Journal Article

Global Roadmaps for Post-Quantum Era in Finance: Policies, Timelines, and a Pragmatic Playbook for Migration

Kuka, C., Muhyaddin, S., Lee Teh, P. and Davies, L.

FinTech

Article

Global Roadmaps for Post-Quantum Era in Finance: Policies, Timelines, and a Pragmatic Playbook for Migration

Colin Kuka [1,*], Sanar Muhyaddin [2], Phoey Lee Teh [1] and Leanne Davies [1]

[1] Cyber Innovation Academy, Wrexham University, Wrexham LL11 2AW, UK
[2] Wrexham Business School, Wrexham University, Wrexham LL11 2AW, UK
* Correspondence: colins.kuka@outlook.com

Abstract

Quantum computing threatens the security foundations of global financial systems, exposing long-lived data and signed digital assets to "harvest-now, decrypt-later" attacks. While the timeline for cryptographically relevant quantum computers remains uncertain, regulatory signals from the USA, UK, EU, Canada, and Australia converge: financial institutions and payment infrastructures must begin migrating to post-quantum cryptography (PQC) now to preserve confidentiality, integrity, and systemic stability. This paper maps emerging standards and roadmaps, contrasting binding requirements like the EU's DORA crypto-agility provisions with non-binding guidance from NIST, ENISA, and ETSI. Despite a shared intent to secure high-risk use cases by 2030–2031 and complete migration by 2035, divergences in enforcement and milestones create uncertainty for cross-border banks and financial market infrastructures. In parallel, technical adoption is advancing: major browsers, cryptographic libraries (OpenSSL/BoringSSL), and CDNs (e.g., AWS CloudFront) have deployed hybrid PQC key exchange in TLS 1.3, proving confidentiality defenses are viable at internet scale. The paper synthesizes historical transition lessons, sector-specific regulatory drivers, and operational constraints in payment infrastructures to derive a new, principle-based migration: crypto-agility, risk-prioritized scoping, hybrid deployment, vendor and supply-chain alignment, independent testing, and proactive supervisory engagement. Acting now reduces long-tail exposure and ensures readiness for imminent compliance and interoperability deadlines.

Keywords: post-quantum; quantum-safe migration; crypto-agility; hybrid TLS; financial market infrastructures; operational resilience; cross-border compliance; NIST FIPS 203/204; ENISA guidance; harvest-now-decrypt-later

JEL Classification: G28; G15; D82; O33; L86

Academic Editor: David Roubaud

Received: 23 October 2025
Revised: 26 December 2025
Accepted: 2 January 2026
Published: 9 February 2026

1. Introduction

Cryptography is the invisible foundation of our digital economy. Every secure website we browse, every bank transfer we authorize, and every digital document we sign relies on cryptographic systems to ensure trust, confidentiality, and integrity. In a world where almost every interaction is mediated by online communications, transactions, digital documenmts and signatures, cryptography quietly underpins the stability of modern life.

The emergence of quantum computing fundamentally challenges this foundation. Quantum computing, once limited to theory and specialized labs, is moving toward real-world uses that could challenge the cryptographic backbone of today's security systems. It

marks a major shift in computing power: unlike classical machines, quantum processors use quantum bits, or "qubits," which can exist in superposition and evaluate many possibilities at once. A striking example came when Google's 53-qubit Sycamore processor performed a targeted task, which involved sampling a quantum circuit one million times in about 200 s. The equivalent task for a state-of-the-art classical supercomputer was estimated to take approximately 10,000 years. [1]. Although that demonstration was tailored to highlight quantum advantage and doesn't immediately endanger encryption, it underscores the rapid progress in quantum tech that is likely to influence payment security in the future.

