

SCBX QUANTUM OUTLOOK: Post-Quantum Cryptography

SPECIAL EDITION
DECEMBER 2025

SCB^x



Foreward

The “PQC Outlook” stands as a highly valuable and vendor-neutral strategic resource for all sectors, particularly at a time when quantum computing is reshaping the very foundation of digital security. This document offers a clear, comprehensive, and unbiased perspective on the existential threat that large-scale, fault-tolerant quantum computers pose to public-key cryptography, which underpins the integrity and trust of today’s digital ecosystem.

Importantly, the material stresses that the quantum threat is already active, defining the immediate and critical challenge as the Harvest-Now, Decrypt-Later (HNDL) strategy—an issue that directly impacts the confidentiality and long-term reliability of encrypted data. For the financial and banking sector, where data trust and durability are paramount, this document underscores the need for a decade-long strategic migration that must begin now, not merely to comply with emerging standards but to safeguard economic stability, operational resilience, and digital trust in the years ahead.













One of the key strengths of this work is its clarity. It distills complex technical concepts into an accessible roadmap that spans the full Post-Quantum Cryptography (PQC) transition lifecycle—from planning and risk assessment to standard adoption and deployment. The paper highlights key milestones and presents actionable strategies including Hybrid Deployment—the concurrent use of classical and PQC algorithms—and Crypto-Agility, essential for long-term operational resilience.

For the financial and banking sector, this document not only provides guidance on managing information technology risks but also serves as a strategic policy instrument—enabling the full integration of cybersecurity into the nation’s digital economy strategy. The “PQC Outlook” is therefore a work that every organization, and especially policymakers, should read in order to strengthen the country’s cybersecurity resilience and ensure sustainable preparedness for the Quantum Era.

AVM. Amorn Chomchoey

Secretary General,
National Cyber Security Agency (NCSA)

Content

	Chapter 1 Executive Summary		Chapter 2 Introduction		Chapter 3 Quantum Technology for the Uninitiated
	Chapter 4 Quantum Computing Threat Landscape		Chapter 5 Overview of Post- Quantum Cryptography		Chapter 6 Standards & Standardization Process
	Chapter 7 Standards & Standardization Process		Chapter 8 Regulatory, Compliance & Governance		Chapter 9 Use Case & Adoption Scenarios
	Chapter 10 Challenges & Open Questions		Chapter 11 Recommendations & Call to Action		Glossary

Chapter 1

Executive Summary

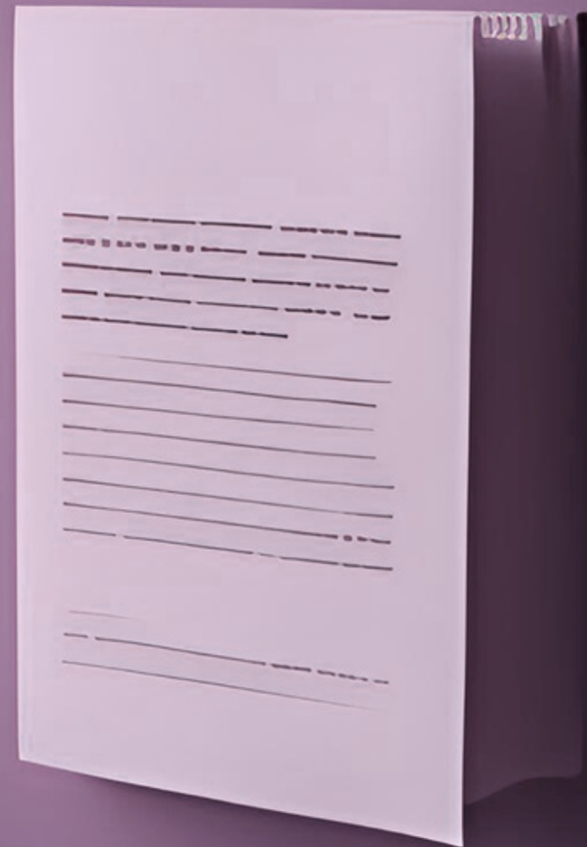
Executive Summary

The emergence of large-scale, fault-tolerant quantum computers represents an existential threat to all public-key cryptography (PKC) currently securing global digital infrastructure. Algorithms like RSA and Elliptic Curve Cryptography (ECC), which underpin secure communications, financial transactions, and classified data storage, are vulnerable to Shor's algorithm, a quantum attack that can efficiently break them. This document serves as a politically neutral, logically organized, and strategically oriented guide for non-experts, detailing the necessary organizational shift to Post-Quantum Cryptography (PQC).

High-level Overview of the Quantum Threat and Why Organizations Must Prepare

The quantum threat is active today, not distant. The immediate risk is the Harvest-Now, Decrypt-Later (HN DL) strategy, where hostile actors capture and store vast amounts of currently encrypted data. This captured data must remain confidential for years or decades—a period known as the confidentiality horizon. Once a cryptographically relevant quantum computer (CRQC) arrives, often projected between 2030 and 2035, this stored data will be compromised en masse, marking the critical date known as Q-Day. Preparation is a decade-long strategic migration, not a quick upgrade, meaning organizations must act now to mitigate this immediate data exposure risk and ensure operational resilience.





Key Findings and Recommendations

The Threat is HNDL

The most urgent priority is cataloging and migrating long-term secrets vulnerable to current data capture.

Standards Exist

The global PQC transition is driven by the NIST Standardization Process, which has finalized the first set of quantum-safe standards (e.g., CRYSTALS-Kyber for encryption, CRYSTALS-Dilithium for signatures).

Migration Must Be Hybrid

The safest, most resilient strategy is Hybrid Deployment, meaning that classical algorithms and new PQC algorithms are run simultaneously, to guarantee backward compatibility while future-proofing security against both classical and quantum threats.

Long-Term Resilience (PQC + QKD)

For long-term key management and environments demanding the highest assurance (e.g., defense, cross-border backbones), organizations should explore the integration of PQC algorithms with Quantum Key Distribution (QKD). PQC provides the default digital upgrade, while QKD offers physics-based tamper evidence for specialized links, creating a layered defense against all future threats.

Crypto-Agility is Mandatory

Success depends on embedding crypto-agility into infrastructure, which is the organizational and technical ability to switch cryptographic algorithms quickly and efficiently in response to new standards or unforeseen cryptanalytic attacks.

Governance is Critical

This transition is a risk-management challenge, not just an IT project. It requires board-level oversight, policy integration, and mandatory inventory programs to track all cryptographic assets and their associated confidentiality horizons.

Chapter 2

Introduction

Purpose and Scope of the Document

This document, PQC Outlook, provides a comprehensive, vendor-agnostic, and globally relevant framework for understanding the quantum threat and executing a successful migration to Post-Quantum Cryptography. Its primary purpose is to cut through technical jargon and political noise, offering a clear roadmap for strategic decision-makers. The scope covers the full lifecycle of the PQC transition: from demystifying quantum concepts and defining the primary algorithm families to detailing global standards (NIST, ETSI, ISO/IEC), outlining phased migration roadmaps, and addressing complex regulatory, governance, and key-management challenges. We specifically address the critical need for regional coordination, particularly within Asia and the ASEAN framework.

Intended Audience

This guide is tailored for two distinct yet equally critical, audiences

Strategic Leaders and Risk Managers

Executives, board members, Chief Information Security Officers (CISOs), and risk compliance officers who need a high-level, policy-driven understanding of the quantum threat, its business impact, and the necessary resource allocation and governance structures required for successful migration.

Security Architects and Technical Professionals

Engineers, application developers, and security operations personnel responsible for cryptographic inventory, systems architecture, standards adoption, interoperability testing, and the hands-on technical execution of the PQC transition roadmap.

Impact on Classical Cryptography

The bedrock of modern digital security, public-key cryptography based on factoring large numbers (RSA) and solving discrete logarithms on elliptic curves (ECC), is fundamentally broken by the properties of a quantum computer. All data secured by these classical algorithms, whether at rest (data stored in databases and servers) or in transit (data moving across networks via protocols like TLS and IPsec), faces compromise. The transition to PQC is therefore non-negotiable and requires systematic replacement of vulnerable algorithms wherever they are used for long-term data protection, code signing, or identity authentication. The coming chapters detail the specific timeline, the PQC alternatives, and the practical steps to manage this large-scale cryptographic transformation.

Chapter 3

Quantum Technology for the Uninitiated

Quantum Technology for the Uninitiated

As we stand on the cusp of a new technological era, quantum technology promises to reshape computing, sensing, and secure communications in profound ways. Unlike classical systems, which manipulate bits that are either 0 or 1, quantum systems harness the strange behaviors of particles at the atomic scale to unlock parallelism and correlations previously unimaginable. For executives and professionals without a physics background, this chapter demystifies the core concepts, explains why quantum matters today, and illustrates concrete impacts across industries. We then explore practical reasons to begin preparing now-both to seize strategic opportunities and to mitigate emerging risks. By the end of this chapter, you will have a clear, high-level understanding of what quantum technology is, why it matters, how it will affect your organization, and the steps needed to get started.

What Is Quantum Technology?

At its essence, quantum technology exploits how particles behave when confined to the smallest scales. Although the underlying physics can be mathematically complex, three key effects drive all applications: superposition, entanglement, and interference. This section defines each phenomenon in simple terms and outlines how they combine to form the building blocks of quantum devices. By focusing on core principles rather than technical detail, we establish a foundation for understanding real-world quantum systems.



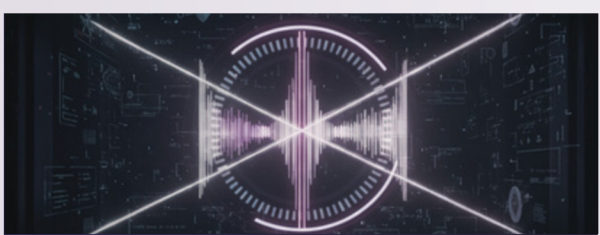
Superposition

A quantum bit (qubit) can exist in multiple states simultaneously (both 0 and 1), rather than being strictly one or the other.



Entanglement

Two qubits become linked so that the state of one instantly influences the state of the other, regardless of distance.



Quantum interference

Probability amplitudes combine in ways that allow constructive or destructive patterns, enabling certain outcomes to be amplified and others suppressed.

Why Quantum?

Quantum technology's promise lies in advantages that classical systems cannot match. From accelerating complex computations to delivering unprecedented sensor precision and future-proofing communications, quantum platforms open new frontiers. This section groups these advantages into three broad categories-computation, sensing, and security-and provides concrete examples of each. Understanding these domains helps organizations align quantum initiatives with strategic objectives.

1. Computational Power

- **Speed-ups for hard problems** Certain optimization, simulation, and search tasks (e.g., chemical modeling, portfolio optimization, supply-chain logistics) could see dramatic accelerations.
- **New algorithms** Quantum algorithms exploit superposition and entanglement to reduce computational steps, potentially turning multi-year simulations into minutes.

2. Sensing & Metrology

- **Ultra-precise measurements** Quantum sensors can detect fields, forces, and time intervals with orders-of-magnitude greater sensitivity-benefiting navigation, medical imaging, and materials inspection.

3. Secure Communication

- **Quantum Key Distribution (QKD)** Uses quantum states to exchange encryption keys with provable tamper-evidence.
- **Post-quantum readiness** As quantum computers mature, classical encryption schemes (e.g., RSA, ECC) will be vulnerable; quantum-safe algorithms and QKD protect future communications.
- In anticipation of both "harvest now, decrypt later" attacks before Q-day and full-scale quantum assaults thereafter, classical encryption schemes (e.g., RSA, ECC) will be vulnerable; adopting quantum-safe algorithms and QKD protects communications today and into the post-quantum era
- **Quantum-assisted Attack and Defend** Bad actors could leverage quantum algorithms to discover novel vulnerabilities on both digital and quantum communication system and craft optimized combinations of exploits, while defenders could employ quantum-enhanced monitoring and anomaly detection to catch subtle signs of malicious activity in real time.

How Will It Impact Our Lives?

Quantum technology’s transformative potential extends across nearly every sector of the global economy. By mapping specific quantum benefits to real-world use cases, organizations can identify early opportunities for pilot projects and partnerships. The following table highlights six sectors where quantum is already influencing research and development, along with tangible examples to ground these advances in practical terms.

Sector	Quantum Benefit	Example
Pharmaceuticals	Rapid molecule simulation	Designing novel cancer therapies via protein-folding models
Finance & Logistics	Complex network optimization Portfolio optimization	Dynamic route planning reducing fuel costs and delays Optimize resource allocation for complex system
Energy & Materials	Discovery of new catalysts and superconductors	Efficient hydrogen-production catalysts
Healthcare	Ultra-high-resolution imaging	Early disease detection with quantum-enhanced MRI
Telecommunications	Provably secure key exchange	
Manufacturing & AI	Accelerated machine-learning training	Smarter predictive maintenance, reducing downtime

Beyond these, quantum advances will drive breakthroughs in AI, national security, and fundamental science-reshaping markets and competitive dynamics.

