 (December 2025); CSWP 48 (September 2025 draft); NSA CNSA 2.0 (2024). • European Commission Recommendation (EU) 2024/1101; NIS CG Roadmap (June 2025); COM(2026) 13 final; Regulations (EU) 2022/2555, 2022/2554, 2024/1183; Commission Delegated Reg 2024/1774. • UK NCSC (2025); CCCS (2025); ASD ISM (2025); APRA CPS 234. • TDRA UAE IAS; NCA KSA ECC-1 and CSCC; SAMA Cyber Security Framework; HKMA SA-2; MAS TRM (2021); Singapore CSA Cybersecurity Code of Practice. • OECD (2025); G7 Cyber Expert Group (2025); FSB (2023); BIS (2021); AU Malabo Convention (2014, in force 2023).

8.3 Compliance Integration

Quantum risk is a cross-jurisdictional compliance failure once standards are final. PQC migration must be mapped to every regulatory obligation that the enterprise carries.

- Privacy regimes: GDPR Article 32, UK DPA 2018, HIPAA, PIPEDA, LGPD, POPIA, PDPA Singapore, APPI, DPDP Act India, PDPL UAE, PDPL KSA, Australia Privacy Act, NZ Privacy Act, China PIPL, Russia FZ-152.
- Financial regulation: Basel BCBS 239, BCBS Principles for operational risk, EBA operational resilience, DORA Chapter II/V, MAS TRM, HKMA SA-2, APRA CPS 234, SAMA CSF, RBI Master Direction.
- Sectoral standards: ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27017, ISO/IEC 27018, NIST CSF 2.0, NIST SP 800-53 Rev. 5, COBIT 2019, PCI DSS v4.0.1, HITRUST CSF v11, SWIFT CSP, ASD Essential Eight.

Required action: compliance teams must document quantum exposure and embed PQC controls into frameworks. Failure to act may be regulatory negligence in any jurisdiction with state-of-the-art encryption obligations.

8.4 Strategic Intelligence Caveat

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

- Nation-state programmes are pursuing cryptographic dominance through undisclosed breakthroughs and parallel modalities.
- Public roadmaps from commercial laboratories reflect commercial and research milestones; they should not be relied on as threat timelines.
- Opaque state programmes accelerate the effective risk horizon by an unknown but non-negligible factor.
- Allied technical authorities consistently advise that migration planning should not be paced against public commercial timelines.

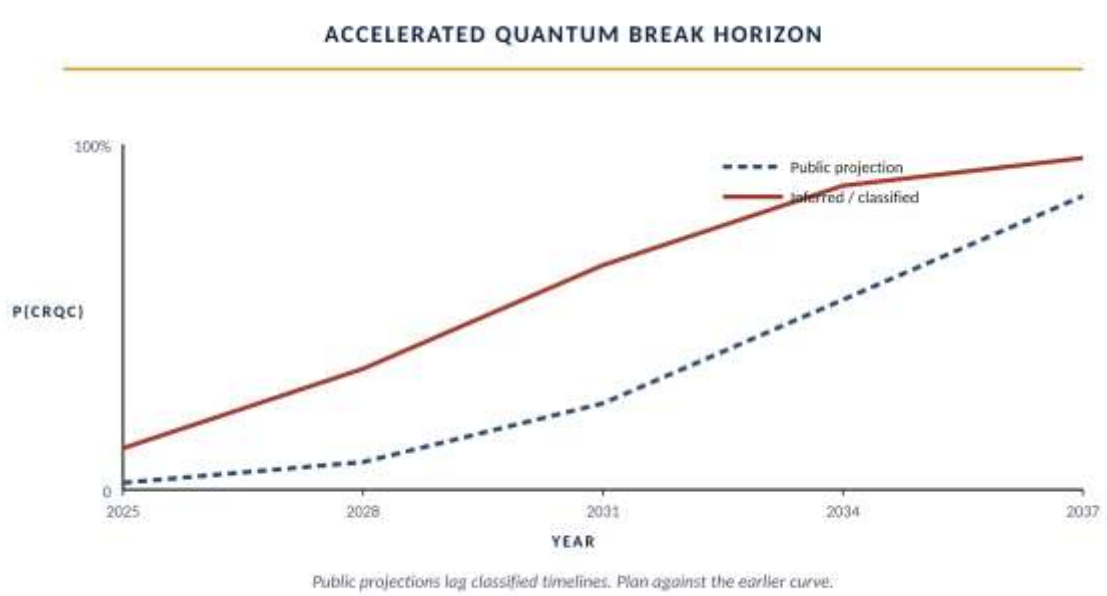

Figure 19. Accelerated Quantum Break Horizon. Public projections lag classified timelines. Real risk is earlier, silent and geopolitically driven.

Board action: treat NIST deprecation dates and the EU 2030 milestone as the latest acceptable date for completion of high-risk migration. Budgets and timelines must be accelerated.

8.5 Audit and Enforcement

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

- Quarterly CBOM audits: independent validation of completeness and accuracy.
- Vendor SLA compliance reports: PQC readiness declared, enforced contractually and tracked.
- Independent algorithm review: external validation of selection and implementation integrity, including side-channel resilience and downgrade prevention.
- Board reporting packs: PQC milestones and KPIs included in quarterly board materials and in annual ICT operational-resilience attestation.
- Supervisory engagement: proactive briefing of relevant supervisors (FCA, PRA, ECB-SSM, BaFin, AMF, EBA, ESMA, EIOPA, SEC, OCC, FRB, FDIC, NYDFS, MAS, HKMA, APRA, ASIC, SAMA, NCA, TDRA, RBI, SEBI).

8.6 The Quantum Readiness Maturity Model

Quantum-resistant cryptography requires a multi-year programme. Boards should manage fiduciary duty using a diagnostic framework that measures progress against the timing constraint imposed by Mosca's inequality.

The maturity model maps progression: Unprepared, Aware, Invested, Mitigated, Surviving. Survey data from TCG, Utimaco, ENISA and CSA consistently places organisations in the Unprepared or Aware stages, both of which carry unmanaged liability and HNDL exposure.

Boards should approve the budget and governance structure required to reach the Invested stage within the next fiscal year, with documented progression to Mitigated within 36 months and Surviving by the relevant 2030 or 2035 jurisdictional milestone.

- KPI: quarterly percentage of critical systems progressing from Aware to Mitigated.
- KPI: cumulative budget executed against multi-year approved envelope (Funding Adherence Index).
- KPI: percentage of Tier-1 vendor contracts with enforceable PQC clauses and submitted CBOMs.

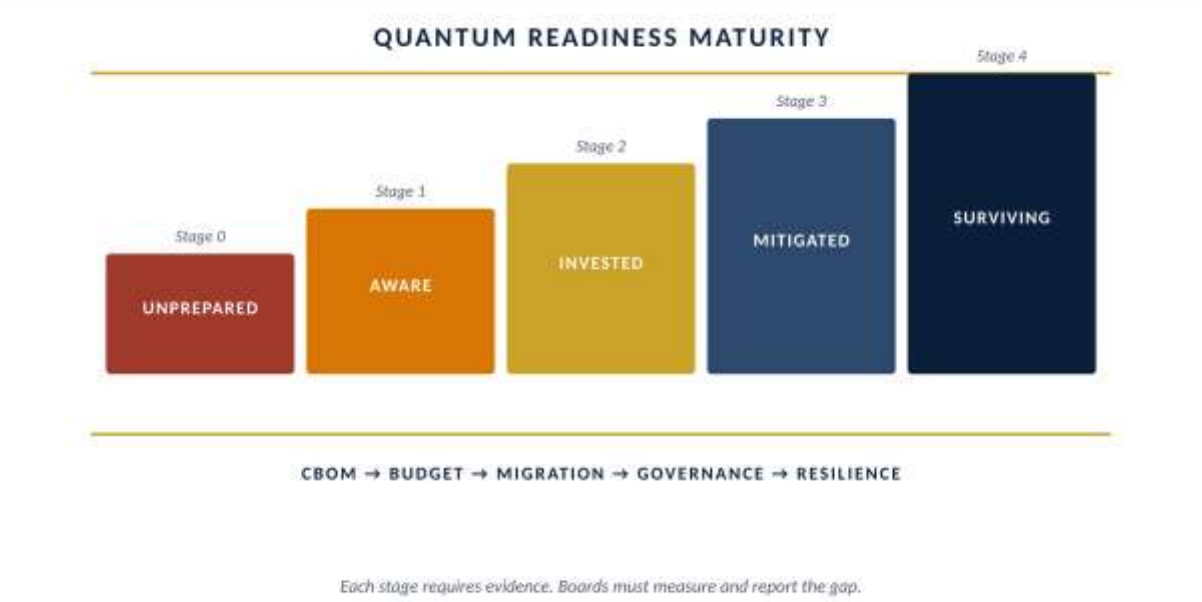

Figure 20. Quantum Readiness Maturity. Five stages from Unprepared to Surviving. CBOM, budget and migration define the path.