Once quantum computers become cryptographically relevant, stored ciphertexts and signed artifacts protected by RSA/ECC will face retrospective compromise under a "harvest now, decrypt later" (HNDL) scheme: adversaries can capture encrypted data today and decrypt it when quantum capabilities mature [2,3]. In this scenario, attackers passively record encrypted data today: such as TLS-protected web traffic, payment messages, encrypted documents, and digitally signed software or PDFs, intending to decrypt or forge them in the future once stronger attacks (e.g., quantum computers breaking RSA/ECC) become feasible. This creates long-tail risk (Figure 1): past online communications can be exposed, historical transactions and stored customer data can be revealed, confidential archives (contracts, IP, medical or financial records) can be read, and legacy systems that still trust old signatures may accept forged updates or falsified documents. The practical defense is to reduce long-term exposure (use forward secrecy, limit retention), build crypto-agility, and begin transitioning to post-quantum cryptography. Furthermore, signatures on software updates, firmware for payment terminals, and payment network infrastructure could be forged if algorithms are not transitioned in time, creating systemic operational and integrity risks.

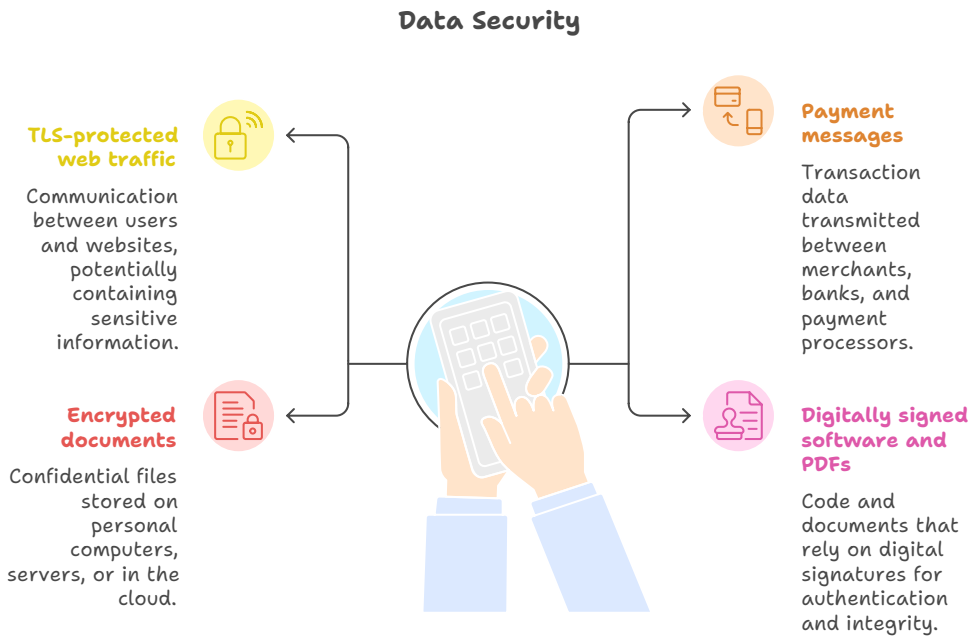


Figure 1. Intuitive illustration highlighting how quantum vulnerabilities relate to everyday digital interactions. The figure connects quantum risk to familiar data security applications such as: payment transactions, TLS-protected communications, encrypted documents, and digitally signed software; in order to emphasise that quantum computing will affect information accessed and transmitted through common devices, including smartphones.

Transitioning global payment infrastructure to quantum-resistant cryptography (post-quantum cryptography, PQC) is a complex sociotechnical challenge. Payment systems span heterogeneous stacks from constrained devices and point-of-sale terminals to data centers

and cloud microservices with strict latency, availability, and compliance requirements. Interoperability across card networks, gateways, and cross-border rails adds further coordination complexity. Significant technical debt in legacy cryptographic implementations, hard-coded algorithm identifiers, certificate profiles, and protocol assumptions (e.g., key sizes, message sizes, handshake flows) complicate replacement [4,5].