Why We Need to Prepare Now

The quantum revolution will not wait for those who lag behind. Early adopters gain critical advantages in innovation, market positioning, and risk management, while unprepared organizations face strategic and security deficits. This section outlines four pillars-strategy, talent, infrastructure, and regulation-to guide executive decision-making on quantum readiness. It concludes with actionable steps to begin building quantum capabilities and partnerships today.

1. Strategic Leadership

First-mover advantage

Shape standards, secure partnerships, and capture market share.

Risk mitigation

Avoid future breaches when classical encryption falls to quantum attacks.

2.Talent & Ecosystem

Workforce readiness:

Cultivate experts in quantum engineering and algorithm design.

Collaborative networks

Partner with academia, labs, and startups for technology transfer.

3.Infrastructure Planning

Use-case identification

Pilot hybrid classical-quantum workflows to validate ROI.

Phased investment

From proofs of concept to scalable prototypes, optimizing funding.

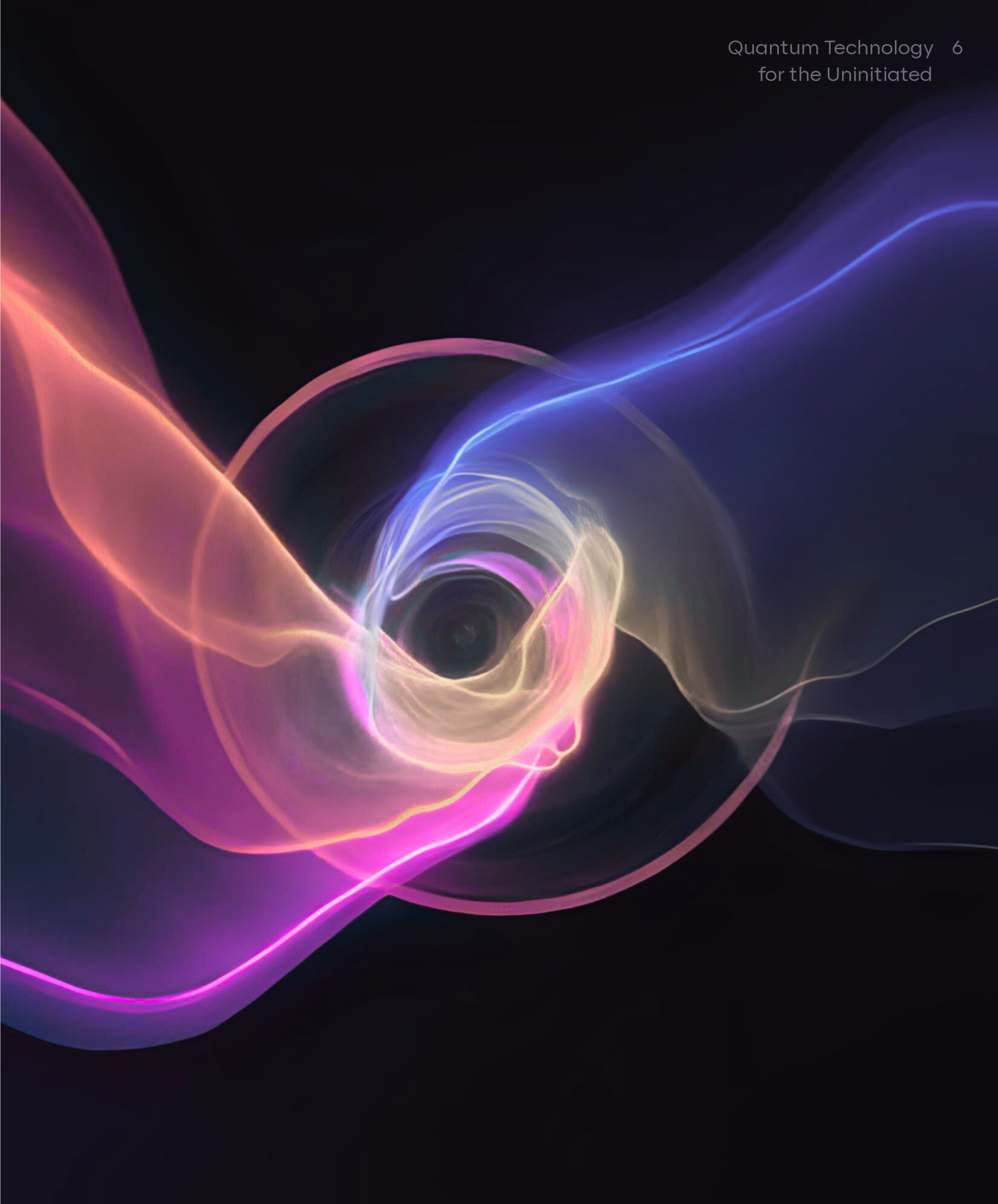
4.Regulatory Alignment

Standards engagement

Influence frameworks for quantum-safe encryption and data privacy.

Interoperability

Adhere early to avoid vendor lock-in and ensure cross-industry compatibility.



Chapter 4

Quantum Computing Threat Landscape

Quantum Computing Threat Landscape

As quantum computing transitions from theory to practice, its disruptive potential brings both opportunity and risk. While quantum systems promise breakthroughs in simulation and optimization, they also threaten current cryptographic foundations-posing existential risks to data security. Executives must understand not only the capabilities of emerging quantum machines but also the timelines for their arrival and the strategic steps required to defend against new attack vectors. This chapter provides a concise primer on quantum computing power, maps projected “Q-Day” milestones, details the harvest-now/decrypt-later threat, and outlines governance frameworks to guide resilient policy and investment. By the end, readers will grasp the urgency of quantum-safe strategies and know how to align organizational defenses with evolving standards.

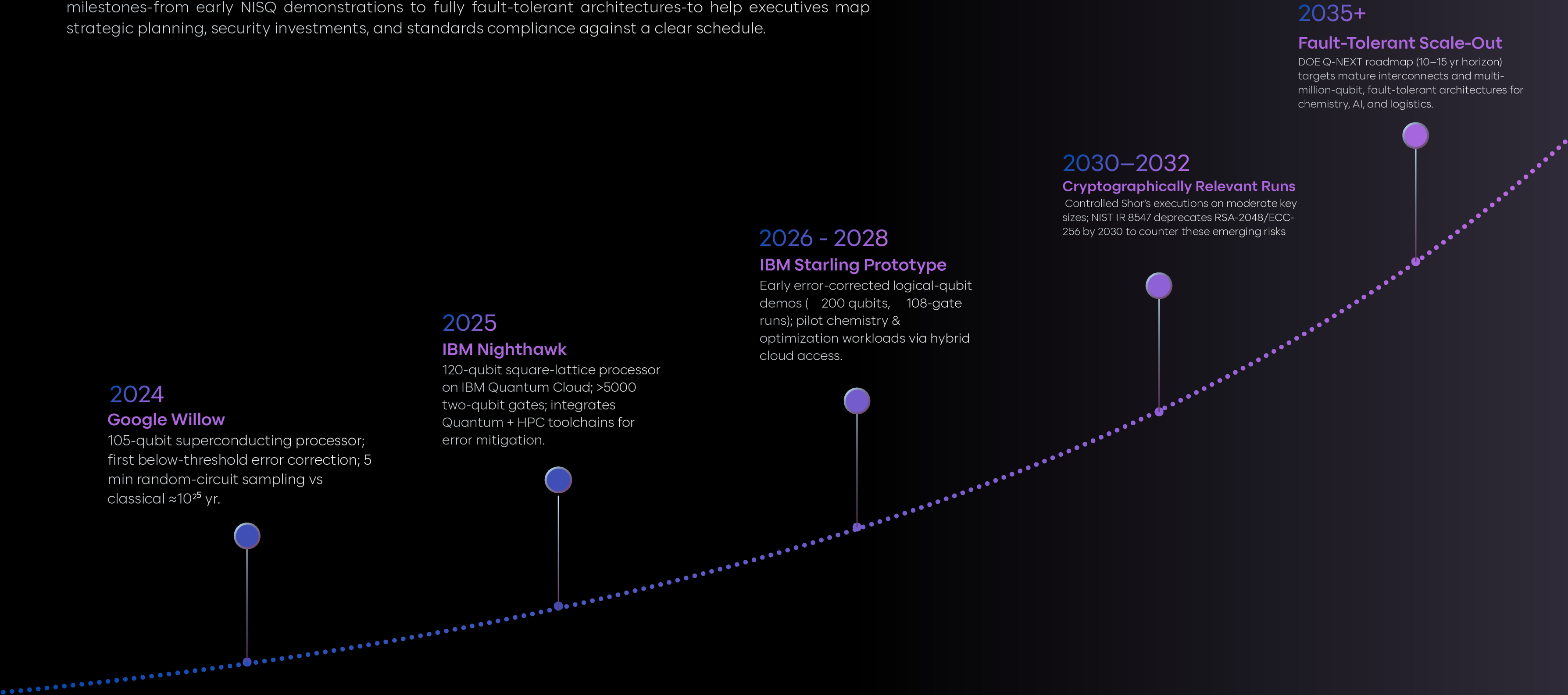
Primer on Quantum Computing Capabilities

Quantum computers operate on qubits, leveraging superposition, entanglement, and interference to perform certain computations exponentially faster than classical counterparts. Today’s NISQ devices-ranging from 50 to 150 qubits-have demonstrated “**quantum advantage**” in specialized tasks but remain limited by noise and scalability. Understanding the gap between current NISQ platforms and future fault-tolerant systems is crucial for assessing when cryptographic and operational risks will materialize. This section outlines present capabilities and key milestones toward large-scale quantum processing.

Quantum processors exploit superposition, entanglement, and interference to tackle classically intractable problems. For example, Google’s 105-qubit Willow processor completed a random-circuit-sampling benchmark in 5 minutes versus an estimated 10^{25} years on a classical supercomputer. Scaling beyond NISQ requires quantum error correction, encoding each logical qubit into many physical qubits. IBM’s roadmap targets 200 logical qubits capable of 100 million-gate runs by 2029 .

Timeline of Projected “Quantum Capable” Machines

Predicting when quantum systems will threaten classical cryptography involves synthesizing vendor roadmaps, government reports, and peer-reviewed forecasts. The following table aggregates authoritative milestones-from early NISQ demonstrations to fully fault-tolerant architectures-to help executives map strategic planning, security investments, and standards compliance against a clear schedule.



Understanding the quantum threat requires insight into the underlying hardware that makes cryptanalysis possible. Unlike classical computers, which use electricity to represent data, quantum systems leverage diverse physical substrates to manipulate qubits (quantum bits). These physical implementations, known as modalities, each present unique advantages in terms of performance, coherence (how long the quantum state can be maintained), and scalability, but all face immense engineering hurdles. The table below outlines the primary quantum computing modalities currently under development, highlighting the core principles and challenges that define the current state of the quantum hardware race.


Comparative Analysis of Key Quantum Computing Modalities


Modality	Principle	Key Advantages	Major Challenges / Limitations	Representative Systems / Entities
Superconducting Qubits	Uses Josephson junctions and superconducting loops; microwave pulses manipulate qubit states	Fast gate operations, good compatibility with integrated electronics	Fast gate operations, good compatibility with integrated electronics	Google Sycamore, IBM, Rigetti
Trapped-ion	Ions are trapped in vacuum; lasers drive transitions and coupling between ions	Very long coherence times, high-fidelity gates, all-to-all connectivity	Slower gate speeds, scaling to many ions, complexity of laser control	IonQ, Quantinuum
Photonic / Linear-optical	Qubits encoded in photon states (polarization, path, etc.), manipulated via beam splitters, phase shifters, etc.	Room-temperature operation, low decoherence from environment, good for communication	Photon loss, difficulty in deterministic photon sources and gates, detection inefficiencies	PsiQuantum, Xanadu, Jiuzhang (photonic quantum supremacy experiment)
Neutral-atom / Atomic arrays	Atoms are trapped (e.g. via lasers) and coupling between atoms (e.g. via Rydberg interactions) enables gates	Good scalability potential, relatively low sensitivity to stray charges	Precision control, weaker interactions, error rates, engineering complexity	QuEra, Pasqal
Quantum dots / Spin qubits	Use the spin or charge states in semiconductor nanostructures, manipulated by electric / magnetic fields	Potential compatibility with semiconductor fabrication, compact size	Decoherence (noise), coupling two qubits reliably, readout fidelity	Research in Intel, silicon qubit programs
Topological (Majorana)	Qubits stored in nonlocal (topological) degrees of freedom (e.g. Majorana zero modes), manipulated by "braiding" operations	Intrinsic error protection, robustness to local noise	Still mostly theoretical / experimental; creating and controlling topological states is extremely challenging	Microsoft's Majorana 1

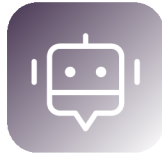
Harvest-Now/Decrypt-Later Risks


One of the most urgent cryptographic threats is not a future quantum hack but today’s silent collection of encrypted data for tomorrow’s decryption. Known as Harvest-Now/Decrypt-Later (HNDL), this strategy exploits the long shelf-life of sensitive archives-financial logs, health records, intellectual property-by storing ciphertext until quantum systems can break RSA and ECC. Understanding the attack sequence and mitigation steps is critical for minimizing exposure before Q-Day arrives.