References on this page • EU Regulation 2016/679 (GDPR) Art. 32; UK DPA 2018; HIPAA Security Rule; LGPD; POPIA; PDPA Singapore; APPI; DPDP Act 2023 (India); PDPL UAE; PDPL KSA; Australia Privacy Act 1988. • BCBS 239 (2013); BCBS Principles for operational risk (2021); EU Regulation 2022/2554 (DORA); MAS TRM Guidelines (2021); HKMA SA-2; APRA CPS 234. • ISO/IEC 27001:2022; ISO/IEC

27002:2022; NIST CSF 2.0 (2024); NIST SP 800-53 Rev. 5; PCI DSS v4.0.1 (2024). • TCG (November 2025) State of PQC Readiness; Utimaco PQC Readiness Report 2025; ENISA (2024) PQC Integration Study; Cloud Security Alliance PQC WG.

8.7 Vendor Dependencies and Supply-Chain Cryptography

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

8.7.1 Vendor readiness is not organisational readiness

Security depends on a chain of trust. A vendor becoming PQC-ready only addresses the primitives within their product. It does not address internal inventory, data confidentiality lifetime or the multi-year process of deploy, test and integrate across dependent internal systems and APIs.

8.7.2 Vendors cannot reduce the risk variables

Vendors cannot reduce X (migration time across the enterprise ecosystem). Vendors cannot reduce Y (confidentiality lifetime, which is dictated by regulation, contract and business strategy). If X + Y > Z, data loss is mathematically guaranteed regardless of vendor updates.

Figure 21. Security Risk Layers. Vendor cryptography, enterprise integration and board liability. Each layer compounds quantum exposure.

8.7.3 Supply-chain crypto: the blind spot

Cryptographic security is embedded within APIs, dependencies, container images, firmware and external services. Supply-chain crypto is the largest blind spot.

- No visibility: without a CBOM that includes third-party dependencies, organisations have no insight into the quantum vulnerability of critical functions.
- Implied liability: if a vendor component fails under quantum attack, vendor non-compliance becomes the organisation's regulatory liability. Supervisors and counterparties increasingly require contractual flow-down under NIS2 Article 21, DORA Chapter V, US EO 14028 and UK TSA 2021.
- Sovereign concerns: cross-border vendor primitives may intersect with export-control regimes (US EAR, UK SECO, EU dual-use), data-sovereignty laws, and sectoral foreign-supplier restrictions.

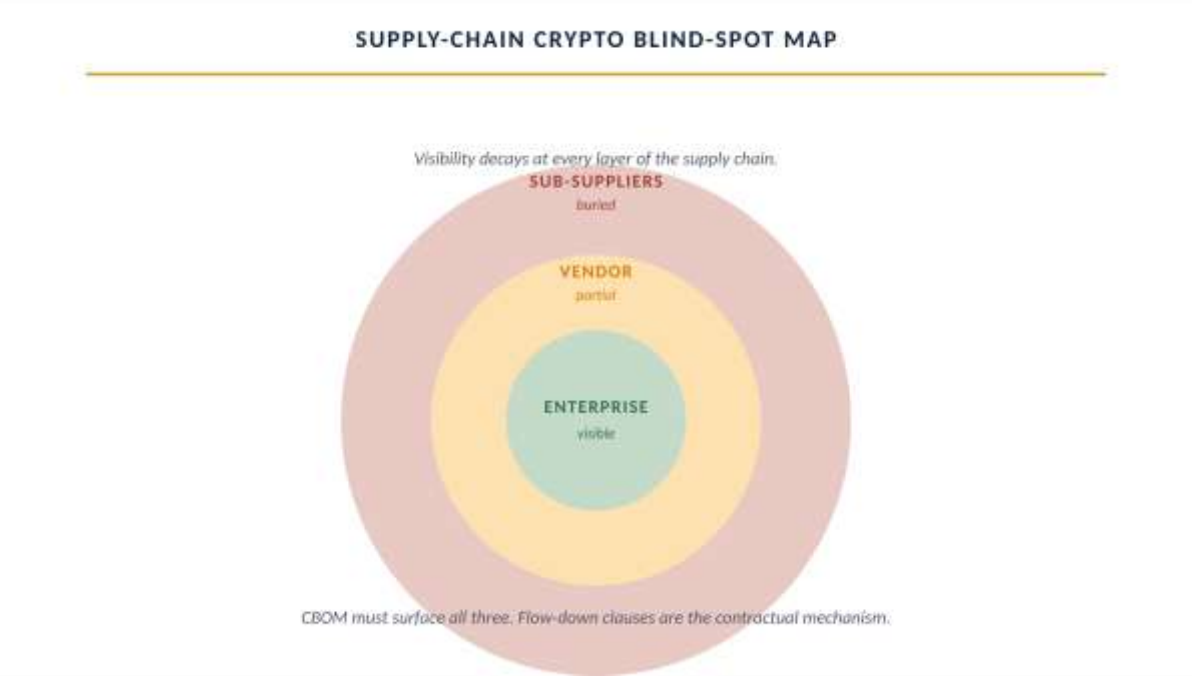

Figure 22. Supply-Chain Crypto Blind-Spot Map. Enterprise crypto is visible. Vendor and supply-chain layers remain buried. CBOM must surface all three.

8.7.4 Board mandate: crypto disclosure requirement

- Mandate: all critical technology vendors must provide cryptographic disclosure detailing transition timeline, PQC algorithms selected, validation status and supply-chain CBOM for product dependencies.
- This positions the organisation to actively manage X and to move from Unprepared to Aware or Invested on the maturity model.

- The cryptographic readiness check becomes mandatory in vendor due diligence, contract negotiation and procurement scoring.

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 across every jurisdiction in which the enterprise operates and validate execution through independent audit. Delegation may mean failure. Delay increases organisational liability exposure. Failure to act may be a breach of duty of care with financial consequences.

References on this page • EU Regulation 2022/2554 (DORA) Chapter V (ICT third-party risk); Commission Delegated Reg 2024/1774; EU Regulation 2022/2555 (NIS2) Art. 21. • US Executive Order 14028 (Improving the Nation's Cybersecurity); CISA Software Bill of Materials guidance. • UK Telecommunications Security Act 2021; UK NCSC Supply Chain Security guidance. • CycloneDX 1.6 Cryptographic Asset Extension; OWASP CBOM Project. • OECD (2025) Transition to PQC Policy Brief; ENISA (2024) PQC Integration Study.

CHAPTER

9. Rebuttal Section: Dismantling Organisational Inertia

This section addresses the misconceptions used to justify delay, underfunding or inaction. Each argument reflects a failure to differentiate between algorithm types or jurisdictional regimes, and each maps directly to board-level financial and legal exposure.

9.1 The Symmetric versus 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 PQC migration is premature.

Rebuttal: AES-256 survives Grover with reduced security margin. The existential danger is the asymmetric collapse of RSA, finite-field DH and ECC under Shor. If the asymmetric key exchange fails, the symmetric session key is compromised. The root of trust (PKI) fails first.

Mandate: boards should require the distinction between symmetric survivability and asymmetric collapse. PQC migration targets asymmetric cryptography. Symmetric upgrades alone are insufficient if the foundation has failed.

9.2 TLS and Protocol Vulnerabilities

Organisations often mistake protocol configuration changes for cryptographic agility, assuming TLS updates contain the threat.

Myth: TLS 1.3 ephemeral keys or routine TLS upgrades 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 (X25519MLKEM768 and successors) are the migration bridge, not the destination.

Mandate: protocol upgrades must include PQC primitives in hybrid configuration. Relying on legacy TLS is a failure to meet the standard of care.

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: FIPS 203, 204 and 205 are final and in production at hyperscale: Cloudflare, AWS, Google, Microsoft, Apple PQ3 and Signal PQXDH. FIPS 140-3 validated modules are commercially available. Vendor maturity is a function of customer demand. Waiting accelerates the certificate-lifecycle squeeze and FIPS 140-2 sunset constraints without resolving HNDL exposure.

9.4 The Wait-and-See Fallacy

Some boards still assume Q-Day will be announced and that vendor patches will be available in time.