The literature contains comprehensive surveys that detail the strengths, limitations, and implementation challenges of various post-quantum cryptography (PQC) algorithms, with particular attention to their suitability for secure financial transactions and digital payment systems (classified in Table 1 [6–11]). The transition to PQC in financial institutions is complex—spanning legacy system compatibility, standardization, and regulatory compliance—and hybrid models that combine classical and post-quantum techniques are widely recommended during the migration phase [6,8,9]. Several reviews focus on post-quantum cryptography (PQC) within blockchain-based decentralized financial systems, highlighting privacy-preserving methods, performance trade-offs, and the need for quantum-safe digital signatures and key management [12–14]. However, centralized finance faces vastly larger challenges from quantum threats, which could undermine the security of traditional banking, payment infrastructures, and global financial networks far more profoundly than in decentralized systems. Across these studies, surveys emphasize the importance of testing environments, hardware acceleration, and cross-platform interoperability to enable robust PQC deployments in financial services [6,7,9,11].

Table 1. Surveyed PQC approaches and challenges for financial systems.

Focus Area	Key Insights	Citations
PQC Algorithm Surveys	Lattice, hash, code, multivariate, isogeny-based schemes reviewed	[6–10]
Financial System Impact	Disruption of secure transactions, need for hybrid/transition models	[6–8]
Blockchain Applications	PQC for privacy, digital assets, and quantum-safe blockchains	[12–14]
Implementation Challenges	Scalability, efficiency, regulatory, and legacy system integration	[6–8,11]

We contend that the international community must initially steer its focus toward the urgent improvement of cryptographic practices to mitigate the HNDL threat. While the long-term evolution of quantum computing remains uncertain in timing and scale, the HNDL vector transforms uncertainty into a present-day risk by converting today's encrypted communications, transactions, and archives into tomorrow's exposed assets. While the feasibility and timelines of large-scale, fault-tolerant quantum computers remain uncertain, this paper adopts the pragmatic assumption used by NIST, NSA, ENISA, and BIS: migration planning must begin irrespective of when cryptographically relevant quantum hardware may be realized. Detailed feasibility analysis—requiring specialised treatment of quantum error correction, qubit architectures, and coherence scaling—lies outside the scope of this financial and policy-focused work. However, regulators consistently emphasize that long migration timelines and the HNDL threat model justify early preparedness even under uncertainty. Our transition discussion is therefore grounded in regulatory and systemic-risk rationale rather than hardware forecasting. Accordingly, this paper positions crypto-agility, rigorous cryptographic asset discovery, and prioritized migration to post-quantum cryptography (PQC) as immediate, actionable imperatives for financial institutions and payment ecosystems. Beyond technical migration, this research aims to systematically examine progress in policies, standards, and legislation, with an em-

phasis on major governmental and institutional updates that define compliance timelines, interoperability requirements, and sector-specific obligations. We continuosly refer the state of guidance from leading bodies (e.g., NIST, NSA/CNSA, PCI SSC, EMVCo, ENISA, ETSI, and relevant national or regional regulations) to clarify what is required, by whom, and by when, thereby reducing ambiguity and helping stakeholders align roadmaps. Our objective is to clarify this continuosly evolving landscape into a practical framework for decision-makers in regulated industries, mapping policy milestones to concrete engineering steps (e.g., hybrid deployments, certificate and protocol profiles, testing and validation regimes, hardware/security module readiness, and operational governance).