Attack Sequence (5 Steps)

- 

Passive Capture
Record encrypted channels (TLS, VPN, email, cloud backups) without real-time decryption.
- 

Long-Term Archival
NIST IR 8547 flags HNDL as a critical risk; catalog long-term secrets and migrate highest-risk assets to PQC.
- 

Quantum Maturation
Await hardware improvements and robust error correction.
- 

Key Extraction
Await hardware improvements and robust error correction.
- 

Bulk Decryption
Use recovered keys to decrypt all archived data.

Mitigation Guidance

- Inventory & Prioritize:** NIST IR 8547 flags HNDL as a critical risk; catalog long-term secrets and migrate highest-risk assets to PQC .
- Hybrid Deployments:** Sectigo (May 2025) recommends running classical and PQC algorithms in parallel and shortening key lifetimes via accelerated rotation.



Quantum Technology Governance

Effectively navigating the quantum era requires coordinated standards, regulatory frameworks, and collaborative initiatives that balance innovation with security. Governments and industry bodies globally are publishing roadmaps, mandating transition timelines, and fostering public-private partnerships to ensure seamless adoption of quantum-safe technologies. This section outlines key governance efforts and best practices to help organizations align their policies and investments with evolving requirements.

NIST Transition Roadmap

- IR 8547 (Nov 2024): Phased PQC migration aligned with NSM-10's goal of full adoption by 2035 .
- "The Road Ahead" (Mar 2025): Updates on algorithm performance and integration guidance .
- FIPS 203–205 (Aug 2024): Finalized PQC algorithms-CRYSTALS-Kyber, Dilithium, Falcon.

CISA Guidance

- Quantum-Readiness Fact Sheet (2023): Directs agencies and vendors to publish PQC roadmaps, perform hybrid testing, and train cybersecurity teams on quantum risks.

NICT Q-ICT Roadmap (Japan)

- Metro QKD Links by 2025: ≥ 1 Mbps over 50 km fiber in Tokyo trials.
- QKD & Repeaters: R&D on > 100 km links integrated with Beyond 5G/6G networks.

European Standardization (CEN-CENELEC)

- 2022 Roadmap: Harmonized agenda for QKD, PQC interfaces, and interoperability tests across EU states.
-

Global Coordination & Ethics

- Proposed Global Quantum Standards Forum to align regulations, embed responsible-innovation assessments, and enable transparent public-private partnerships.

Chapter 5

Overview of Post-Quantum Cryptography (PQC)

Overview of Post-Quantum Cryptography (PQC)

As quantum computers edge closer to breaking widely deployed public-key schemes, organizations must transition to cryptographic algorithms resilient against both classical and quantum attacks [1]. Post-Quantum Cryptography (PQC) encompasses families of mathematically grounded schemes designed to interoperate with existing protocols and networks while remaining secure in the face of quantum-capable adversaries [2]. In 2016, NIST published IR 8105 to launch a multi-year standardization process, evaluating over 70 candidates across five main algorithm families [3]. After three rigorous rounds of public review, NIST finalized its first encryption (CRYSTALS-Kyber) and signature (CRYSTALS-Dilithium, FALCON) standards in August 2024 [4]. The following sections define PQC's goals, then survey its principal algorithm families-lattice-, code-, multivariate-, hash-, and supersingular-isogeny-based schemes-highlighting flagship examples and unpacking all specialized terms and assumptions.

Definition and Goals of PQC

Post-Quantum Cryptography aims to replace quantum-vulnerable primitives (e.g., RSA, ECC) with alternatives built on mathematical problems believed immune to both Shor's factoring algorithm and Grover's search speed-ups [3]. Its primary objectives are:

Quantum Resistance

Ensuring that no known quantum algorithm can efficiently break the scheme-typically by relying on problems for which only exponential-time quantum attacks are known, such as decoding noisy lattices or solving structured code problems [3].

Interoperability

Allowing new PQC algorithms to "plug in" to existing infrastructure (TLS, SSH, IPsec) without redesigning entire communication stacks-minimizing deployment friction [3].

Performance

Balancing key and signature sizes, computational workload (CPU cycles, memory), and network bandwidth so that PQC can run acceptably on current hardware-from servers to IoT devices [2].

Main Algorithm Families

NIST's PQC standardization grouped candidate schemes into five families, each based on a distinct hardness assumption. The table below summarizes these families, the underlying problems they exploit, and representative standards.

Family	Core Assumption	Example Schemes
Lattice-based	Learning With Errors (LWE), Module-LWE, Short Integer Solution (SIS)	CRYSTALS-Kyber (KEM), Dilithium (SIG)
Code-based	Hardness of decoding random linear error-correcting codes	Classic McEliece (KEM)
Multivariate	Difficulty of solving large systems of multivariate (quadratic) polynomials	Rainbow (SIG)
Hash-based	Collision- and preimage-resistance of cryptographic hash functions	LMS & XMSS (stateful signatures)
Supersingular Isogeny	Difficulty of computing isogeny maps between supersingular elliptic curves	SIKE (KEM)

Scope and depth of following discussion are up for discussion.
I set the summary styles up for everyone to pitch their ideas and openions.

Main Algorithm Families

1. Lattice-Based

Lattice-based schemes derive security from problems defined over high-dimensional point lattices:

- **Learning With Errors (LWE)** : Given a random matrix A and a vector $b = A \cdot s + e \pmod{q}$, where s is a secret vector and e is small noise, recovering s is conjectured hard even for quantum computers.
- **Short Integer Solution (SIS)** : Finding a short, nonzero integer combination of public lattice vectors that sums to zero.

NIST selected CRYSTALS-Kyber for key-encapsulation (KEM)-a mechanism to establish shared encryption keys-and CRYSTALS-Dilithium for digital signatures, both offering kilobyte-scale keys and signatures with efficient polynomial-arithmetic implementations [4]. “Key-encapsulation” refers to encrypting a randomly chosen symmetric key under a public key, then securely transmitting it; “digital signatures” provide non-repudiable message authentication.

2. Code-Based

Code-based cryptography rests on the syndrome decoding problem:

- **Random Linear Codes:** Error-correcting codes, such as Goppa codes, generate codewords by multiplying message bits with a public generator matrix and adding structured redundancy.
- **Decoding Hardness:** Recovering the original message given a random codeword plus errors is believed intractable.

Classic McEliece uses binary Goppa codes with large (≈ 1 MB) public keys but extremely fast decryption and key-generation speeds [5]. Its conservatively studied security makes it a strong fallback, especially where key storage is less constrained.

3. Multivariate

Multivariate schemes exploit the difficulty of solving large systems of quadratic equations over finite fields:

- **Oil–Vinegar Equations:** The public key is a set of multivariate quadratic polynomials; signing involves finding a solution vector that satisfies them.
- **Rainbow:** A layered variant where “Oil” variables mix with “Vinegar” variables in successive layers, improving structure and performance.

Rainbow produces small signature sizes (a few kilobytes) and rapid verification times, though the public key can be large. It remains under study following the third-round of NIST evaluation [6].

4. Hash-Based

Hash-based signatures rely on well-understood properties of cryptographic hash functions:

- **Collision Resistance:** It is computationally infeasible to find two distinct inputs hashing to the same output.
- **Preimage Resistance:** Given a hash output, finding any input that maps to it is difficult.

Leighton–Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS) use Merkle trees to construct many one-time keys securely. They require careful stateful management-tracking which one-time key has been used-to avoid key reuse. Multi-tree variants (HSS, XMSS^(mt)) stack Merkle trees to support larger signing capacities [7].

5. Supersingular Isogeny

Supersingular Isogeny Key Encapsulation (SIKE) uses:

- **Elliptic Curves:** Algebraic curves over finite fields whose point-addition laws form a group.
- **Isogeny Maps:** Structure-preserving functions (morphisms) between elliptic curves; computing the secret isogeny given only public curve parameters is believed hard even for quantum adversaries.

SIKE’s strength lies in very small key and ciphertext sizes (a few hundred bytes), though its performance (encryption/decryption speed) is slower compared to lattice- or code-based schemes [8]. It currently sits in NIST’s alternate track pending further analysis.

Chapter 6

Standards & Standardization Process

Standards & Standardization Process

Standards bodies play a pivotal role in validating, harmonizing, and promoting cryptographic algorithms that can withstand both classical and quantum attacks. The NIST Post-Quantum Cryptography (PQC) Standardization Process has become the global benchmark, engaging researchers and practitioners through a transparent, multi-round evaluation of candidate schemes [1]. Following three competitive rounds and extensive peer review, NIST published its first FIPS standards in August 2024, specifying both encryption (KEM) and signature algorithms ready for deployment [4]. In July 2022, further updates solidified the signature suite by adding SPHINCS+ and dropping candidates compromised by practical cryptanalysis [5]. Complementary efforts by organizations such as ETSI, ISO/IEC, South Korea’s KISA, ASEAN, China’s SAC/TC 260, Japan’s NICT, Russia’s Rosstandart, and Singapore’s CSA, MAS, and IMDA ensure regional alignment and interoperability. This chapter first reviews NIST’s phased timeline, then presents the officially ratified protocols alongside their vetted alternatives, and concludes with an overview of other standards-development bodies’ initiatives.

Standard Protocols & Alternative Candidates

Sub-intro (3–5 sentences):

In August 2024, NIST ratified three KEM and three signature protocols as Federal Information Processing Standards (FIPS 203–205) [4]. Together with the July 2022 update, the standardized suite now covers all major hardness assumptions-lattice- and hash-based- while removing schemes compromised by cryptanalysis. Alongside these, NIST recognizes a vetted set of alternative candidates spanning lattice-, code-, and hash-based approaches that organizations may evaluate for specialized requirements or future standardization rounds [1]. Table 6.2 contrasts the current standards with their approved alternatives.

Category	Standard Protocols	Alternative Candidates
KEM (Encryption)	CRYSTALS-Kyber [4]	NTRU; SABER; Classic McEliece; BIKE; FrodoKEM; HQC [1]
Signatures	CRYSTALS-Dilithium; FALCON; SPHINCS+ [4][5]	Picnic [1]

NIST PQC Competition Phases and Timeline

NIST’s standardization process began with IR 8105 in April 2016, issuing a “Call for Proposals” and hosting the first PQC workshop [16]. Subsequent rounds narrowed 69 initial submissions to 26, and finally to a set of finalists and alternates in July 2020 [1][2]. Periodic status reports (IR 8240, IR 8309, IR 8545) and PQC conferences provided updates on security analyses, performance benchmarking, and implementation progress. Table 6.1 summarizes these key milestones.



Other Standards Bodies: ETSI, ISO/IEC, Asia

Regional and national bodies complement NIST’s work to ensure global interoperability, address jurisdictional needs, and pilot real-world deployments. ETSI defines hybrid-scheme profiles; ISO/IEC extends core security standards; KISA and SAC/TC 260 manage national contests and roadmaps; ASEAN fosters multilateral cooperation; NICT supports quantum ICT integration; Rosstandart updates GOST standards; and Singapore’s CSA, MAS, and IMDA drive local guidelines and testbeds. Each plays a distinct role in the broader PQC ecosystem.

ETSI

- TS 104 015 V1.1.1 “Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies” (Feb 2025) specifies how to combine classical KEMs (e.g., X25519) with PQC KEMs (e.g., Kyber) under attribute-based policies [6].
- TR 103 966 V1.1.1 “Deployment Considerations for Hybrid Schemes” (Oct 2024) analyzes key management, performance tuning, and compliance testing for integrated PQC deployments [7].