Myth: We can wait until quantum threats materialise.

Rebuttal: HNDL is operational now. The Federal Reserve FEDS 2025-093, G7 CEG, ECB, BIS, BoE, MAS, HKMA and ASD treat it as a present risk. By the time Q-Day is recognised publicly, data harvested over preceding years and decades stands to be decrypted. Migration takes years. Mosca's inequality treats migration time as the deadline, not Q-Day.

Mandate: the only defensible answer is to start now, fund the CBOM and approve the roadmap.

References on this page • Shor (1994); Grover (1996); Mosca (2018). • NIST FIPS 203/204/205 (2024); CNSA 2.0 (2024); CSWP 39 (December 2025). • IETF draft-ietf-tls-hybrid-design; Cloudflare X25519MLKEM768 deployment data; Apple PQ3 (2024); Signal PQXDH (2023). • Federal Reserve FEDS 2025-093 (2025) Quantum Risk in Financial Networks. • G7 Cyber Expert Group (2025) PQC roadmap for the financial sector; BIS Innovation Hub Project Leap.

CHAPTER

10. Legal and Compliance Implications: The Global Liability Bridge

This chapter sets out the cross-jurisdictional liability framework attaching to PQC inaction. Boards should treat this as legal preparedness, not legal theory.

10.1 Breach of Fiduciary Duty: Foreseeable Harm

Failure to act on a quantifiable, standardised risk after standards have been finalised may, in many jurisdictions, support a finding that directors and officers failed in their duty of care.

- Failure of oversight: not establishing the Quantum Risk Committee or equivalent and neglecting its mandates.
- Information ignorance: dismissing the findings in this paper or in supervisory and standards publications.
- Misallocation of capital: treating PQC migration as a discretionary IT cost instead of a mandatory resilience investment.
- Documented inaction: failure to initiate CBOM within six months of receiving evidence of HNDL exposure may establish a record of negligence.
- Board minutes: failure to record PQC migration as a standing agenda item may itself constitute evidence of inadequate oversight.

10.2 Regulatory Enforcement and Penalties by Jurisdiction

Global data-protection and operational-resilience regimes increasingly require state-of-the-art security. With FIPS 203/204/205 finalised and EU, UK, Canadian, Australian, GCC, ASEAN, Japanese and Korean roadmaps published, classical-only cryptography no longer meets the standard for long-lived data.

- European Union: GDPR Article 32 (administrative fines up to 4 percent of global turnover); NIS2 enforcement up to 2 percent of global turnover with personal sanctions for senior management; DORA supervisory powers including remediation orders.
- United Kingdom: UK GDPR and DPA 2018 (penalties up to 4 percent of global turnover); FCA and PRA enforcement under Principles for Businesses, SYSC, SS1/21.
- United States: SEC Reg S-K Item 106 disclosure and Form 8-K material incident reporting; FTC Section 5; state-AG enforcement under CCPA/CPRA, NYDFS Part 500; HHS HIPAA Security Rule; federal contracts under DFARS 7012 and CMMC.

- Canada: PIPEDA penalties; OPC enforcement; Bill C-26 penalties up to CAD 15 million per violation.
- Australia: Privacy Act civil penalties (up to AUD 50 million or 30 percent of adjusted turnover); SOCI Act enforceable directions; APRA enforcement actions.
- GCC: SAMA, NCA, TDRA, QCB and CBUAE enforcement under PDPL frameworks; supervisor-led restitution orders; ECC-1 and CSCC findings.
- ASEAN: MAS supervisor-led remediation and licensing impact; PDPC fines up to SGD 1 million or 10 percent of annual turnover; HKMA and PCPD enforcement; Malaysia NACSA enforcement.
- Latin America and Africa: ANPD (Brazil), POPIA Information Regulator (South Africa), CNBV (Mexico) and equivalent authorities enforcing state-of-the-art encryption under LGPD, POPIA and sectoral standards.

10.3 The Emergence of Cyber Liability Law

Legal consensus across major jurisdictions points to the board's role in cybersecurity governance as non-delegable.

- SEC Cybersecurity Disclosure Rules (US): material cybersecurity incidents require timely disclosure on Form 8-K. A future HNDL decryption event would be material.
- D&O liability: claims increasingly cover negligent oversight of cyber preparedness. Inaction on PQC may provide plaintiffs with a clear path to alleging breach of duty of care.
- Contractual enforcement: legal teams should include PQC compliance clauses in vendor and supply-chain contracts. Absence exposes principals to vendor negligence.
- Insurance exclusions: cyber insurers increasingly exclude or sub-limit losses arising from known, unmitigated cryptographic risk. Boards cannot rely on insurance as mitigation.
- Securities and stock-exchange liability: failure to disclose PQC risk in investor filings may constitute securities fraud under SEC, FCA Listing Rules, ESMA, JFSA, MAS, HKEX and ASIC guidance.

10.4 Investor and Class-Action Liability

Beyond regulatory fines, a quantum breach creates immediate litigation exposure across jurisdictions that recognise class-action mechanisms (US Rule 23, UK CPR 19.10, Australia Part IVA Federal Court Act, Netherlands WAMCA, Brazil CDC mass actions, the EU Representative Actions Directive 2020/1828).

- Shareholder derivative suits: failure to protect corporate assets against a standardised threat supports allegations of mismanagement.
- Class-action risk: HNDL-enabled mass decryption of PII will trigger consumer actions in every jurisdiction with a class-action mechanism.

- Securities-fraud exposure: undisclosed material PQC risk in investor filings may attract regulator and private actions.

10.5 Strategic Legal Mandates

General counsel should convert technical risk into legal preparedness.

- Formal risk assessment: legal should assess exposure of all datasets classified as long-secrecy (high Y).
- Contractual hardening: all new contracts must include PQC compliance clauses referencing NIST FIPS 203/204/205, NSA CNSA 2.0, ETSI TR 103 619 and the relevant regional roadmap.
- Personal liability review: confidential review of D&O exposure concerning PQC inaction, using this paper and supervisory publications as the documented standard of care.
- Regulator engagement: general counsel should proactively brief supervisors, demonstrating PQC migration plans to mitigate enforcement risk.
- Audit linkage: legal mandates integrated into CBOM audits, vendor due diligence and board reporting packs.

Required action: legal and compliance must integrate PQC into control frameworks and audit cycles. The cost of migration is minimal compared with punitive fines, supervisor-led remediation, civil litigation and personal liability arising from a quantum breach.

References on this page • EU Regulation 2016/679 (GDPR); UK DPA 2018; SEC 17 CFR 229.106; HIPAA Security Rule 45 CFR §164.312. • EU Regulation 2022/2555 (NIS2); EU Regulation 2022/2554 (DORA); Commission Delegated Reg 2024/1774. • Privacy Act 1988 (Cth) and Privacy and Other Legislation Amendment Act 2024; APRA CPS 234. • Canada PIPEDA; Bill C-26 Critical Cyber Systems Protection Act. • UAE Federal Decree-Law 45/2021 (PDPL); KSA PDPL; Brazil LGPD; South Africa POPIA; Singapore PDPA. • EU Directive 2020/1828 on Representative Actions; FRCP Rule 23.

CHAPTER

11. Strategic Survival KPIs: Measuring Solvency, Not Activity

These are solvency KPIs. They measure whether the board has discharged its duty of care in the face of a foreseeable and standards-recognised risk. They are auditable, binary and escalation-ready. Quarterly review by the Risk Committee is mandatory, and the same KPIs are suitable for supervisory reporting under DORA, NIS2, SEC, MAS, HKMA, APRA and equivalent regimes.

Figure 23. Strategic Survival KPIs Dashboard. CBOM, roadmap and governance define solvency. Red-zone breaches trigger escalation.

11.1 Visibility and Auditability (CBOM Focus)

Visibility is the precondition for solvency. If the board cannot see cryptographic exposure, it cannot survive it.

CBOM Completion Score

- Definition: percentage of Tier-1 systems with a CBOM that is 100 percent accurate and dynamically updated.
- Target: 95 percent within 12 months.

- Audit evidence: continuous CBOM scan reports, date-stamped inventories, audit logs proving no manual overrides.
- Red flag: score below 80 percent 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, hard-coded keys, custom crypto libraries.
- Red flag: discovery rate drops to zero.

Risk Prioritisation Accuracy

- Definition: percentage of vulnerable assets correctly ranked by Y factor (data confidentiality lifetime).
- Target: 99 percent accuracy.
- Audit evidence: third-party validation of classification lifecycle.
- Red flag: any high-value IP or PII with Y greater than ten years left mis-classified.