In doing so, we contribute three elements: (i) a synthesis of current technical pathways for mitigating HNDL through crypto-agile architectures and PQC adoption; (ii) a policy and compliance landscape review highlighting interdependencies, gaps, and harmonization challenges across jurisdictions and ecosystems; and (iii) a prioritized set of near-term measures that organizations can adopt to reduce long-tail exposure. We conclude with an action-oriented agenda that identifies urgent steps—tightening key management and data retention, enabling forward secrecy and hybrid classical–post-quantum modes, preparing PKI and protocol upgrades, establishing testbeds and performance baselines, and instituting governance for rapid algorithmic change—while outlining a research roadmap to address open questions in performance, usability, certification, and cross-network interoperability. This rationale frames the work not as a speculative exercise in future-proofing but as a present necessity to safeguard the confidentiality, integrity, and availability of global payment and financial systems against foreseeable decryption and forgery risks. The remainder of this paper is structured as follows. Section 2 introduces the threat model and explains the long-term risks posed by harvest-now–decrypt-later attacks, as well as the barriers to rapid migration. Section 3 reviews historical lessons from previous cryptographic transitions, including adoption patterns and operational inertia. Section 4 examines system-wide challenges financial institutions face when migrating to quantum-safe cryptography, including the complexity of implementation across heterogeneous environments. Section 5 analyses quantum threats in the context of payment systems and outlines emerging regulatory drivers that may influence migration timelines. Section 6 presents a practical framework for quantum-safe transition planning, focusing on cryptographic governance, hybrid deployments, and vendor alignment. Section 7 discusses government-led post-quantum cryptography (PQC) roadmaps and the need for sector-wide coordination. Section 8 outlines near-term measures to reduce long-tail exposure, and Section 9 examines financial dependencies. Section 10 provides a practical playbook that can be used as a reference, while Section 11 discusses future waves of migration. Finally, Section 12 concludes the paper with key policy and technical recommendations.

2. Impact of Quantum Computing on Cybersecurity

Building on our rationale—prioritizing immediate mitigation of the HNDL risks and aligning technical migration with emerging policy and compliance milestones, we now examine how quantum-enabled adversaries affect core security properties in practice. Its impact is felt across three critical dimensions of cryptography [15]. First, it threatens *confidentiality* [16]: the security of the data we transmit and share with others could be compromised by quantum-enabled attackers capable of breaking encryption schemes that protect our information today. Second, it undermines *authentication*: the mechanisms by which we prove our identity and verify others. For example, when you install software, your computer automatically checks that it has been signed by a trusted publisher. A quantum-capable adversary could forge such a digital signature, inserting malicious software into trusted supply chains without detection. Finally, it jeopardizes *legal integrity*.

Digital signatures are often used to validate contracts and legal agreements. If an attacker could reconstruct a private key from past signatures, they would not only be able to falsify new documents but also call into question the validity of every past agreement signed using that key [17]. This would create profound legal and operational risks, extending far beyond any single contract.

A primary risk in preparing for the quantum era is underestimating its impact by overlooking how foundational cryptography is to the digital economy (Figure 2). Secure communications, financial transactions, software authenticity, and legal digital records all rely on cryptographic primitives and infrastructure [18,19].

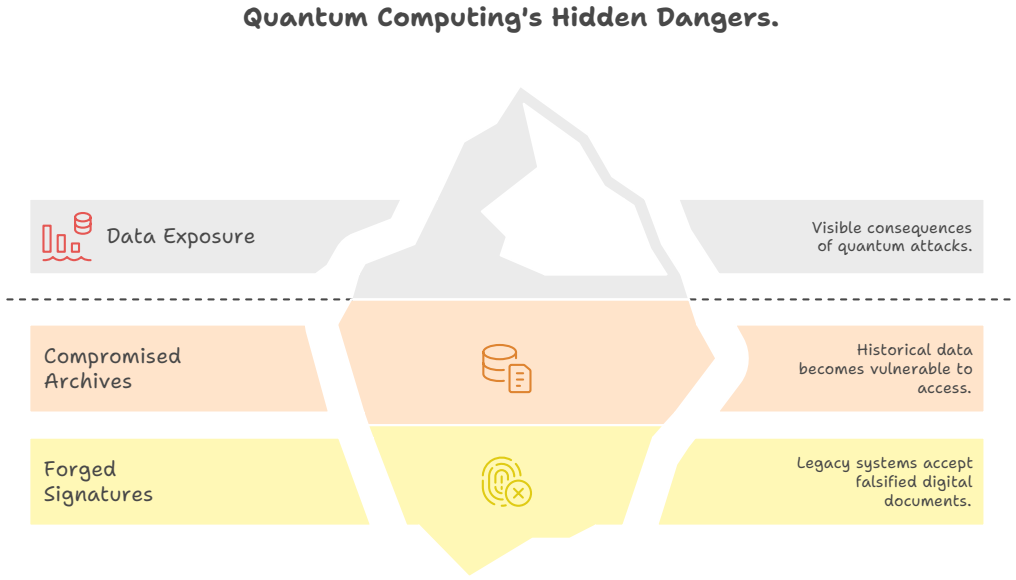


Figure 2. Conceptual overview of the depth of quantum-enabled cyber threats. While data exposure is the most visible consequence, the figure illustrates that more significant risks—such as compromise of historical archives and the ability to forge digital signatures—lie beneath the surface. This visual framing is intended to help readers recognise that quantum threats extend far beyond simple decryption.