ISO/IEC JTC 1/SC 27

- WG 2 updates ISO/IEC 18033-3 (encryption algorithms) to include test vectors and parameter sets for NIST-approved KEMs, and ISO/IEC 19790 (cryptographic module requirements) to mandate validation of PQC modules [8].
- Committee Document SD11 (2024) outlines SC 27’s work programme, confirming PQC integration as a top priority [9].
-

South Korea (KISA)

- Quantum-Resistant Cryptography National Contest (KpqC) launched Nov 2021; by Dec 2023, 16 algorithms advanced to Round 1, with four finalists selected Jan 2025 under the national roadmap [10].
- The Quantum-Safe Cryptography Standardization Roadmap (2023) mandates phased testing, certification, and mandatory PQC deployment across critical sectors by 2026 [11]

ASEAN

- The ASEAN Cybersecurity Cooperation Strategy (2021–2025) calls for regional PQC workshops, joint assessments, and harmonized guidelines to integrate quantum-safe algorithms into national frameworks [12].
- Member states collaborate on pilot projects-such as cross-border secure communications trials-to ensure readiness for future quantum threats.

China (SAC/TC 260)

- Notice on International Standard Proposals for Cybersecurity and PQC (Jan 23, 2025) invites contributions to ISO/IEC frameworks, aligning Chinese cybersecurity standards with global PQC efforts [13].

Japan (NICT)

- The Q-ICT Roadmap (2023) outlines phased deployment of QKD, integration of PQC into Beyond 5G networks, and standardization support for metro- and long-haul quantum links [14].

Russia (Rosstandart)

- As a P-member of ISO/IEC JTC 1/SC 27, Rosstandart contributes to amendments of GOST R 34 encryption standards to incorporate PQC algorithms and publishes national guidelines consistent with ISO/IEC developments [15].

Singapore (CSA, MAS, IMDA)

- CSA Quantum Security Guidelines (Dec 2024) provide planning frameworks for transitioning to quantum-safe systems [17].
- MAS Advisory on PQC (2023) outlines requirements for financial institutions to inventory cryptographic assets and adopt PQC algorithms [18].
- MAS recommendation for QKD sandbox to evaluate the use of Quantum Key Distribution (QKD) [18].

Actionable items for Thailand and ASEAN

- Public sector alignment: Coordinate with relevant Thai stakeholders (e.g., NCSA for national cybersecurity posture; NT for telecom backbones; sector regulators such as NBTC and BOT depending on domain). Map migration phases to their guidance and reporting cycles.
- Critical-infrastructure pilots: Prioritize pilots on networks that underpin government services, finance, healthcare, and utilities; consider hybrid TLS/IPsec at inter-agency gateways and PQC-wrapped key envelopes in KMS/HSMs.
- Local ecosystem readiness: Engage Thai universities and regional startups for interoperability testing, training, and conformance pilots. This de-risks deployment and builds in-country capability.
- Cross-border interop: ASEAN data flows (cloud, payments, logistics) benefit from harmonized hybrid profiles; plan for interop with international partners to avoid vendor lock-in.
- Procurement & compliance: Bake crypto-agility and PQC support roadmaps into RFPs and SLAs. For regulated entities, align program KPIs to risk-management and operational resilience requirements already recognized by regional supervisors.

Actionable next steps for Thailand-based stakeholders.

- Stand up a PQC Migration Working Group spanning agency/enterprise security, NT/ISP partners, and critical vendors.
- Create a Thai-context cryptography inventory template (English/Thai) capturing algorithm, key length, system owner, confidentiality horizon, and regulatory mapping.
- Establish a regularly governance review to track KPIs, vendor readiness, and cross-border interoperability issues, especially for critical infrastructure and services.

Chapter 7

Migration Roadmap & Best Practices

Migration Roadmap & Best Practices

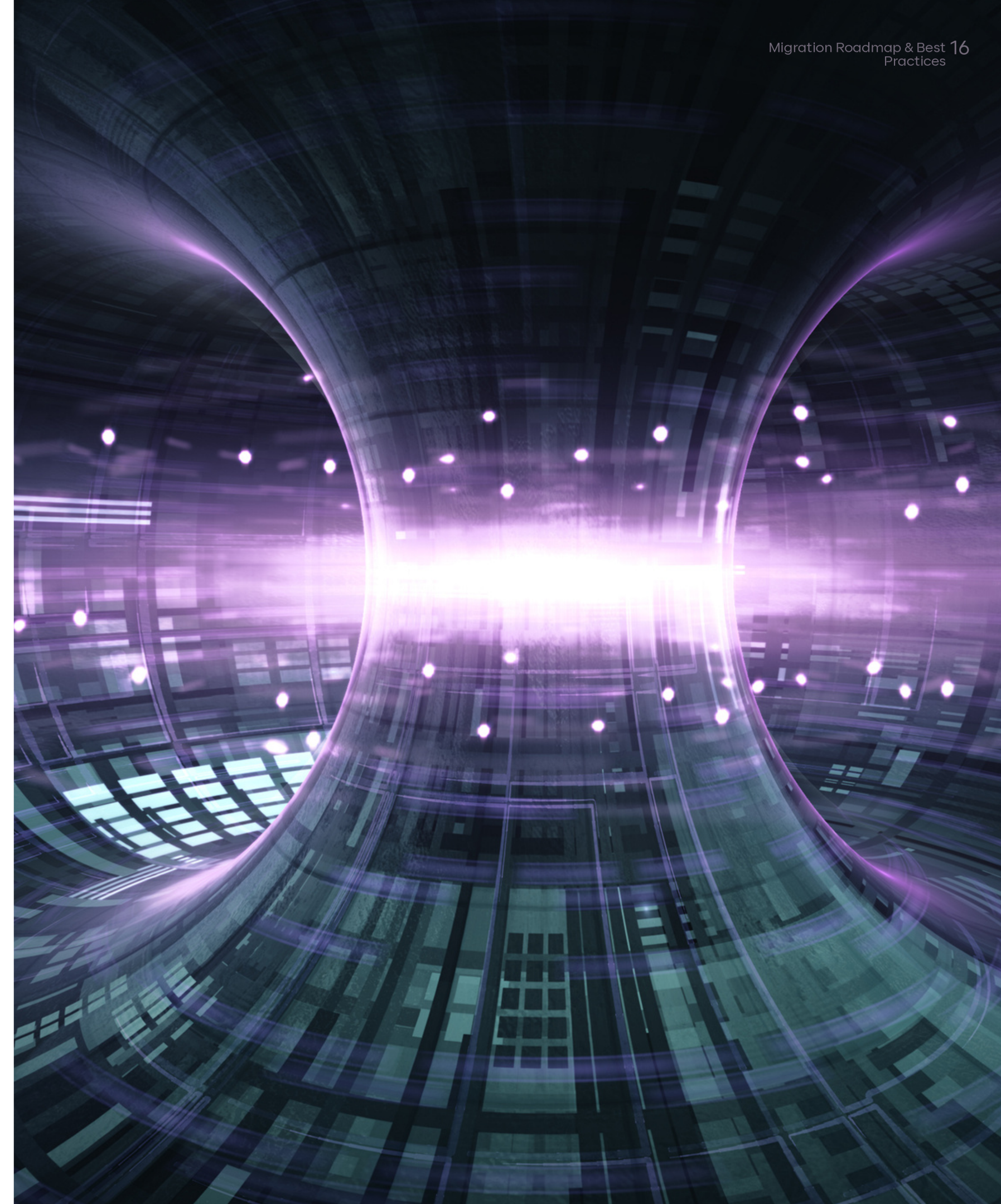
Transitioning to post-quantum cryptography is a strategic imperative that spans people, processes, and technology. A successful migration roadmap begins with a comprehensive inventory of existing cryptographic assets, followed by phased rollouts that mitigate risk while preserving business continuity [1][2]. Rigorous interoperability testing and module validation ensure that new PQC primitives integrate seamlessly with legacy systems and satisfy compliance mandates [3][4]. Equally critical is developing workforce readiness: security teams must comprehend algorithm properties, manage evolving key lifecycles, and respond promptly to integration issues [5][6]. Embedding crypto-agility capabilities enables rapid algorithm replacement in response to new vulnerabilities, while continuous monitoring and governance guarantee that the cryptographic estate adapts over time [7][8][9].



Inventory & Classification of Existing Crypto Assets

An accurate, up-to-date inventory is the foundation of any cryptographic transition. NIST's IR 8547 instructs organizations to catalog every instance where encryption, digital signatures, or key exchange is used-across servers, applications, network devices, and cryptographic libraries [1]. For each asset, record the algorithm name (e.g., RSA-2048), key length, mode of operation (e.g., RSA-OAEP for key wrap), and context of use (TLS, S/MIME, code-signing, database encryption). Assess dependencies such as hardware security modules (HSMs), cloud-managed KMS, and third-party SDKs to uncover hidden uses. Classify assets by confidentiality horizon-the period during which data must remain secure (e.g., 1 year for ephemeral logs, 10 years for financial records)-to prioritize high-impact migrations [1]. Finally, map each asset to its business owner and risk profile to streamline governance.

- **Discovery Tools** Leverage automated scanners and code analysis tools to detect cryptographic API calls and certificate stores.
- **Metadata Tagging** Annotate each asset with custom attributes: data classification, compliance requirements (e.g., GDPR data), and recovery procedures.
- **Risk Scoring** Apply a scoring model that weights factors such as data sensitivity, attack surface, and confidentiality horizon.





Phased Rollout Strategy

A phased rollout balances minimizing exposure to quantum threats with maintaining system stability. NIST IR 8547 prescribes a wave-based approach: begin with non-production testbeds to validate basic functionality, then pilot PQC in low-risk services, before expanding to mission-critical systems [1]. The CISA factsheet emphasizes vendor engagement early-confirming PQC support in product roadmaps and firmware updates [2]. Each phase should include performance benchmarks, error-handling tests, and rollback plans. Documenting lessons learned in each iteration reduces risk when migrating high-value assets.

- **Phase 1-Proof-of-Concept (PoC)** Deploy PQC in isolated environments. Validate key-generation, encryption/decryption, and signature flows.
- **Phase 2-Pilot** Integrate PQC into a limited set of production endpoints (e.g., VPN gateways, partner APIs). Measure handshake latency, CPU/memory overhead, and error rates.
- **Phase 3-Broad Deployment** Extend to customer-facing services (web TLS, mobile apps). Enforce hybrid mode (classical + PQC) to maintain interoperability.
- **Phase 4-Deprecation & Audit** Remove legacy algorithms once PQC coverage is verified. Conduct third-party audits to confirm compliance.



Interoperability Testing & Validation Frameworks

Interoperability testing verifies that different implementations of PQC schemes can communicate correctly under real-world conditions. NIST SP 1800-38C provides a Performance and Interoperability Workstream, which includes test harnesses, sample configurations, and failure-mode analyses [3]. FIPS 140-3 validation under the CMVP certifies that cryptographic modules adhere to defined security and physical protection requirements [4]. Together, these frameworks reduce deployment risk by catching integration issues-such as mismatched parameter sets or message-size overflows-early in the process.

- **Test Vector Validation** Use the official NIST PQC Test Vector Packages to ensure each implementation produces the correct ciphertext, shared secret, or signature for given inputs.
- **Protocol Interoperability** Execute hybrid TLS handshakes combining classical (e.g., X25519) and PQC KEMs (e.g., Kyber). Record handshake success rates, round-trip times, and fallback behaviors.
- **Module Certification** Submit hardware and software modules incorporating PQC to FIPS 140-3 testing labs. Validate logical interfaces, state management, and side-channel resistance.



Training & Operational Readiness

People are the linchpin in a successful PQC migration. NIST SP 800-50 and SP 800-16 offer guidance on creating role-based training programs, from executive briefings to deep-dive labs for cryptographic engineers [5][6]. For PQC specifically, curricula should cover algorithm principles, parameter choices (e.g., security levels), library integrations (e.g., OpenSSL, BoringSSL PQC forks), and incident response procedures for cryptographic failures.

- **Executive Awareness** Workshops that explain the quantum threat, migration timelines, and business impacts-ensuring leadership buy-in.
- **Technical Deep Dives** Hands-on sessions where engineers implement PQC KEM and signature APIs, troubleshoot integration errors, and benchmark performance.
- **Operational Playbooks** Create runbooks detailing PQC key generation, rotation schedules, backup procedures, and rollback steps.
- **Incident Response Drills** Simulate cryptographic failures (e.g., deprecated algorithm use) and practice recovery workflows



Crypto-Agility & Framework Integration

Crypto-agility is the organization's ability to switch cryptographic algorithms and parameters quickly in response to new vulnerabilities or standards updates. NIST SP 800-57 Part 3 and IR 8417 outline architecture patterns-such as abstraction layers, policy engines, and key envelopes-that decouple application logic from specific algorithms [7][8]. The emerging NIST Cybersecurity Framework 2.0 embeds cryptography within its "Protect," "Detect," and "Respond" functions, emphasizing continuous algorithm review and replacement mechanisms [9]. International standards-ISO/IEC 27001 (control A.10.1.2) and ENISA's Crypto-Agility Guidelines-similarly mandate planning for algorithm migration and modular cryptographic implementations.