11.2 Mitigation and Deployment (Roadmap Focus)

Execution against the transformation roadmap is the measure of operational solvency. Delay is liability.

HNDL Remediation Rate

- Definition: percentage of high-value, long-lived datasets re-encrypted using hybrid PQC.
- Target: 90 percent within 24 months.
- Audit evidence: database records showing dual-encryption status; Y-factor reduction reports.
- Red flag: remediation rate falls below roadmap trajectory for two consecutive quarters.

PKI Agility Score

- Definition: percentage of PKI components migrated to hybrid PQC or post-classical primitives.
- Target: 100 percent within 18 months for Tier-1 issuance hierarchies.
- Audit evidence: certificate transparency logs, internal CA adoption reports, HSM attestation.
- Red flag: any critical service still using pure RSA or ECC after 12 months.

Test Lab Readiness

- Definition: PQC test environment fully operational, simulating load and latency under hybrid and pure-PQC modes.
- Target: 100 percent within six months.
- Audit evidence: load testing reports, hardware sign-offs, latency metrics, side-channel analysis.

- Red flag: test environment unavailable after six months.

11.3 Governance and Enforcement (Risk Committee Focus)

Governance is survival architecture. Funding and compliance are non-negotiable.

Funding Adherence Index

- Definition: actual spending versus mandated solvency expenditure.
- Target: 100 percent 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 and the relevant regional roadmap.
- Target: 95 percent within 18 months.
- Audit evidence: legal review of contracts; Risk Committee sign-off on vendor roadmaps.
- Red flag: refusal by any critical vendor to provide a PQC compliance roadmap or CBOM.

Fiduciary Mandate Compliance

- Definition: quarterly RAG rating by Risk Committee on board adherence to PQC resolutions.
- Target: continuous Green.
- Audit evidence: board minutes recording approvals; audit logs of board action.
- Red flag: Amber or Red for two consecutive quarters.

11.4 Board Directive: Accountability Mandate

Failure to meet the targets defined above is not a technical delay. It is a governance failure. These KPIs are the board's final line of defence in supervisory dialogue, civil litigation and shareholder challenge.

The Risk Committee is mandated to:

- Report escalations: any red-flag condition reported directly to the CEO and chair.
- 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 Committee should document all escalations as evidence of fiduciary compliance, ensuring liability transfer is explicit and defensible.

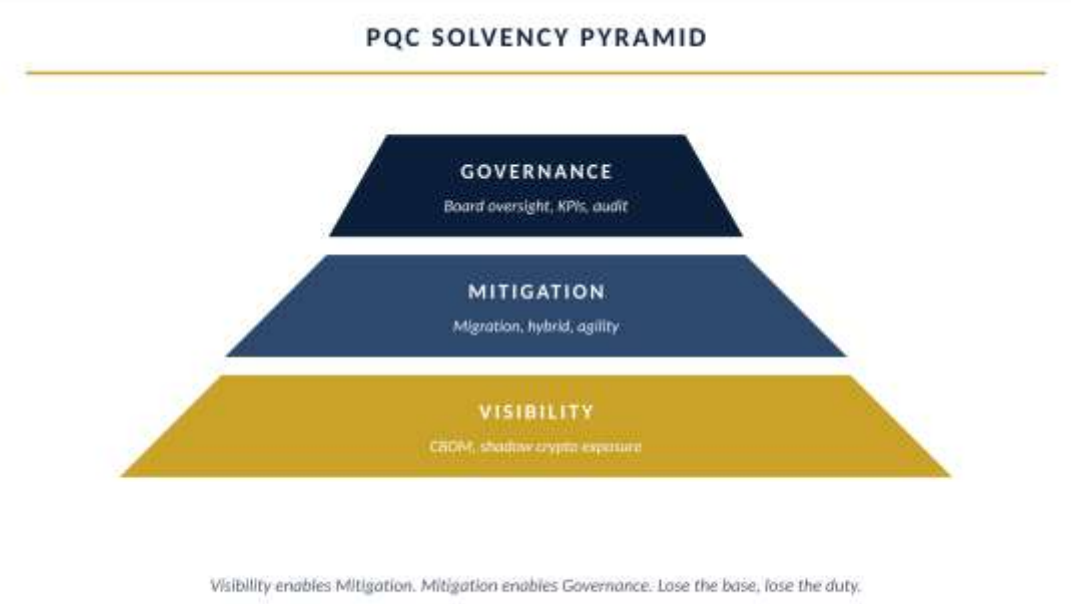

Figure 24. PQC Solvency Pyramid. Visibility enables mitigation. Mitigation enables governance. Board duty collapses if the base fails.

References on this page • NIST CSWP 39 (December 2025) Cryptographic Agility; NIST CSWP 48 (September 2025 draft) PQC Capability Mappings. • EU Regulation 2022/2554 (DORA) Art. 6, 9, 28; Commission Delegated Reg 2024/1774. • EU Regulation 2022/2555 (NIS2) Art. 21, 23. • FCA SYSC 13; PRA SS1/21; APRA CPS 234; MAS TRM Guidelines (2021); HKMA SA-2. • SEC 17 CFR 229.106 (Reg S-K, Item 106); 17 CFR 229.305.

CHAPTER

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 infrastructure without disruption. NIST CSWP 39 (December 2025) formalises this as essential capability, with a maturity model that supervisors and auditors are already adopting.

- Abstraction layers: encapsulate cryptographic calls within dedicated modules or services, isolating them from business logic. Avoid direct application coupling to library APIs.
- Centralised policy: enforce algorithm selection from a single control plane, with cryptographic policy distributed through configuration management.
- Metadata integration: generate algorithm, parameter and key metadata for CBOM inclusion and audit traceability. Align with CycloneDX cryptographic asset extension and SPDX 3.0 cryptographic profile.
- Lifecycle automation: automated key rotation, certificate lifecycle (ACME, EST, SCEP) and post-quantum-ready PKI hierarchies prepared for CA/B Forum certificate-lifetime reductions.

12.2 The Q-Resilience Mindset

Quantum resilience is a strategic mindset embedded in corporate culture, supply-chain expectations and procurement instruments.

- Assume failure: all cryptography is temporary. Plan for the next migration before the current one is complete.
- Minimise data lifetime: reduce Y in Mosca's inequality through strict retention, minimisation and lawful destruction policies.
- Mandate agility: systems without cryptographic agility are security debt requiring remediation, not new procurement.

12.3 Quantum Key Distribution Caveat

Quantum Key Distribution (QKD) is an optical key-exchange technology with limited operational scope and important caveats.

- Limited scope: photon loss restricts reliable operation; specialised fibre or satellite links are required.
- No general solution: QKD does not secure data at rest, does not address signature schemes and does not natively support common protocols such as TLS.
- Standardisation status: ETSI ISG-QKD specifications; ITU-T Y.3800-series. ENISA, NCSC, NSA and ASD have all explicitly warned that QKD does not substitute for PQC migration.
- Strategic research: QKD may complement PQC for very-high-value point-to-point links, particularly in defence, diplomatic and sovereign infrastructure. It does not delay PQC migration.

12.4 Quantum Incident Response Plan

PQC migration must conclude with a formal Quantum Incident Response Plan (Q-IRP) anticipating an unannounced quantum break or a discovered cryptanalytic weakness in a deployed PQC family.

- Decryption contingency: identify and protect data exposed by a post-breach decryption event; pre-position re-encryption tooling and key rotation procedures.
- PKI revocation: predefined procedures for global certificate revocation, OCSP stapling, CRL distribution and emergency root-of-trust replacement.
- Forensic protocol: analyse logs, telemetry and metadata to determine breach scope and notification obligations across jurisdictions.
- Regulator notification: pre-drafted templates for SEC Form 8-K, NIS2 Article 23 incident reporting, DORA Article 19, MAS, HKMA, APRA, SAMA and equivalent disclosure regimes.

Required action: the Q-IRP must be drafted, tested and rehearsed before the conclusion of the transformation programme (Gate 6: BAU Handover) and reviewed annually thereafter.

12.5 Strategic Continuity Mandate

Cryptographic agility is a permanent governance function, not a project deliverable.

- Horizon watchlist: monitor lattice cryptanalysis (BKZ sieving, GPU-accelerated attacks), side-channel discoveries, AI-accelerated cryptanalysis, and next-generation primitives (FN-DSA, HQC, post-lattice candidates).
- Strategic intelligence integration: feed horizon data into board briefings, vendor contracts and procurement scoring.
- Survival architecture extension: extend the PQC Solvency Pyramid to include cryptographic horizon intelligence as a permanent layer.