2.1. Risk Timeline and Migration Urgency

A second, equally critical issue concerns the *transition path* to quantum-safe cryptography. How urgently an organization needs to move to quantum-safe cryptography for a specific system depends on three key factors (Figure 3):

- Data lifetime (shelf life): how long the information handled by the system must remain secure.
- Migration time: how long it will take to upgrade or replace the system with a quantum-safe solution.
- Threat timeline: how soon attackers are expected to have quantum computers capable of breaking today's cryptographic methods.

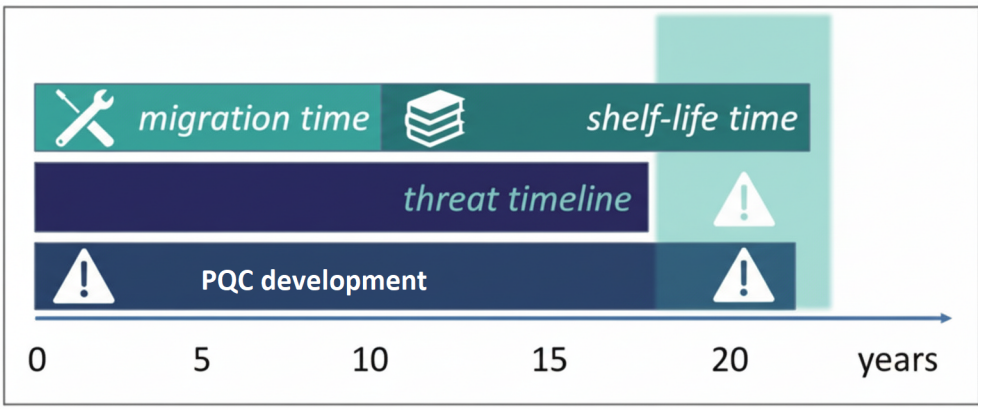


Figure 3. Conceptual illustration of the cryptographic transition risk window based on the commonly used Mosca inequality [2]. The timeline is not a quantitative prediction but a qualitative depiction of the relationship between migration time, data-protection lifetime, and the uncertain arrival of cryptographically relevant quantum computers. Exclamation marks indicate uncertainty ranges rather than specific dates.

If the time before quantum attacks become feasible is shorter than the combined period of how long the data needs to stay protected plus the time it takes to migrate, the system could be exposed before the transition is complete. Understanding the likely threat timeline helps organizations know how much time they really have to shift to post-quantum security. Estimating this timeline, however, is extremely difficult. Developing a practical quantum computer faces major scientific and engineering challenges, and experts still cannot predict when such machines will be powerful enough to threaten current encryption. Still, having an informed sense of how quickly progress is happening — and what milestones might signal growing risk — can help security managers plan and act before it is too late. It is important to clarify the assumptions underlying the discussion that follows. This work does not attempt to predict when quantum computers capable of breaking RSA or ECC will be engineered. Such forecasting depends on unresolved challenges in quantum error correction and scalable qubit design. Instead, we follow the approach taken by major standards and supervisory bodies, which treat PQC migration as a long-horizon resilience and compliance requirement independent of specific hardware timelines. Under this framing, the relevant drivers are the multi-year remediation period required for PQC adoption and the asymmetric risk posed by the HNDL model, which converts uncertainty about quantum capability into a present-day security concern. A commonly used risk framing (often attributed to Mosca) stipulates that organizations must ensure

$$T_{\text{migration}} + T_{\text{protection}} < T_{\text{threat-time}} \quad (1)$$

where $T_{\text{migration}}$ is the time required to discover, inventory, and migrate cryptographic assets and dependencies to post-quantum algorithms; $T_{\text{protection}}$ is the period during which today's sensitive data and signatures must remain secure and verifiable; and $T_{\text{threat-time}}$ is the projected arrival of cryptographically relevant quantum computers [2,20,21].