- **Abstraction Layers** Implement cryptographic service providers (CSPs) or crypto-service APIs that expose generic interfaces (encrypt, decrypt, sign, verify), hiding algorithm-specific details.
- **Policy Engines** Store algorithm preferences and parameter roll-out schedules in external policy files or configuration databases to avoid code changes for algorithm swaps.
- **Key Envelopes** Wrap data-encryption keys (DEKs) with key-encryption keys (KEKs) bound to specific algorithms-simplifying bulk re-encryption when KEK algorithms change.
- **Vendor Requirements** Include crypto-agility capabilities in procurement contracts and require timely firmware or library updates to support new algorithms.



Training & Operational Readiness

Cryptographic risk is dynamic: new attacks, algorithm deprecations, or implementation flaws can emerge at any time. Embedding continuous monitoring and governance processes ensures the cryptographic estate remains robust. NIST CSF 2.0's "Detect" and "Respond" functions mandate automated alerts for deprecated algorithm usage, performance anomalies, and validation failures [9]. FIPS 140-3 revalidation cycles and ISO/IEC 27002's control A.12.6.1 on technical review of applications reinforce the necessity of recurring audits.

- **Automated Alerts** Integrate cryptographic module logs into SIEM systems and set alerts for deprecated algorithm calls or failed certificate validations.
- **Performance Baselines** Maintain metrics on encryption/decryption latencies, error rates, and resource consumption. Investigate significant deviations.
- **Vulnerability Assessments** Schedule annual third-party penetration tests focused on cryptographic implementations, including side-channel and fault injections.
- **Governance Board Reviews** Convene a Cryptography Governance Board quarterly to review audit findings, algorithm roadmaps, incident reports, and update migration plans.

Chapter 8

Regulatory, Compliance & Governance

Regulatory, Compliance & Governance

As organizations advance toward quantum-safe operations, they must navigate a complex landscape of directives, mandates, and governance frameworks. Regulatory pressure now extends beyond traditional information-technology (IT) security into quantum readiness, requiring enterprises to embed cryptographic agility into their risk-management and compliance programs. This chapter examines (a) global directives that set high-level expectations; (b) industry-specific mandates shaping sectoral compliance; (c) cross-cutting governance frameworks for policy, oversight, and auditing; and (d) the vendor ecosystem, including certification bodies. By understanding these elements and the specific terminology they employ, executives can align their Post-Quantum Cryptography (PQC) strategies with current and emerging obligations.

Global Directives

Global directives are high-level policy instruments-often non-binding recommendations-issued by governmental or multinational organizations to harmonize practices across borders

- EU Commission Recommendation on Post-Quantum Cryptography urges Member States to develop coordinated plans for migrating to quantum-resistant algorithms by 2026 (general infrastructure) and 2030 (critical services) [1].
- U.S. NSTAC (National Security Telecommunications Advisory Committee) Study on National Preparedness for Post-Quantum Cryptography (Aug 2024) analyzes gaps in critical-infrastructure security; NSTAC reports inform presidential policy but do not carry legislative force [2].
- NIST IR 8547 (“Initial Public Draft”) formalizes a phased migration roadmap, defining key concepts such as confidentiality horizon (the duration data must remain secure) and hybrid deployment (running classical and PQC algorithms in parallel) to standardize U.S. federal guidance [3].
- ETSI TS 104 015 V1.1.1 is a Technical Specification that prescribes hybrid key-exchange profiles-layering classical algorithms (e.g., X25519) with post-quantum Key-Encapsulation Mechanisms (KEMs, e.g., Kyber) under attribute-based access policies for fine-grained decryption control [4].
- ITU-T Recommendation Y.3800 establishes the architectural framework for Quantum Key Distribution (QKD) networks, defining terms such as QKD link, trusted node, and key-management layer to ensure global interoperability [5].
- BIS (Bank for International Settlements) Paper No 158, “Quantum-readiness for the financial system: a roadmap,” provides a structured framework for central banks and financial institutions, emphasizing awareness, comprehensive cryptographic inventory, crypto-agility, defence-in-depth, and phased migration planning [13].

Industry Mandates

Industry mandates are regulatory requirements or standards embedded within sector-specific compliance regimes:

Finance

- EBA (European Banking Authority) Guidelines on ICT (Information and Communications Technology) and Security Risk Management (EBA/GL/2019/04) require robust cryptographic risk assessments and key-rotation policies. These guidelines feed into the EU’s DORA (Digital Operational Resilience Act), which mandates that financial entities maintain crypto-agility capabilities-that is, the ability to switch algorithms quickly-in support of continuous operations [6][7].
- MAS (Monetary Authority of Singapore) Advisory MAS/TCRS/2024/01 outlines the cybersecurity risks posed by quantum computing and recommends measures such as algorithm inventory, hybrid-scheme adoption, and governance updates for financial institutions [14].

Healthcare

- FDA (U.S. Food and Drug Administration) **“Cybersecurity in Medical Devices”** Guidance (Jun 2025) requires device manufacturers to demonstrate reasonable assurance that encryption controls remain effective over the product lifecycle, and to plan for post-market algorithm updates [8].

Critical Infrastructure

- CISA (Cybersecurity and Infrastructure Security Agency) Critical Infrastructure Cybersecurity Framework incorporates findings from RAND’s Quantum Vulnerabilities Assessment, urging operators to develop sector-specific PQC roadmaps and treat quantum-hardening as a core resilience activity [9].

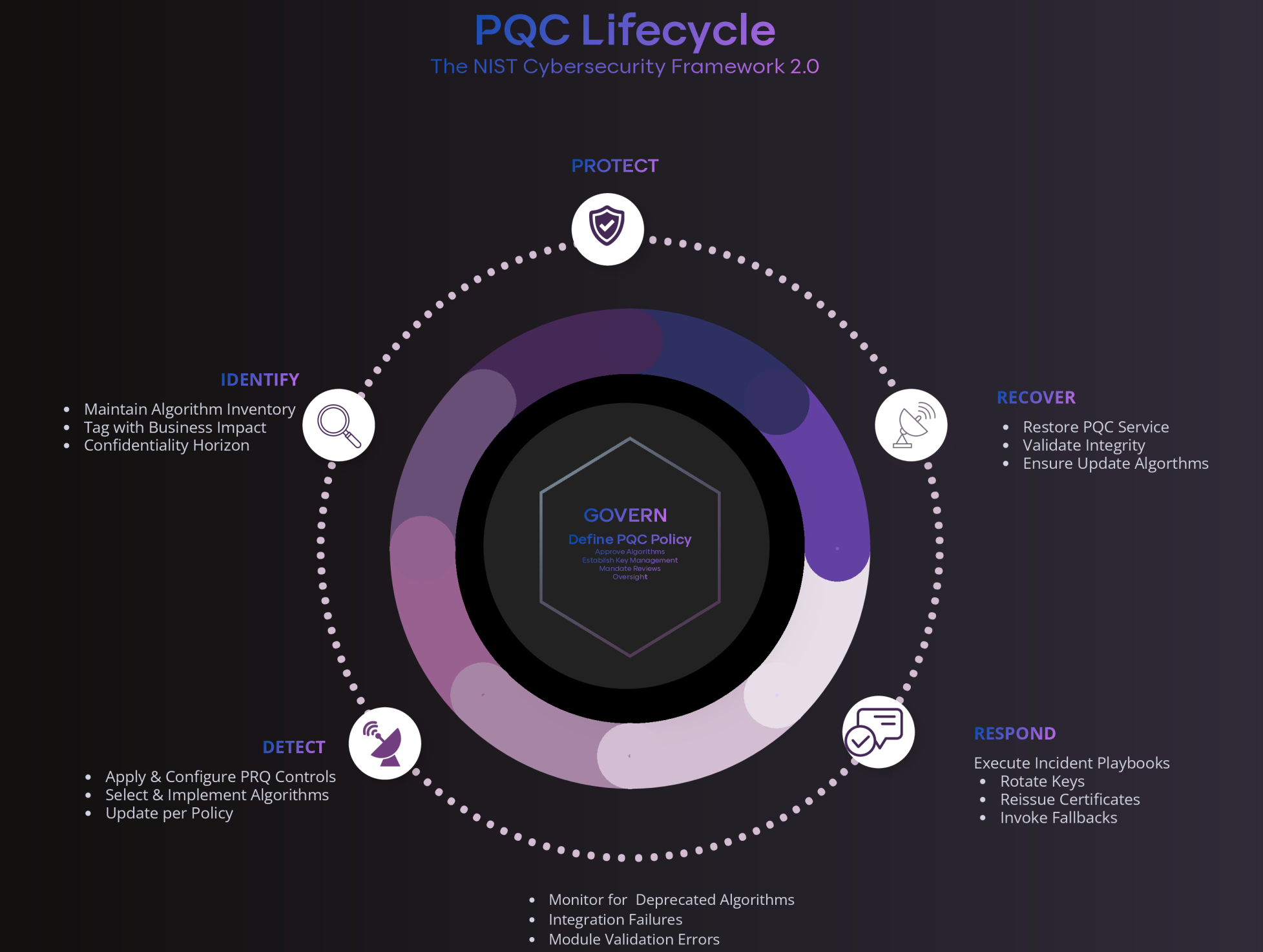
Frameworks for Policy & Oversight

To govern PQC adoption, organizations should leverage established governance and compliance models:

- **The NIST Cybersecurity Framework 2.0** (Draft, Mar 2024) introduces a new top-level function, **Govern**, explicitly recognizing the need for organizational oversight and policy management of the cybersecurity program-including cryptographic governance. Under Govern, roles and responsibilities are defined for approving algorithm choices, establishing key-management policies, and mandating periodic reviews. The existing five functions are then applied to cryptography as follows
 - **Identify:** Maintain a complete algorithm inventory, tagged with business impact and confidentiality horizon [3].
 - **Protect:** Apply and configure cryptographic controls-selecting, implementing, and updating algorithms per policy.
 - **Detect:** Monitor for usage of deprecated or weakened algorithms, integration failures, and module validation errors.
 - **Respond:** Execute pre-approved incident playbooks for cryptographic failures-rotating keys, reissuing certificates, and invoking fallback mechanisms.
 - **Recover:** Restore cryptographic services and validate integrity post-incident, ensuring updated algorithms are in place.

Together, Govern plus the five core functions establish a continuous, metrics-driven lifecycle for cryptographic assets-covering inventory, validation, deprecation, and oversight [10].

- **ISO/IEC 27001:2013** defines an **Information Security Management System (ISMS)** with Annex A.10 mandating documented **cryptographic policies, key-management procedures, and periodic key reviews** [11].
- **ISO/IEC 27002:2013** offers a **code of practice** detailing controls-such as **Control 8.24** (Use of cryptography), mandating that cryptographic mechanisms be designed and operated to protect the confidentiality, integrity, and authenticity of information, and that key management processes support their secure lifecycle..
- **COBIT 2019** provides a governance framework introducing objectives like **EDM05 (Ensure Risk Optimization)**and **DSS05 (Manage Security Services)**, which can be mapped to cryptographic governance processes and crypto-agility requirements [12].



Ecosystem & Vendor Landscape

The PQC ecosystem comprises several vendor and service categories, each contributing to a secure, resilient infrastructure. Key roles, typical activities, and illustrative examples are outlined below:

1. Crypto-Inventory Providers

- **Role** Automated discovery and classification of all cryptographic assets (algorithms, key lengths, protocol contexts) across networks, applications, and endpoints.
- **Activities**
 - Initial baseline scan; asset annotation with metadata (e.g., confidentiality horizon per NIST IR 8547).
 - Continuous integration with configuration-management databases or GRC (Governance, Risk, and Compliance) platforms.
- **Examples** Venafi Crypto-Inventory Service; Thales CipherTrust Discovery.

2. Threat-Register Services

- **Role** Real-time intelligence on cryptanalytic advances, new vulnerabilities, and PQC standard updates.
- **Activities**
 - Publishing subscription feeds of side-channel exploits, algorithm deprecations, and draft standards.
 - Correlating advisories with inventory to flag at-risk assets and trigger governance workflows.
- **Examples:** CISA Quantum-Readiness Alerts; Recorded Future PQC Intelligence.