- Funding mandate: allocate budget for cryptographic R&D and maintain test environments for emerging standards (FIPS 206, HQC draft, additional digital-signature schemes from NIST onramp).

12.6 Anticipating the Emergent

Boards should prepare for primitives not yet conceived and attack vectors not yet demonstrated.

- Post-lattice breakthroughs: prepare for code-based, multivariate, isogeny-based or zero-knowledge constructs becoming primary stacks if lattice families weaken.
- AI and quantum hybrid attacks: anticipate adversaries combining quantum computing with AI-accelerated cryptanalysis, GPU clustering and side-channel automation.
- Entropy collapse: diversify entropy pools (hardware RNGs, TEE-anchored randomness, NIST SP 800-90 compliant DRBGs) and mandate continuous entropy audits.
- Blockchain and digital-asset risks: address PQC migration for smart contracts, Layer-2 protocols, dormant assets, central-bank digital currency designs and tokenised securities settlement.

12.7 Board Call to Action

- Approve a permanent Risk Committee mandate to track post-PQC threats quarterly.
- Enforce future-proofing clauses in vendor contracts.
- Fund cryptographic R&D and sandboxing of unstandardised primitives.
- Treat cryptographic obsolescence, including primitives not yet invented, as potential fiduciary risk.

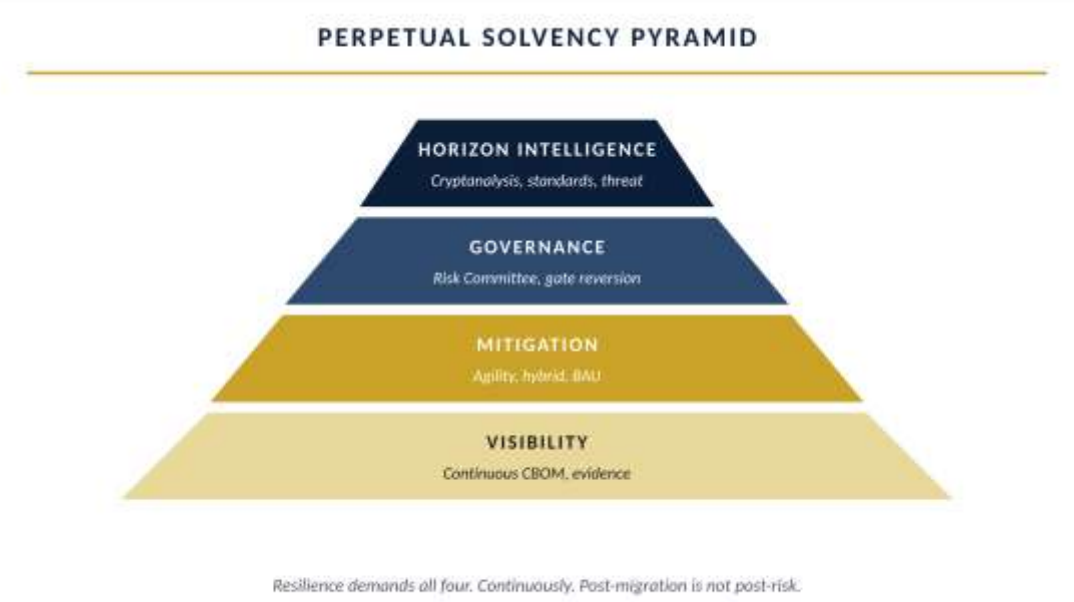

Figure 25. Perpetual Solvency Pyramid. Visibility, mitigation, governance and horizon intelligence. Resilience demands all four, continuously.

References on this page • NIST CSWP 39 (December 2025); NIST IR 8547 (transition draft). • ETSI ISG-QKD specifications; ITU-T Y.3800-series; ENISA (2023) Post-Quantum Cryptography – Anticipating Threats and Preparing the Future. • NIST SP 800-208 (Stateful Hash-Based Signatures); NSA CNSA 2.0 firmware-signing guidance. • CA/Browser Forum SC-081v3 (certificate-lifetime reductions). • BIS Innovation Hub Project Leap (2024–2025); BIS Project Pyxis (CBDC quantum-safe design).

CHAPTER

13. Case Studies: Systemic Failure Pattern Overview

Boards often dismiss quantum risk as speculative physics. History documents the opposite: cryptographic obsolescence is a recurring, predictable governance failure. The pattern is forensic and crosses industries, decades and jurisdictions: visibility failure, delayed decryption, solvency expenditure under pressure, migration inertia. Across the cases that follow, delayed action repeatedly converted a technical issue into solvency liability.

Each case is examined under Context, Failure, Impact and Board Lesson. The iceberg below renders the shared substrate.

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:

Visibility failure (Equifax)

- Context: lack of cryptographic visibility.
- Failure: blind inventory and expired certificate on a network inspection device.

- Impact: USD 1.38 billion in remediation, settlements and supervisory penalties; 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 triggering a global scramble.
- Impact: USD 300–600 billion globally in 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: twelve-year delay culminating in the SHAttered collision attack and emergency migration.
- Board lesson: migration always takes longer than predicted; delay guarantees exposure.

Cryptographic failures are not technology failures. They are governance failures. Each precedent demonstrates the same pattern: delayed action converts predictable technical degradation into solvency damage.

References on this page • GAO (2018) Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (GAO-18-559). • NSA (1996) VENONA: Soviet Espionage and the American Response 1939–1957; NARA VENONA archives. • GAO (1999) Year 2000 Computing Crisis: Business Continuity and Contingency Planning (AIMD-10.1.19). • Stevens et al. (2017) The first collision for full SHA-1; shattered.io.

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 egress traffic left the network uninspected because the tool could not decrypt it.

Cost: USD 1.38 billion in remediation, fines and settlements; subsequent SEC, FTC, multi-state AG and UK ICO penalties; sustained reputational damage and director departures.

Forensic link to quantum risk: Equifax suffered from certificate blindness, the same condition that produces shadow crypto exposure today. The breach was not caused by a quantum computer but by a lack of visibility – the precise failure mode that the CBOM is designed to eliminate.

Forced-expiration parallel: just as the Equifax certificate expired unnoticed, quantum computing will cause the silent invalidation of security guarantees upon CRQC availability. Without a CBOM, boards will be blind to that expiration until after data is exfiltrated and decrypted.

Mosca application: time to discover the failure (X) was 76 days. Y was indefinite (consumer credit data has lifetime measured in decades). The vulnerability window (Z) was immediate. X exceeded Z; solvency was impacted.

Lesson: you cannot secure what you cannot see. A missing CBOM is a material risk today, not only in the quantum future.

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

Analog: proof that Harvest Now, Decrypt Later is standard tradecraft, not theoretical risk.

Event: during the Second World War and into the early Cold War, US and British signals intelligence harvested thousands of encrypted Soviet diplomatic cables. At the time of capture, the cables were secured by one-time pads considered mathematically unbreakable.

Decryption event: the cables were captured in the 1940s and stored. Years later, cryptanalysts at Arlington Hall discovered a flaw in pad generation. Over 37 years, the NSA decrypted these messages, exposing atomic spies, espionage networks and diplomatic positions long after the participants believed the data was safe.

Modern intelligence-community framing: G7 CEG (2025), the Federal Reserve FEDS 2025-093 (2025), ECB, BIS, NCSC, ASD, CCCS and Five Eyes joint statements now classify HNDL as a present operational risk. The Bundesnachrichtendienst and BSI public statements confirm that adversary harvesting programmes are active. The pattern is no longer historical curiosity; it is the contemporary operating environment.

Retroactive decryption: data encrypted today with RSA-2048 is being harvested. When Shor is applied, decryption will be retroactive, as it was with VENONA.

Implementation risk: VENONA failed due to implementation, not mathematics. PQC adoption faces the same risk through side-channel attack, fault injection and decryption-failure-rate analysis. This validates the necessity of cryptographic 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, your archives are likely already in a foreign harvest queue 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, telecommunications, transport and infrastructure systems due to a legacy date-format error embedded across decades of code.

Spend: organisations spent hundreds of billions globally on remediation (commonly cited at USD 300–600 billion).

Solvency lesson: critics cite Y2K as a hoax because aircraft 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.

Ten-times premium: Y2K had a fixed deadline (Z). PQC has an unknown deadline. Banks that funded remediation in 1996 paid standard rates. Organisations that waited until late 1999 scrambled and paid up to ten times the premium for contractors and rushed implementations. The pattern repeats for any deadline-driven cryptographic transition.