3. PQC Software Vendors

- **Role** Implementations of NIST-approved PQC algorithms in two forms: reference code for proof-of-concept and production SDKs for enterprise deployment.
- **Activities:**
 - Compatibility validation using libraries such as liboqs (Open Quantum Safe).
 - Performance benchmarking and integration into pilot environments.
- **Examples** PQShield SDK; ISARA Radiate; QuSecure Universe.

4. Digital-Communication Hardware Vendors

- **Role** Embedded PQC support in devices securing data-in-transit (e.g., firewalls, VPN gateways, HSMs).
- **Activities**
 - Firmware updates enabling hybrid key-exchange (e.g., X25519+Kyber) in TLS (Transport Layer Security) or IPsec (Internet Protocol Security) handshakes.
 - Configuration interfaces for PQC parameter selection and monitoring handshake metrics.
- **Examples:**
 - Firewalls & VPNs: Cisco Secure Appliance PQC Module; Palo Alto Networks TLS+Kyber Preview.
 - HSMs: Thales nShield PQC Firmware; Utimaco CryptoServer PQC Edition.

5. Open-Source vs. Commercial Suites

- **Open-Source Projects** Community-driven, transparent codebases (e.g., liboqs) under permissive licenses but without formal SLAs or certification.
- **Commercial Solutions** Offer SLAs, integration services, certified modules, graphical management, and policy-engine capabilities.
- **Activities** Early proofs-of-concept with open-source, followed by production deployment on commercial platforms.
- **Examples** liboqs; Thales CipherTrust Manager with PQC plug-in; Venafi KeyProtect PQC.

6. Certification & Conformance Labs

- **Role** Validation and certification of cryptographic modules against security and interoperability standards.
- **Activities**
 - FIPS 140-3 testing under NIST CMVP, yielding Validation Certificates for U.S. federal compliance [3].
 - Common Criteria (ISO/IEC 19790/24759) evaluations assigning EALs (Evaluation Assurance Levels).
 - Interoperability events (e.g., ETSI Plugtests) to verify conformance to PQC profiles and hybrid-TLS specifications.
- **Examples** NCC Group, TÜV Rheinland, A-LIGN (CMVP labs); BSI (Germany), ANSSI (France) (Common Criteria test bodies).

Chapter 9

Use Cases & Adoption Scenarios

Use Cases & Adoption Scenarios



Financial Services: Secure Payments & Blockchai

Financial institutions rely heavily on public-key cryptography-for TLS in payment networks, EMV™ chip cards, and digital signatures on transactions and smart contracts. Quantum computers running Shor’s algorithm could factor RSA keys or solve elliptic-curve discrete logarithms, exposing payment data and blockchain integrity to retroactive decryption and forgery [4].

Context & Risk

- **Secure payments** Payment Card Industry (PCI) networks use RSA/ECDSA for transaction authentication. A “harvest-now/decrypt-later” adversary can record card-holder data today and decrypt it once quantum-capable machines appear [4].
- **Blockchain** Cryptocurrencies like Bitcoin and Ethereum use ECDSA for account control; a sufficiently large quantum computer could forge transactions and steal funds [3].

PQC Solutions

- Hybrid TLS deployments combine classical key exchange (e.g., X25519) with a PQC Key-Encapsulation Mechanism (KEM) such as CRYSTALS-Kyber, preserving backward compatibility while beginning the PQC transition [4].

PQC-enabled payment SDKs replace or augment existing card-provisioning and authorization logic with lattice-based signatures (e.g., Dilithium) or hash-based signatures (e.g., SPHINCS+).

Examples

- FS-ISAC’s “Future State” paper outlines a 5–20 year roadmap for PQC readiness in financial services, recommending early PoC pilots on card-authorization systems and payment gateways [1].
- PCI DSS 4.0’s requirement 12.3.3 mandates an up-to-date “inventory of cryptographic cipher suites and protocols,” which includes planning for PQC migration under best-practice guidance [2].
- The QRL Show’s November 2023 panel detailed “Downtime Required for Bitcoin Quantum Safety,” highlighting blockchain-specific migration steps such as key rotation schedules and signature-scheme upgrades [3].



Government & Defense: Classified Communications & Satellite Links

Sensitive government and defense communications-from VPNs protecting classified networks to encrypted satellite telemetry-depend on public-key systems that are vulnerable to quantum attacks. A breach could expose national secrets or disable critical command-and-control channels [4][5].

Context & Risk

- **Classified comms** IPsec VPNs and TLS tunnels often use ECC-256; Shor’s algorithm on a fault-tolerant quantum computer would instantly compromise their confidentiality [4].
- **Satellite links** Spaceborne encryption (uplink commands, downlink telemetry) uses classical ciphers secured by public-key wrapping; interception of these long-lived signals poses a high HNDL risk [4][6].

PQC Solutions

- Hybrid IPsec configurations embed lattice-based KEMs (e.g., Kyber) into IKEv2 exchanges, ensuring that even if ECC is broken, sessions remain secure.
- Space-qualified PQC libraries provide key wrappers compatible with satellite hardware, enabling post-launch firmware updates of ground-station decryptors.

Examples

- CISA’s Post-Quantum Cryptography Initiative coordinates federal agencies to inventory vulnerable assets and pilot PQC in government networks [5].
- QuSecure demonstrated a live Earth-to-satellite PQC link using a lattice-based KEM, marking the first post-quantum-resilient data transmission to multiple orbits [6].
- The U.S. General Services Administration (GSA) published a guide for federal agencies to adopt hybrid cryptography in critical systems, including PQC pilots in classified-level networks [7].



IoT & Embedded Systems

IoT devices-sensors, industrial controllers, smart meters-are constrained by processing power, memory, and energy. Yet many already use RSA or ECC for firmware updates and secure telemetry, creating a vast quantum-vulnerable attack surface [4].

Context & Risk

- Resource constraints limit key sizes and computational complexity, making naïve PQC adoption challenging.
- Long device lifespans (5–10 years) mean that firmware-signed images stored today could be retroactively compromised via HNDL attacks [4].

PQC Solutions

- Lightweight lattice schemes (e.g., NTRU, Saber) and streamlined code-based protocols have been optimized for low-power microcontrollers, balancing security and performance [8].
- Hybrid bootloaders validate firmware signatures using both ECDSA and a PQC signature (e.g., Dilithium), smoothing the migration path.

Examples

- Fernandez-Carames et al. survey post-quantum IoT architectures, recommending parameter-tuned implementations of Saber and NTRU-Prime for embedded deployments [8].
- Arm’s CryptoCell-P module offers dual-stack support, enabling PQC key-exchange alongside traditional ECC in constrained devices



Cloud Services & Data at Rest

Cloud platforms encrypt data at rest using key-envelope techniques: symmetric Data-Encryption Keys (DEKs) are wrapped by asymmetric Key-Encryption Keys (KEKs). If an attacker obtains DEKs via a quantum-broken KEK, all stored data becomes exposed [4].

Context & Risk

- Key-envelope vulnerability: RSA or ECC KEKs used in Hardware Security Modules (HSMs) for DEK wrapping are quantum-vulnerable; data stored today may be held for years before decryption using a future quantum computer [4].
- Shared responsibility: Cloud customers must ensure that provider-managed keys also transition to PQC.

PQC Solutions

- PQC KEK integration: Replace RSA/ECC KEKs in HSMs with lattice-based KEMs (e.g., Kyber) for wrapping DEKs, requiring no changes to existing symmetric-key operations.
- Interoperability testing: NIST’s SP 1800-38C workstream provides reference test suites for PQC in TLS, SSH, and HSMs, enabling cloud-service providers to validate PQC support [9].

Examples

- Several cloud providers (AWS, Azure, Google Cloud) are rolling out preview features for PQC-wrapped key-envelope services, allowing customers to generate and rotate Kyber-wrapped KEKs.
- NIST NCCoE’s Interoperability and Performance report includes guidance on deploying PQC algorithms in virtualized HSMs and containerized TLS proxies [9].

Chapter 10

Challenges & Open Questions

Challenges & Open Questions

As organizations advance along their PQC (Post-Quantum Cryptography) migration journey, they face unresolved technical, operational, and governance challenges. These open questions highlight areas where standards are evolving, solutions are being tested, and long-term answers remain uncertain. Addressing them requires sustained collaboration across industry, academia, and government.



Performance Bottlenecks in Constrained Environments

Post-quantum schemes generally demand larger key sizes (the mathematical “locks” used in cryptography) and higher computational loads than legacy algorithms. While server-class hardware can absorb this cost, resource-constrained devices-IoT (Internet of Things) sensors, embedded controllers, smart meters-may struggle

- **Latency and bandwidth:** Lattice-based KEMs (Key Encapsulation Mechanisms, protocols that set up shared encryption keys) such as Kyber generate kilobyte-scale ciphertexts (encrypted messages), potentially straining wireless links or mobile applications.
- **Energy consumption:** Increased arithmetic operations reduce battery life in edge devices.
- **Hardware acceleration:** Efficient implementations (using specialized chips such as GPUs, FPGAs, or ASICs) are emerging, but not yet widely deployed.

Open question: Can streamlined PQC variants (e.g., Saber, NTRU-Prime) or hybrid bootloaders (firmware that supports both classical and PQC signatures) strike the right balance of security and efficiency for massive IoT deployments?



Standard Maturity and Algorithm Agility

While NIST (U.S. National Institute of Standards and Technology) has finalized its first set of PQC standards, cryptanalysis (the practice of breaking ciphers) is ongoing. New attacks may expose weaknesses, and future rounds may introduce replacements. Organizations must avoid treating PQC adoption as “one and done.”

- **Crypto-agility gaps:** Legacy applications often hard-code algorithm identifiers (fixed references to specific algorithms), preventing smooth migration.
- **Interoperability:** Divergent parameter sets (different technical options for the same algorithm) across vendors create fragmentation.
- **Regulatory pressure:** Compliance regimes may freeze requirements before standards have fully matured.

Open question: How can enterprises design architectures that treat cryptographic primitives (the building blocks of encryption) as interchangeable modules without constant re-engineering?



Long-Term Key-Management Strategies

Key management (the way organizations generate, distribute, and retire encryption keys) becomes more complex in a PQC world. Larger key sizes strain certificate infrastructures (the systems that issue and validate digital IDs), and stateful schemes (where each key must be carefully tracked to prevent reuse, such as hash-based signatures) require new operational discipline.

- **Certificate lifetimes:** Shortened key-rotation intervals (changing keys more often) mitigate HNDL (Harvest-Now/Decrypt-Later) risks but increase administrative overhead.
- **Archival data:** Long-term confidentiality horizons (how long data must remain secure-e.g., decades for medical or defense records) demand strategies for re-encrypting stored assets as standards evolve.
- **Integration with HSMs/KMS:** HSMs (Hardware Security Modules) and KMS (Key-Management Services) will need firmware updates and new APIs to support PQC without breaking existing workloads.



Integration with Quantum Key Distribution (QKD)

QKD offers physics-based key exchange that complements PQC, but integration remains challenging. To guide decision-making, organizations should recognize the fundamental differences. Organizations should balance the deployment of PQC and QKD by using a risk-based, layered defense framework that utilizes PQC for its versatility and scalability, reserving QKD for where its physics-based guarantee is necessary.

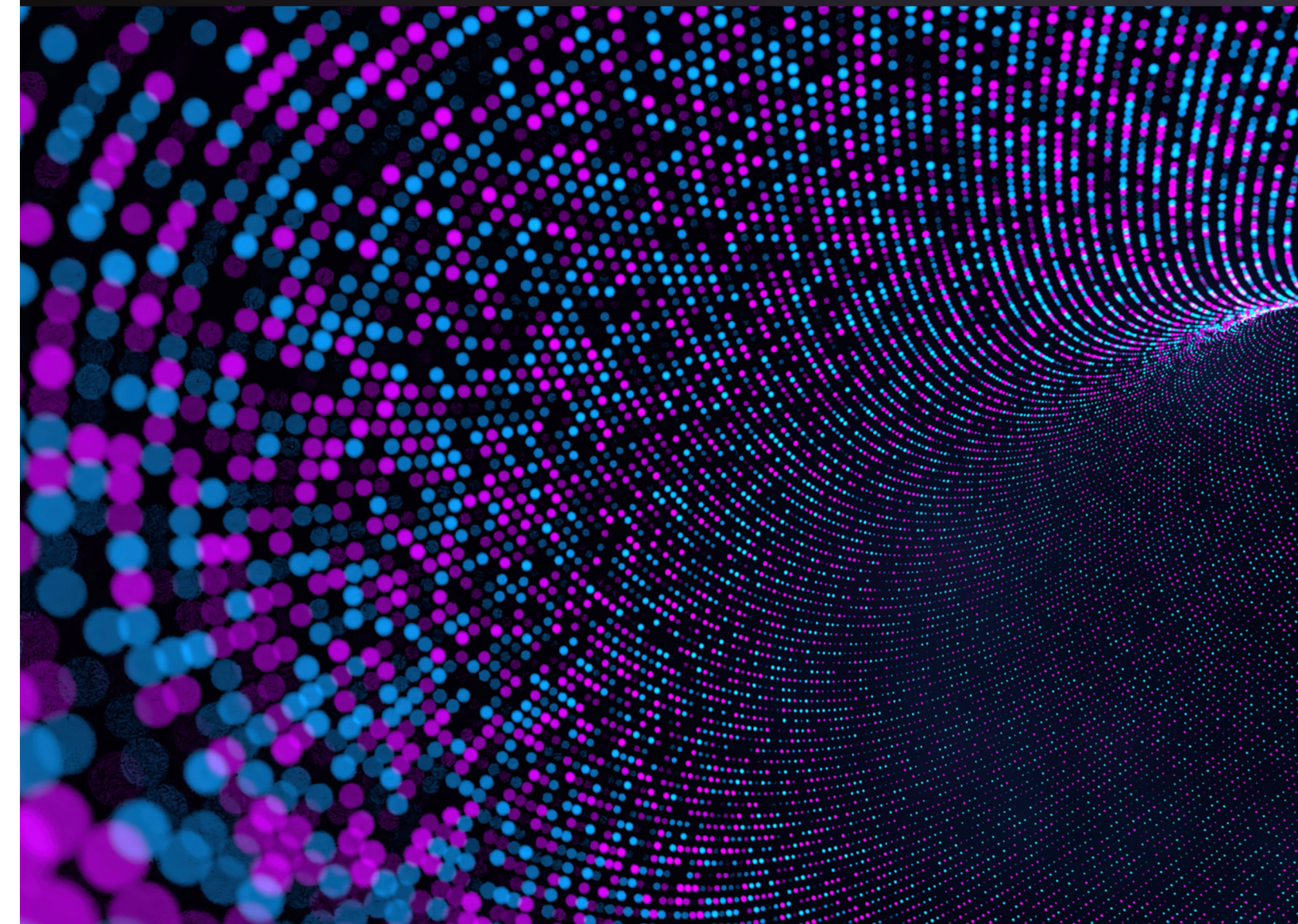
PQC should be the broad, default upgrade path for quantum resistance across the entire organization.

- **Software-Based Solution** PQC algorithms are software-based and designed to integrate easily into existing protocols like TLS, IPsec, and SSH.
- **Broad Coverage:** It is cost-effective and practical for virtually all digital systems, including servers, cloud environments, and mass-market IoT (Internet of Things) devices, where performance and memory constraints exist.
- **Mitigation of HNDL** PQC is essential for mitigating the Harvest-Now, Decrypt-Later (HNDL) risk across all long-term data archives.

QKD should be implemented for high-value, point-to-point environments where the guarantee of physics-based, tamper-evident key exchange is a mandatory security requirement.

- **Critical Links:** This includes defense, classified governmental communications, interbank financial backbones, and cross-border links.
- **Infrastructure Investment:** QKD requires significant investment in dedicated fiber optic channels or satellites, making it generally unsuitable and uneconomical for most standard enterprise applications.
- **Layered Resilience:** Combining PQC KEMs with QKD-derived keys provides layered resilience, offering the highest possible assurance, although standardized profiles for this hybrid approach are still immature.

What frameworks will ensure continuity of trust when re-signing archives or migrating root CAs (Certificate Authorities) to PQC algorithms?





Decision-Making Framework

The implied framework for determining the right balance is based on data classification and risk profile, driven by **the Confidentiality Horizon**:

Factor	Guide for Decision-Making	Allocation
Data Sensitivity	How sensitive is the data? Does it have a long confidentiality horizon (decades)?	Higher sensitivity mandates PQC. Highest sensitivity (national security) may justify QKD for the link.
Risk Profile	Is the security requirement crypto-agility (PQC's strength) or physics-based assurance (QKD's strength)?	PQC for general agility; QKD for provable tamper-evidence.
Infrastructure	Is the environment constrained (IoT, mobile, cloud)? Can it support dedicated fiber?	PQC for constrained/cloud environments; QKD where dedicated trusted node infrastructure is feasible.

There are several approaches to guarantee both short and long term security being explored.

- **Hybrid approaches** Combining PQC KEMs with QKD-derived keys could provide layered resilience, but standardized profiles (common rules for combining them) are still immature.
- **Infrastructure readiness** QKD requires dedicated fiber optic channels or satellites-investments that exceed most enterprise budgets today.
- **Governance and assurance** Certification frameworks for QKD are still developing, raising questions about interoperability and auditability (the ability to independently verify correctness).

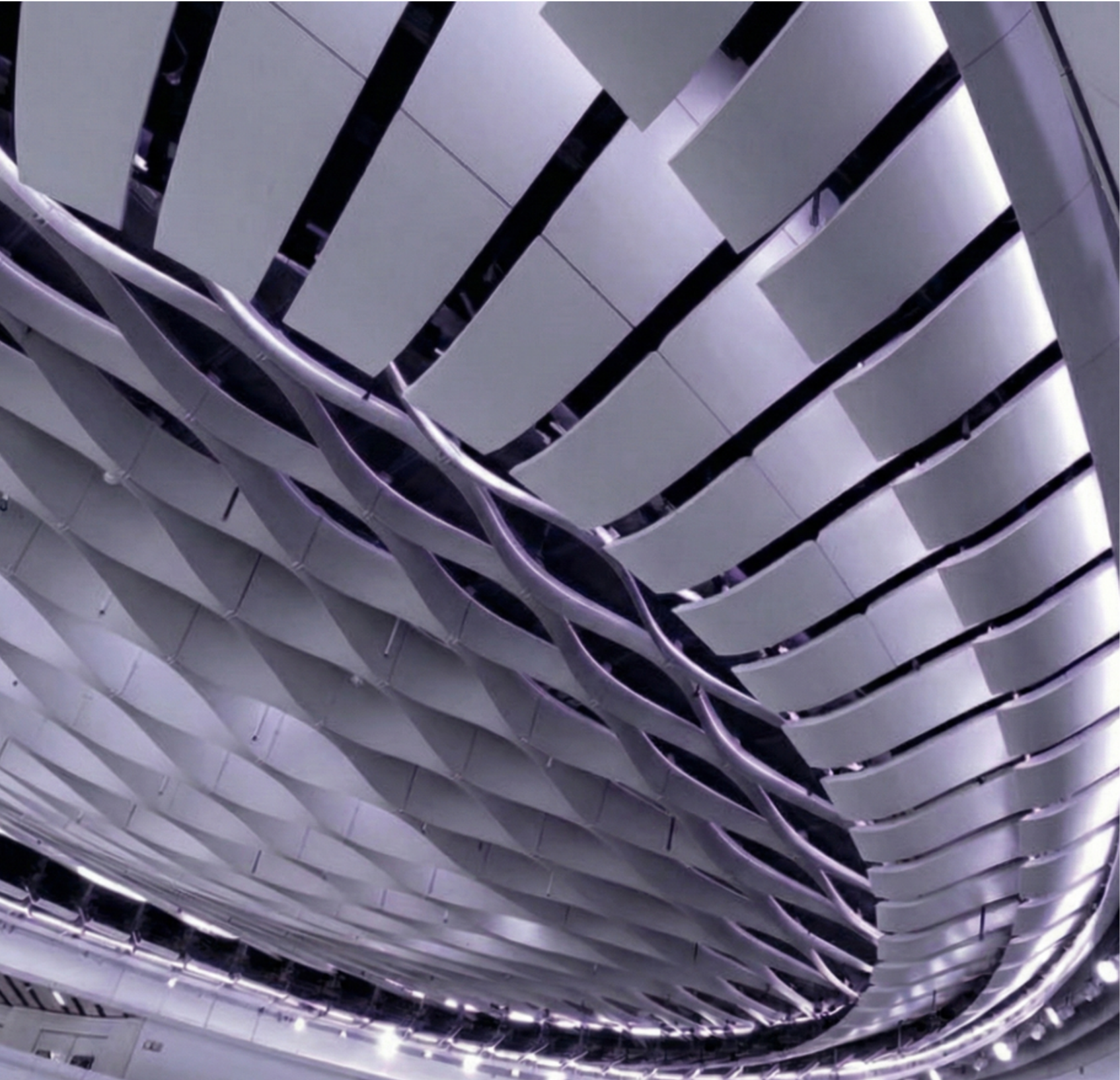
Open question How can organizations set the right balance between PQC and QKD-deploying PQC broadly as the default upgrade for digital systems, while reserving QKD for environments where physics-based assurance is critical (e.g., defense, interbank, or cross-border backbone links)? What frameworks can guide decision-making so that each technology is applied to the environments where it delivers the most value?

Chapter 9

Recommendations & Call to Action

Recommendations & Call to Action

The quantum threat is no longer theoretical. With standards now available, organizations must begin migration activities today to safeguard long-term data security. This chapter provides concise, actionable guidance for executives, technologists, and industry consortia.



Executive-Level Imperatives

- **Mandate cryptography governance** Establish a board-level charter and designate accountable executives for crypto risk (e.g., a “Chief Cryptography Officer” or equivalent mandate).
- **Fund inventory and pilots** Allocate budget for asset discovery (mapping where and how cryptography is used), hybrid deployments (running classical + PQC in parallel), and conformance testing.
- **Embed quantum into enterprise risk** Treat PQC migration as integral to operational resilience, not as a side project.
- **Engage regulators and peers** Stay ahead of compliance by aligning with NIST IR 8547 (U.S.), EU Quantum-Safe Roadmap, and sector mandates in finance, healthcare, and defense.



Technology and Process Checkpoints

- **Inventory & classification** Maintain a living inventory of all cryptographic assets, annotated with confidentiality horizons (how long each dataset must remain secure).
- **Hybrid deployment pilots** Begin with TLS/IPsec pilots (core protocols for secure internet and VPN connections) using PQC KEMs in parallel with classical algorithms.
- **Crypto-agility architecture** Introduce abstraction layers (software wrappers) and policy engines (central rulesets) that decouple applications from algorithm choices.
- **Validation & certification** Ensure modules undergo FIPS 140-3 or Common Criteria validation (formal testing standards for cryptographic products).
- **Training & readiness** Deliver role-specific education for executives (high-level awareness), engineers (technical implementation), and operators (day-to-day response); run incident-response drills for cryptographic failures.

Collaboration and Sharing within Industry Consortia

- **Sector working groups** Participate in industry consortia to exchange lessons learned.
- **Open-source engagement** Contribute to libraries such as Open Quantum Safe Project to accelerate maturity and broaden testing coverage.
- **Cross-border pilots** Collaborate on regional PQC/QKD trials to ensure interoperability and reduce fragmentation across jurisdictions.
- **Certification ecosystems** Support the growth of test labs and conformance programs to build trust in implementations.

Call to Action

Begin your PQC journey now. Start with inventory and hybrid pilots, institutionalize crypto-agility (design systems to swap algorithms quickly), and engage with peers and regulators to shape interoperable standards. Early adopters will not only reduce exposure to HNDL (Harvest-Now/Decrypt-Later) attacks but also position themselves as leaders in the emerging quantum economy.

The most resilient approach is a layered defense. By institutionalizing crypto-agility and executing hybrid pilots now, organizations can mitigate the immediate Harvest-Now/Decrypt-Later (HNDL) threat while staying aligned with global standards.

Call to Action : Begin your PQC journey now. Start with inventory and hybrid pilots, institutionalize crypto-agility (design systems to swap algorithms quickly), and engage with peers and regulators to shape interoperable standards. Early adopters will not only reduce exposure to HNDL (Harvest-Now/Decrypt-Later) attacks but also position themselves as leaders in the emerging quantum economy.



Glossary

Term (English)	Explanation (for general readers)
Quantum Technology	Technology that uses the rules of quantum physics (superposition, entanglement, interference) to create new kinds of computing, communication, and sensing.
Quantum Computing	Computers that use qubits (quantum bits) instead of classical bits, allowing them to solve some problems much faster than normal computers.
Qubit	A unit of quantum information that can be both 0 and 1 at the same time.
Superposition	A quantum effect where a qubit can be in multiple states at once.
Entanglement	A quantum effect where two qubits remain linked, so changing one instantly affects the other.
Interference	The way quantum states reinforce or cancel each other, shaping final outcomes.
NISQ (Noisy Intermediate-Scale Quantum)	Current generation of quantum computers (50–150 qubits), powerful but error-prone.
Post-Quantum Cryptography (PQC)	New cryptographic algorithms designed to resist attacks from quantum computers, while still running on classical computers.
Harvest Now, Decrypt Later (HNDL)	An attack method: record encrypted data today and wait until quantum computers can break it in the future.
RSA / ECC	Widely used classical cryptographic systems vulnerable to quantum computers.
Lattice-based Cryptography	PQC based on hard math problems in high-dimensional grids (lattices).
Code-based Cryptography	PQC based on the hardness of decoding random error-correcting codes.
Hash-based Cryptography	PQC using secure hash functions to build digital signatures.
Multivariate Cryptography	PQC based on solving systems of polynomial equations.
Supersingular Isogeny Cryptography	PQC using hard problems on elliptic curves.
KEM (Key Encapsulation Mechanism)	A method to securely exchange encryption keys.