Lesson: the cost of orderly migration is high. The cost of panic is higher. PQC migration is the Y2K-scale event of the present decade, with no fixed date to force action. Spending now is solvency insurance. Spending later is a distress purchase.

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

Analog: the operational reality of how long migration (X) takes.

Event: in 2005 the SHA-1 hash function was shown theoretically broken by Wang, Yin and Yu. NIST deprecated SHA-1 in 2011.

Inertia: despite warnings, industry delayed. In 2017 Google demonstrated the SHAttered collision attack, forcing emergency migration across browsers, CAs, code-signing infrastructure, document signing, version-control systems and embedded firmware.

Operational reality: migration took twelve years from theoretical risk to active exploit. Vendors, legacy hardware and hard-coded dependencies stalled the transition. Some embedded environments still carry SHA-1 residue in 2026.

Quantum parallels: if PQC migration takes twelve years and a CRQC arrives in ten, the inequality $X + Y > Z$ is unconditionally violated.

Lesson: migration always takes longer than predicted. Starting now is the only way to compress X to fit inside 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 confirms implementation risk. Y2K demonstrates that early solvency expenditure prevents catastrophe while delay incurs a panic premium. SHA-1 shows that migration inertia is the norm, not the exception.

Boards should treat PQC migration as a solvency expenditure, enforced through CBOM completion, roadmap funding and governance mandates now.

References on this page • GAO (2018) GAO-18-559 Equifax breach analysis; SEC complaint and consent orders; FTC Equifax settlement. • NSA (1996) VENONA: Soviet Espionage and the American Response; NARA VENONA archives. • Federal Reserve Board FEDS 2025-093 (2025); G7 Cyber Expert Group (2025) PQC roadmap. • GAO (1999) AIMD-10.1.19 Year 2000 contingency planning. • Wang, Yin & Yu (2005) Finding collisions in the full SHA-1; Stevens et al. (2017) The first collision for full SHA-1; NIST SP 800-131A Rev. 2 (2019).

CHAPTER

14. Societal Wellbeing and ESG Risk Impacts

Retroactive decryption is a present environmental, social and governance (ESG) risk. It destroys privacy and trust. PQC migration is a 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 PQC migration plan are governance-deficient and create material liability for shareholders, employees, customers and the public.

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, sexual-health data, immigration files and identity attributes 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, water-treatment SCADA, transport signalling, defence procurement and critical blueprints, can cascade into service outages, supply-chain failures, public-safety incidents and geopolitical destabilisation.

14.1.4 Equity and vulnerability. Remediation is costly and slow. People with limited resources, low digital literacy or weak legal protections, and populations in jurisdictions without modern privacy or class-action frameworks, 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 immediately.

14.2 Post-Quantum Vulnerability as a Governance Failure

14.2.1 Fiduciary duty. Boards should treat PQC migration as a core fiduciary obligation. Failing to secure long-lived, sensitive encrypted data against a known, quantifiable, standards-published threat may be categorised as a governance failure in any jurisdiction with modern director duty-of-care principles.

14.2.2 Materiality. Social and governance impacts are material now. Organisations must classify post-quantum vulnerability as an ESG risk in risk registers, in IFRS S2 sustainability disclosures, in CSRD/ESRS reporting, in SASB-aligned filings and in equivalent regional frameworks. The threat maps to the Social pillar through irreparable privacy destruction and to the Governance pillar through inadequate 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, securities-class-action risk and personal fiduciary liability for board members.

> Key point 14.2. Post-quantum 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.

- Protect people first. Prioritise migration for health records, identity systems, financial data, refugee and immigration files, and critical-infrastructure control systems.
- Assign executive accountability. Require PQC resilience KPIs in CISO, CIO, CRO, CDO and General Counsel performance metrics, tied to measurable consequences.
- Mandate transparency. Require public reporting of cryptographic inventories, migration milestones and remediation plans so stakeholders, supervisors and customers can verify progress.
- Embed equity. Include an equity assessment in data triage to identify and mitigate disproportionate impacts on vulnerable groups and on populations in jurisdictions with weaker remediation regimes.
- Targeted deadlines. Board-approved deadlines: complete cryptographic inventory within 90 days; approve funded transformation programme within 180 days; migrate top-tier high-impact data within 24 months; complete critical migrations within 48 months, aligning to EU 2030 and global 2035 milestones.

> 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, supervisors and stakeholders.
- Stakeholder communications. Prepare tested disclosure templates and remediation playbooks aligned to SEC Form 8-K, NIS2 Article 23, DORA Article 19 and equivalent reporting regimes.
- Remediation planning. Design support programmes for affected individuals including identity protection, fraud remediation and cross-border restitution.

14.4.2 Required metrics

- Technical progress. Percentage of high-impact data inventories completed; percentage migrated to PQC 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 PQC 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. PQC migration is 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 by orders of magnitude. Boards should act now.

Board checklist

- Complete cryptographic inventory within 90 days.
- Approve funded transformation programme 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.

References on this page • IFRS S2 Climate-related Disclosures (companion to S1); ISSB sustainability standards. • EU Directive 2022/2464 (CSRD); ESRS standards (Commission Delegated Regulation 2023/2772). • OECD (2023) Guidelines for Multinational Enterprises on Responsible Business Conduct. • UN Guiding Principles on Business and Human Rights (2011). • EU Regulation 2016/679 (GDPR) Art. 32; Council of Europe Convention 108+; AU Malabo Convention.

CHAPTER

15. Conclusion and Board Call to Action

The quantum security gap is a present governance and resilience challenge. Shor establishes the mathematical threat. The first-wave NIST standards are finalised, the second wave is in development, and enterprise solutions are deployed at hyperscale. The Harvest Now, Decrypt Later attack is operational, classified by central banks and intelligence-community publications as a present privacy risk. Fragmented global harmonisation is closing as the EU writes PQC into NIS2, the UK NCSC publishes a binding three-phase roadmap, Canada CCCS issues departmental deadlines, the ASD ISM bans asymmetric beyond 2030, and the G7 Cyber Expert Group adopts the same framing. Delay is increasingly difficult to justify.

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

PQC GOVERNANCE CHECK LIST

DIRECTIVE	OWNER	RAG
CBOM mandated and funded	*CISO*	GREEN
Cryptographic Risk Committee constituted	*Board*	GREEN
Tier entry decision approved at board	*Board*	AMBER
Gate 1 evidence pack signed off	*SteerCo*	AMBER
Vendor CBOM clauses in master contracts	*Procurement*	RED
Q-IRP drafted, tested, rehearsed	*CISO*	RED
Quarterly KPI reporting cadence active	*Risk Committee*	AMBER

No directive is optional. Each is board accountable.

Figure 28. PQC Governance Check List. Directives, owners and RAG status.

15.1 Survival Framing: Inaction as Negligence Defined

This paper establishes the PQC transition as a function of corporate survival. Any decision to delay, underfund or delegate responsibility converts a technical risk into legal and financial liability across every jurisdiction in which the enterprise operates.

- 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: when Y plus X exceeds Z, long-lived data loss is mathematically guaranteed under HNDL.
- Regulatory exposure: reliance on quantum-vulnerable algorithms for long-lived PII violates state-of-the-art expectations under GDPR, UK DPA, NIS2, DORA, HIPAA, PCI DSS v4.0.1, LGPD, POPIA, PDPA, APPI, DPDP, PDPL and equivalent regimes.
- Governance failure: chronic underfunding and lack of Risk-Committee oversight prevents accurate tracking of Survival KPIs and masks unmanaged, material risk.
- Negligence threshold: failure to authorise and begin the CBOM project within six months of this report may constitute reckless disregard in the event of a future quantum cryptographic breach.

15.2 Perpetual Q-Resilience: The Architectural Mandate

The immediate PQC migration is the first cycle 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 model defines this: horizon intelligence feeds governance; governance enforces mitigation; mitigation depends on visibility.

- Solvency-expenditure imperative: PQC migration funding is solvency expenditure, not IT cost. It is non-discretionary, multi-year, ring-fenced and protected from cuts to maintain 100 percent Funding Adherence. Any pause accepts existential liability.
- Global standards reality: first-wave NIST standards are finalised. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) are ready for immediate use. FIPS 206 (FN-DSA / FALCON) is imminent. HQC (NIST IR 8545) provides code-based diversity. CNSA 2.0, the EU 2026/2030/2035 milestones, UK NCSC 2028/2031/2035 phases, Canada CCCS 2026/2031/2035, ASD ISM end-2030, and the G7 CEG roadmap converge on the same migration arc.