Term (English)	Explanation (for general readers)
Digital Signature	A cryptographic method to prove authenticity and integrity of a message.
Crypto-Agility	The ability of a system to switch cryptographic algorithms quickly when old ones are broken.
TLS / IPsec / SSH	Core internet security protocols that will need PQC upgrades.
HSM (Hardware Security Module)	A secure hardware device for storing and managing cryptographic keys.
KMS (Key Management Service)	A service that handles cryptographic key lifecycle (generation, rotation, retirement).
Certificate Authority (CA)	A trusted entity that issues digital certificates for secure communications.
FIPS	U.S. standard for security requirements of cryptographic modules.
Common Criteria (CC)	International standard for evaluating IT security.
International standard for evaluating IT security.	A method of secure key exchange using quantum physics-detects eavesdropping.
Hybrid Cryptography	Using classical algorithms (e.g., RSA, X25519) in parallel with PQC algorithms (e.g., Kyber) and QKD system to ensure communications are secure against both today's classical threats and tomorrow's quantum threats.
Confidentiality Horizon	The length of time data must remain secure.
Governance	Oversight structures to ensure cryptography is used securely and updated properly.
NIST IR 8547	Key U.S. migration guidance for PQC adoption.
ENISA	EU Agency for Cybersecurity, issuing PQC migration guidelines.

References

Chapter 4: Quantum Computing Threat Landscape

[1] Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond (arXiv:1801.00862).

[2] IBM Quantum Development & Innovation Roadmap. (2025). IBM.

[3] Mosca, M., & Piani, M. (2019). Quantum Threat Timeline. Global Risk Institute.

[4] National Institute of Standards and Technology. (2024, November). IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft). NIST CSRC.

[5] U.S. Department of Energy. (2024, December). Quantum Information Science Applications Roadmap. U.S. DOE.

[6] Sectigo. (2025, May). Harvest Now, Decrypt Later Attacks & How They Relate to the Quantum Threat. Sectigo Resource Library.

[7] National Institute of Standards and Technology. (2025, March). The Road Ahead: Post-Quantum Cryptography Integration Guidance. NIST CSRC.

[8] National Institute of Standards and Technology. (2024, August). NIST Releases First Three Finalized Post-Quantum Encryption Standards (FIPS 203–205). NIST News.

[9] Cybersecurity and Infrastructure Security Agency. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography. CISA.

[10] National Institute of Information and Communications Technology. (2023). Q-ICT Roadmap: Quantum ICT for Future Networks. NICT.

[11] CEN-CENELEC. (2022). Standardization Roadmap on Quantum Technologies. CEN-CENELEC.

Chapter 5: Overview of Post-Quantum Cryptography (PQC)

[1] National Institute of Standards and Technology. Post-Quantum Cryptography. CSRC.

[2] National Institute of Standards and Technology. Report on Post-Quantum Cryptography (IR 8105). CSRC, 2016.

[3] National Institute of Standards and Technology. What Is Post-Quantum Cryptography? NIST, June 2023.

[4] National Institute of Standards and Technology. NIST Releases First Three Finalized Post-Quantum Encryption Standards (FIPS 203–205). NIST News, August 2024.

[5] Persichetti, E. Classic McEliece Update. NIST PQC Seminar #18, April 2024.

[6] Moody, D., & Robinson, A. Cryptographic Standards in a Post-Quantum Era. NIST, July 2022.

[7] National Institute of Standards and Technology. Recommendation for Stateful Hash-Based Signature Schemes (SP 800-208), October 2020.

[8] Seo, S., et al. "SIKE Round 2 Speed Record on Embedded Processors." NIST PQC Conference, 2018.

Chapter 6: Standards & Standardization Process

[1] NIST. (2020, July 22). PQC Third-Round Candidate Announcement. CSRC.

[2] NIST. (2019, Jan 31). IR 8240: Status Report on the First Round of the NIST PQC Standardization Process.

[3] NIST. (2020, Mar 9). IR 8309: Status Report on the Second Round of the NIST PQC Standardization Process.

[4] NIST. (2024, Aug). FIPS 203–205: First Three Finalized Post-Quantum Cryptography Standards. NIST News.

[5] NIST. (2022, July 5). Announcement of SPHINCS+ Addition; Removal of Protocols due to Cryptanalysis. CSRC.

[6] ETSI. (2025, Feb). TS 104 015 V1.1.1: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies.

[7] ETSI. (2024, Oct). TR 103 966 V1.1.1: Deployment Considerations for Hybrid Schemes.

[8] ISO/IEC JTC 1/SC 27 WG 2. (2024). Proposed Updates to ISO/IEC 18033-3 and ISO/IEC 19790.

[9] ISO/IEC JTC 1/SC 27. (2024). Committee Document SD11: Structure, Members, and Work Programme.

[10] Korea Internet & Security Agency. (2023, Dec). Quantum-Resistant Cryptography National Contest (KpqC) Finalist Announcement.

[11] Korea Internet & Security Agency. (2023). Quantum-Safe Cryptography Standardization Roadmap.

[12] ASEAN Secretariat. (2022). ASEAN Cybersecurity Cooperation Strategy (2021–2025).

[13] SAC/TC 260. (2025, Jan 23). Notice on International Standard Proposals for Cybersecurity and PQC.

[14] National Institute of Information and Communications Technology (NICT). (2023). Q-ICT Roadmap.

[15] ISO/IEC JTC 1/SC 27. (2024). Membership and Contributions of the Russian Federation.

[16] NIST. (2016, Apr 28). IR 8105: Report on Post-Quantum Cryptography.

[17] Cyber Security Agency of Singapore. (2024). Quantum Security Guidelines.

[18] Monetary Authority of Singapore. (2023). Advisory on Post-Quantum Cryptography Adoption in Financial Institutions.

[19] Infocomm Media Development Authority. (2023, Jun 6). National Quantum-Safe Network Plus (NQSN+) Framework.

References

Chapter 7: Migration Roadmap & Best Practices

[1] National Institute of Standards and Technology. IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft, Nov 2024). <https://doi.org/10.6028/NIST.IR.8547.ipd>

[2] Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. Quantum-Readiness: Migration to Post-Quantum Cryptography (Fact Sheet, Aug 21 2023). <https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography>

[3] National Institute of Standards and Technology. SP 1800-38C: Migration to Post-Quantum Cryptography – Technology Interoperability and Performance Report (Preliminary Draft, Dec 2023). <https://nccoe.nist.gov/projects/building-blocks/pqc-migration>

[4] National Institute of Standards and Technology. FIPS 140-3: Security Requirements for Cryptographic Modules (Mar 22 2019). <https://csrc.nist.gov/publications/detail/fips/140/3/final>

[5] National Institute of Standards and Technology. SP 800-50: Building an Information Technology Security Awareness and Training Program (Aug 2003). <https://doi.org/10.6028/NIST.SP.800-50>

[6] National Institute of Standards and Technology. SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model (Feb 1998). <https://doi.org/10.6028/NIST.SP.800-16>

[7] National Institute of Standards and Technology. SP 800-57 Part 3: Transitioning Cryptographic Algorithms and Key Lengths (2019). <https://doi.org/10.6028/NIST.SP.800-57pt3rev1>

[8] National Institute of Standards and Technology. IR 8417: Report on Crypto-Agility (Nov 2023). <https://doi.org/10.6028/NIST.IR.8417>

[9] National Institute of Standards and Technology. Cybersecurity Framework 2.0 (Draft, Mar 2024). <https://www.nist.gov/cyberframework>

[10] International Organization for Standardization. ISO/IEC 27001: Information Security Management Systems – Requirements (2013).

[11] European Union Agency for Cybersecurity. Guidelines on Cryptographic Agility (ENISA, Aug 2022). <https://www.enisa.europa.eu/publications/guidelines-on-cryptographic-agility>

Chapter 8: Regulatory, Compliance & Governance

[1] European Commission. (2024). Commission Recommendation on Post-Quantum Cryptography. Official Journal of the European Union.

[2] Cybersecurity and Infrastructure Security Agency. (2024). NSTAC Study on National Preparedness for Post-Quantum Cryptography. U.S. Department of Homeland Security.

[3] National Institute of Standards and Technology. (2024). IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft). NIST Computer Security Resource Center. <https://doi.org/10.6028/NIST.IR.8547.ipd>

[4] ETSI. (2025). TS 104 015 V1.1.1: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies. European Telecommunications Standards Institute.

[5] ITU-T Study Group 13. (2019). Recommendation Y.3800: Overview on Networks Supporting Quantum Key Distribution. International Telecommunication Union.

[6] European Banking Authority. (2025). Guidelines on ICT and Security Risk Management (EBA/GL/2019/04). EBA.

[7] European Parliament & Council. (2025). Regulation (EU) 2024/xxxx: Digital Operational Resilience Act (DORA). Official Journal of the European Union.

[8] U.S. Food and Drug Administration. (2025). Cybersecurity in Medical Devices: Quality System Considerations and Premarket Submissions. FDA.

[9] RAND Corporation. (2022). Assessments of Quantum Computing Vulnerabilities of National Critical Functions. RAND.

[10] National Institute of Standards and Technology. (2024). Draft Cybersecurity Framework 2.0. NIST.

[11] International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO.

[12] ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

[13] Bank for International Settlements. (2025). Quantum-Readiness for the Financial System: A Roadmap (BIS Paper No. 158). BIS.

[14] Monetary Authority of Singapore. (2022). Advisory on Addressing the Cybersecurity Risks Associated with Quantum Computing (MAS/TCRS/2024/01). MAS.

Chapter 9: Use Cases & Adoption Scenarios

[1] FS-ISAC. (2023). “Future State – Post-Quantum Cryptography (PQC) Working Group.” FS-ISAC.

[2] Encryption Consulting. (2023). “PCI DSS 4.0’s Role in Quantum-Safe Cryptography Transition.

[3] The QRL Foundation. (2023, November). The QRL show: Downtime required for Bitcoin quantum-safety <https://www.theqrl.org/>

[4] National Institute of Standards and Technology. (2024). “IR 8547: Transition to Post-Quantum Cryptography Standards” (Initial Public Draft). NIST CSRC.

[5] Cybersecurity and Infrastructure Security Agency. (2024). “Post-Quantum Cryptography Initiative.” CISA.

[6] QuSecure. (2022). “Post-Quantum Satellite Protection Rockets Towards Reality.”

[7] General Services Administration. (2025). “GSA and Post-Quantum Cryptography: Enabling a Secure Federal Future.”

[8] Fernández-Cárames, T. M., et al. (2024). “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things.” arXiv.

[9] National Cybersecurity Center of Excellence, NIST. (2023). “Interoperability and Performance of Post-Quantum Cryptographic Algorithms” (SP 1800-38C Preliminary Draft).

About SCBX

SCBX is the mothership of the financial technology business group, operating across three key business pillars: Banking Business, Consumer and Digital Finance Business, and Platform and Technology Business. In addition, SCBX also focuses on Climate Technology, aspiring to become The Most Admired Regional Financial Technology Group'.

The company conducts its business with flexibility and prudence in governance and risk management and has processes the potential to compete equally in global competitions.

Authors



Tutanon Sinthuprasith, Ph.D.
Head of R&D, SCBX



Poompong Chaiwongkhot, Ph.D.
Senior Research Fellow and Co-founder, QTFT



Nut Chukamphaeng
Senior Research Scientist, SCBX



Koravich Sangkaew
AI Engineer, SCBX



Artid Sringam
Cloud and AI Technology Risk Specialist, SCBX



Kaweewut Temphuwapat
Cheif Innovation Officer, SCBX
Cheif Executive Officer, SCB10X



Parinya Jutasen
Technology Risk Manager, SCB



Noppadol Songsakaew
Head of Security Advisory, SCB



Khanittha Sivakoses
Head of Encryption Key Management & Application
Deployment, SCB



Book Designer
Thunkamon Payakkachon
Project Coordinator, SCBX

This publication was made possible through the collaboration of



SCB^x