Architectural mandates beyond the transformation programme

- Mandate cryptographic abstraction across all system development to isolate algorithms from business logic and enable rapid replacement.
- Institutionalise the Q-Resilience mindset. Treat current cryptography as temporary. Require cryptographic agility in all application development, infrastructure design and procurement.
- Finalise the Q-IRP. Draft and exercise the Quantum Incident Response Plan by the conclusion of the transformation programme. Include mass PKI revocation, certificate re-issuance, archival decryption containment, forensic protocols and cross-border regulator notification templates.

- Adopt secure code signing now. Implement hash-based signatures per NIST SP 800-208 (LMS, XMSS) for software and firmware signing, consistent with CNSA 2.0 posture and aligned with the SLSA and S2C2F supply-chain frameworks.

15.3 Final Call to Action: The Board's Decision

Executive leadership must act now to secure enterprise longevity, meet regulatory standards across every jurisdiction and mitigate personal liability.

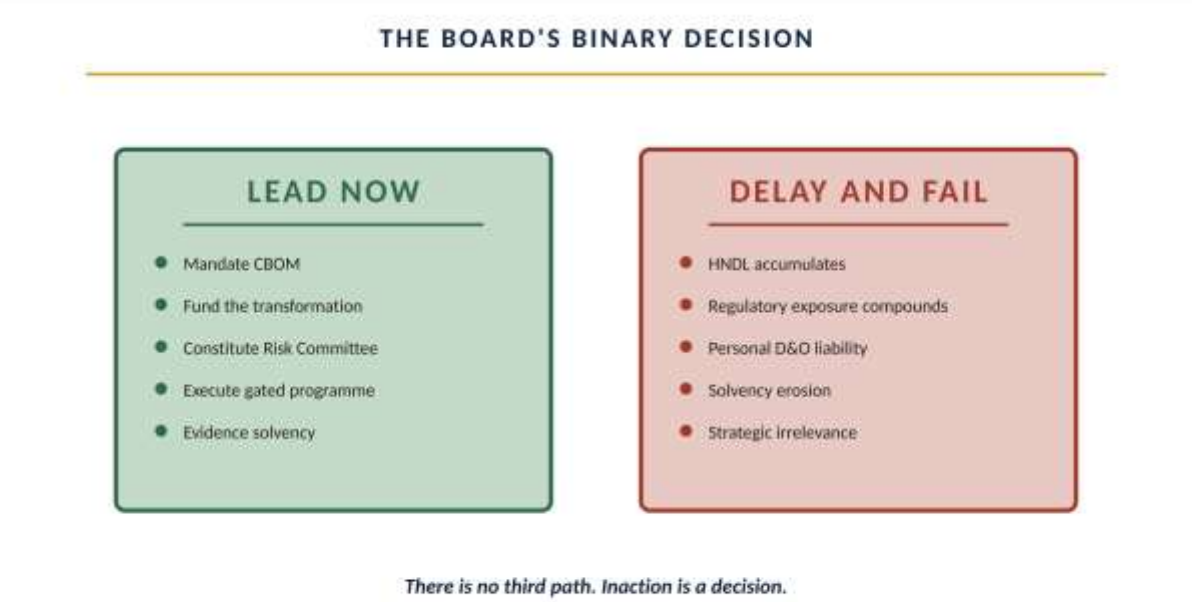

Figure 29. The Board's Decision Point. The board can lead a funded transition now or carry the exposure that delay creates.

- Immediate CBOM authorisation. Authorise and fully fund the dynamic CBOM project immediately. CBOM completion is the binary first KPI for visibility.
- Non-negotiable funding. Approve a dedicated, multi-year budget for the gated cryptographic transformation programme and forbid cuts to solvency expenditure.
- Empower Risk-Committee governance. Formalise and empower the Risk Committee with direct board reporting to enforce Survival KPIs and mandate aggressive vendor PQC compliance aligned to NIST FIPS, CNSA 2.0, ENISA and the relevant regional roadmaps.
- 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, FIPS 206 and HQC progress, EU NIS2 amendment passage, UK NCSC phases, Canada

CCCS milestones, ASD ISM updates, GCC and ASEAN supervisory positions, with documented impacts on vendors, contracts and controls.

- Vendor contract clauses. Insert obligations for crypto-agility, timelines for adopting second-wave algorithms, FIPS 140-3 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 procedures and breach forensics.
- External alignment: KPIs aligned to recognised deprecation and migration targets through 2030 to 2035 (NIST IR 8547, EU roadmap, UK NCSC, CCCS, ASD ISM). 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 authorise the CBOM and fund the roadmap within six months may create a documented record of reckless disregard for a known, standards-published, supervisor-

acknowledged risk. The decision is straightforward. Lead the transition now or risk being held responsible for the failure to act later.

References on this page • NIST FIPS 203/204/205 (2024); FIPS 206 (in development); NIST IR 8545 (2025); NIST IR 8547 (draft); NIST CSWP 39 (December 2025); NIST CSWP 48 (September 2025 draft); NIST SP 800-208. • NSA CNSA 2.0 (December 2024). • EU Recommendation 2024/1101; NIS CG Coordinated Implementation Roadmap (June 2025); COM(2026) 13 final. • UK NCSC (2025); CCCS (2025); ASD ISM (2025); HKMA Quantum Preparedness Index (2026); G7 CEG (2025). • SEC 17 CFR 229.106; EU Regulation 2022/2555 (NIS2) Art. 21, 23; EU Regulation 2022/2554 (DORA) Art. 19.

CHAPTER

Appendix

Lexicon for Quantum Risk

Concise definitions for board, supervisory and operational audiences.

TERM	DEFINITION FOR THE BOARD
PQC	Post-Quantum Cryptography. Quantum-resistant algorithms (notably ML-KEM, ML-DSA, SLH-DSA, FN-DSA, HQC) standardised by NIST and adopted globally to replace RSA and ECC.
RSA / ECC	Rivest–Shamir–Adleman and Elliptic-Curve Cryptography. The asymmetric primitives underpinning modern PKI, TLS, code signing, identity and digital signatures. Both fall to Shor on a CRQC.
HNDL	Harvest Now, Decrypt Later. The contemporary adversary tactic of capturing encrypted long-lived data today for retroactive decryption once CRQC capability arrives.
Q-Day	The point at which a cryptographically relevant quantum computer is confirmed operational, whether by public disclosure, intelligence assessment or inferred capability.
Mosca's Inequality	X + Y > Z. Migration time plus data confidentiality lifetime exceeds time to CRQC. For long-lived data, the inequality is true today.
CBOM	Cryptographic Bill of Materials. A comprehensive, auditable, dynamic inventory of every cryptographic primitive, algorithm, key, certificate and dependency across the enterprise and its supply chain.
CRQC	Cryptographically Relevant Quantum Computer. A fault-tolerant quantum computer with sufficient logical qubits to run Shor at deployed RSA/ECC key sizes within useful runtime.
Cryptographic Agility	The architectural capability to swap algorithms, key sizes, protocols and parameters rapidly across the enterprise without redesign or downtime. NIST CSWP 39.

TERM	DEFINITION FOR THE BOARD
Shadow Crypto	Undocumented or unmanaged cryptographic implementations: hard-coded keys, undisclosed library calls, legacy primitives in firmware, build-pipeline secrets. The principal source of unmanaged liability.
CNSA 2.0	Commercial National Security Algorithm Suite 2.0. NSA-mandated PQC posture for US National Security Systems and their vendor ecosystem.
NIS2	EU Directive (Regulation 2022/2555) on a high common level of cybersecurity across the Union; subject to amendment by COM(2026) 13 final to explicitly require PQC transition policies.
DORA	EU Regulation 2022/2554 on the Digital Operational Resilience of the financial sector, with ICT-risk and third-party-risk obligations applicable to PQC migration.
Hybrid PQ/T	Concurrent use of a classical primitive (RSA, ECC) and a PQC primitive (ML-KEM, ML-DSA, FN-DSA) such that an attacker must break both. The migration-period default.
Q-IRP	Quantum Incident Response Plan. Pre-positioned procedures for mass PKI revocation, certificate re-issuance, archive decryption containment and regulator notification following an unannounced quantum break or PQC family weakness.

CHAPTER

Bibliography and Sources

Foundational and Academic

- Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE.
- Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC).
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers. IEEE Security & Privacy 16(5), 38–41.
- Gidney, C. & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433.
- Castryck, W. & Decru, T. (2022). An Efficient Key Recovery Attack on SIDH (preliminary version). EUROCRYPT.
- Wang, X., Yin, Y. L. & Yu, H. (2005). Finding Collisions in the Full SHA-1. CRYPTO.
- Stevens, M. et al. (2017). The first collision for full SHA-1. CRYPTO.
- Mosca, M. & Piani, M. (2025). 2024 Quantum Threat Timeline Report. Global Risk Institute / evolutionQ.
- Federal Reserve Board (2025). FEDS 2025-093: Quantum Risk in Financial Networks.

Standards and Technical Guidance

- NIST (2024). FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).
- NIST (2024). FIPS 204 Module-Lattice-Based Digital Signature Algorithm (ML-DSA).
- NIST (2024). FIPS 205 Stateless Hash-Based Digital Signature Algorithm (SLH-DSA).
- NIST (in development). FIPS 206 FN-DSA Digital Signature Algorithm.
- NIST IR 8545 (2025). Status Report on the Fourth Round of the NIST PQC Standardization Process – HQC selection.
- NIST IR 8547 (draft, 2025). Transition to Post-Quantum Cryptographic Standards.
- NIST CSWP 39 (19 December 2025). Considerations for Achieving Cryptographic Agility.
- NIST CSWP 48 (September 2025 draft). Mappings of Migration to PQC Project Capabilities to NIST CSF 2.0 and SP 800-53 Rev. 5.
- NIST SP 800-208 (2020). Recommendation for Stateful Hash-Based Signature Schemes.
- NIST SP 800-131A Rev. 2 (2019). Transitioning the Use of Cryptographic Algorithms and Key Lengths.

- NIST IR 8413 (2022). Status Report on the Third Round of the NIST PQC Standardization Process.
- NSA (December 2024). Commercial National Security Algorithm Suite 2.0.
- ETSI TR 103 619 (2020). Migration strategies and recommendations to Quantum-Safe schemes.
- ETSI ISG-QKD specifications; ITU-T Y.3800-series QKD networks.
- ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 18033-3; ISO/IEC JTC 1/SC 27 WG 2 work programme on Quantum-Safe Cryptography.
- IETF: RFC 8446 (TLS 1.3); draft-ietf-tls-hybrid-design; draft-ietf-ipsecme-ikev2-multiple-ke; draft-ietf-openpgp-pqc; draft-ietf-cose-pqc.
- CycloneDX 1.6 Cryptographic Asset Extension; SPDX 3.0 Cryptographic Profile; OWASP CBOM Project.
- CA/Browser Forum SC-081v3 TLS certificate-lifecycle reduction.

European Union

- European Commission (11 April 2024). Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to PQC.
- NIS Cooperation Group (June 2025). Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.
- European Commission COM(2026) 13 final (20 January 2026). Proposed Directive amending NIS2 (PQC and other cybersecurity-simplification provisions).
- Regulation (EU) 2016/679 (GDPR), Art. 32.
- Regulation (EU) 2022/2555 (NIS2); Commission Implementing Regulation (EU) 2024/2690.
- Regulation (EU) 2022/2554 (DORA); Commission Delegated Regulation (EU) 2024/1774 (ICT risk RTS).
- Regulation (EU) 2024/1183 (eIDAS 2.0).
- ENISA (2024). Post-Quantum Cryptography – Integration Study.
- ENISA (June 2025). NIS2 Technical Implementation Guidance.
- ECCG (May 2025). Agreed Cryptographic Algorithms v2.
- Directive (EU) 2020/1828 on Representative Actions.

United Kingdom

- NCSC (2025). Timelines for migration to post-quantum cryptography.
- NCSC PQC migration guidance for critical infrastructure (2024–2025).
- UK GDPR; Data Protection Act 2018; ICO encryption guidance.
- FCA SYSC 13; PRA SS1/21 Operational Resilience.
- Telecommunications Security Act 2021 and Code of Practice.

North America

- Canadian Centre for Cyber Security (June 2025). Canadian Government Post-Quantum Cryptography Roadmap.
- Treasury Board of Canada Secretariat. ITSG-33 IT Security Risk Management.
- PIPEDA; Bill C-26 Critical Cyber Systems Protection Act.
- SEC 17 CFR 229.106 (Reg S-K, Item 106); Form 8-K cybersecurity disclosure.
- US Executive Order 14028 (2021); OMB M-23-02.
- Quantum Computing Cybersecurity Preparedness Act (Public Law 117-260, 2022).
- HIPAA Security Rule 45 CFR §164.312; HITECH Act.
- CCPA / CPRA; NYDFS 23 NYCRR Part 500.
- DFARS 252.204-7012; CMMC.
- GAO (2018) GAO-18-559 (Equifax); GAO (1999) AIMD-10.1.19 (Y2K).

Asia-Pacific

- Australian Signals Directorate (2025). Information Security Manual – Cryptography section.
- Security of Critical Infrastructure Act 2018 (as amended by SLACIP).
- APRA CPS 234 Information Security; Privacy Act 1988 (Cth).
- Singapore CSA. Cybersecurity Code of Practice for CII; National Quantum Strategy.
- MAS Technology Risk Management Guidelines (2021); Notice 655/657.
- HKMA Supervisory Policy Manual SA-2; HKMA Quantum Preparedness Index (2026).
- Personal Data (Privacy) Ordinance (Hong Kong); PDPA Singapore; APPI Japan; PIPA Korea.
- India: National Quantum Mission – Implementation of Quantum Safe Ecosystem (2025); CERT-In Directions; RBI Master Direction on IT Governance, Risk, Controls and Assurance (2023); DPDP Act 2023; SEBI cyber-security framework.
- Malaysia: Cyber Security Act 2024; NACSA; PDPA 2010 (as amended 2024).
- Thailand: PDPA 2019; Bank of Thailand technology-risk guidance; NCSA framework.
- Indonesia: BSSN; UU PDP 27/2022; OJK cyber-risk guidance.
- METI / CRYPTREC (Japan) PQC migration guidance.

Gulf, Africa and Latin America

- UAE: TDRA Information Assurance Standards; Federal Decree-Law 45/2021 PDPL; DESC Information Security Regulation; ADGM/DIFC data-protection regulations.
- Saudi Arabia: NCA Essential Cybersecurity Controls (ECC-1) and Critical Systems Cybersecurity Controls (CSCC); SAMA Cyber Security Framework; PDPL (2023).

- Qatar: NCSA National Information Assurance Framework; QFC Data Protection Regulations.
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, in force 2023).
- South Africa: POPIA; SARB Cyber Resilience Standard.
- Brazil: LGPD; ANPD; Banco Central do Brasil cyber-resilience requirements.
- Mexico: LFPDPPP; CNBV cyber-security circular.

Global Multilateral and Industry

- OECD (2023). G20/OECD Principles of Corporate Governance.
- OECD (2025). Policy Brief on the Transition to Post-Quantum Cryptography.
- G7 Cyber Expert Group (2025). Roadmap for the Financial Sector's Transition to Post-Quantum Cryptography.
- FSB (2023). Cyber Lexicon (revised).
- BIS Committee on Payments and Market Infrastructures (2016, updated 2021). Guidance on cyber resilience for financial market infrastructures.
- BIS Innovation Hub Project Leap (2024–2025); Project Pyxis.
- BCBS 239 (2013); BCBS Principles for operational resilience (2021).
- Trusted Computing Group (November 2025). State of PQC Readiness Survey.
- Utimaco PQC Readiness Report 2025.
- Cloud Security Alliance PQC Working Group; PCI SSC PQC Working Group.
- SWIFT Customer Security Programme PQC guidance.
- IFRS Sustainability Disclosure Standards (S1, S2); ISSB.
- PCI DSS v4.0.1 (2024).

Historical and Case-Study Sources

- NSA (1996). VENONA: Soviet Espionage and the American Response 1939–1957; NARA VENONA archives.
- GAO (1999). AIMD-10.1.19 Year 2000 Computing Crisis.
- GAO (2018). GAO-18-559 Data Protection: Equifax 2017 Breach.
- Stevens, M. et al. (2017). The first collision for full SHA-1; shattered.io.

Quantum Risk: A 2026 Global Doctrine for PQC Migration, Board Accountability and Cryptographic Solvency. Edition 2026.1.

Page 1 of 1 | Edition 2026.1 | Non-commercial reference document

SITG-Consulting
Strategy | Intelligence | Technology | Growth
STRATEGY.
INTELLIGENCE.
TECHNOLOGY.
GROWTH.
Insights that drive decisions.
Solutions that drive growth.