Failure to respect this inequality can produce concrete harms. For example, a digital signature placed today on a long-term contract (e.g., a multi-decade mortgage) may be rendered insecure in the future if an adversary can derive the private key using a quantum computer and then forge signatures. This threatens not only the integrity of a single document but the trustworthiness of every signature ever produced with that key. The operational, financial, and legal implications within regulated sectors, including finance, are significant [18,19,21].

2.2. Barriers to Timely Migration

Despite increasing awareness of the quantum threat, many organizations risk missing the safe transition window because the process of migrating to post-quantum cryptography (PQC) is considerably more complex than it appears at first glance. Several interrelated factors contribute to delay. As mentioned above, the primary cause is the persistent underestimation of quantum computing's impact on existing cryptographic infrastructures. The threat is often perceived as a distant or theoretical problem, leading to slow strategic planning and weak prioritization. Yet, as emphasized in policy analyses and technical advisories [18,19,21], cryptography underpins the confidentiality, authentication, and legal integrity of global digital and financial systems. A second source of delay is misunderstanding the complexity of migration itself. Transitioning from vulnerable schemes such as RSA and ECC to quantum-resistant algorithms is not a simple software update but a systemic overhaul that requires discovering and inventorying cryptographic assets, redesigning and testing communication protocols, replacing certificates and key hierarchies, validating interoperability across heterogeneous infrastructures, and preserving operational continuity [4,20]. Finally, the uncertainty surrounding the arrival of cryptographically relevant quantum computers encourages organizations to defer action, framing the risk as long term. This overlooks the "harvest now, decrypt later" (HNDL) threat model, in which adversaries capture encrypted communications and signatures today with the intent to decrypt or forge them once quantum capabilities mature [2,3].

In the financial sector, these challenges are magnified by systemic interdependencies and the long coordination cycles required for safe change. Financial institutions operate within a dense network of peers and shared market infrastructure, including Central Counterparties (CCPs) and Central Securities Depositories (CSDs). CCPs act as guarantors of trades between buyers and sellers (becoming the buyer to every seller and the seller to every buyer), while CSDs enable the transfer and safekeeping of securities through book-entry records rather than physical certificates. In such ecosystems, faster-moving entities are often constrained by the need to remain interoperable with the slower ones to adopt. The public–private coupling further complicates the picture: core payment and settlement systems—frequently owned or operated by central banks and other public bodies—*must migrate in parallel to preserve end-to-end security*. Any misalignment between private institutions and public infrastructure can create choke points that delay quantum-safe deployment.

Despite growing awareness, a persistent awareness and readiness gap remains. A 2022 report by KPMG and Germany's Federal Office for Information Security (BSI) surveying 100 large German companies concluded that many organizations were unlikely to achieve quantum safety in time [22]. Although some indicators may have improved since then, responses to two questions were particularly concerning: nearly 30% of respondents indicated plans to begin transitioning to quantum-resilient cryptography only in five years or more, and 32% considered the topic not applicable to them. This reflects a widespread misunderstanding of the criticality and ubiquity of cryptography in large organizations and hesitancy to initiate concrete actions despite clear signals and available guidance [3,23].

The cross-sector dependencies add further risk. Telecommunications and energy networks, both essential to the operation of digital payments and trading systems, must also adopt quantum-resistant mechanisms to maintain sector-wide resilience. Technology and service providers represent another critical dependency: financial firms rely on third-party cryptographic libraries, secure hardware modules, and cloud-based services. Prematurely deploying immature quantum-safe implementations can introduce instability or vulnerabilities, yet delaying adoption until commercial solutions are proven further extends migration timelines. The standards and governance ecosystem also moves slowly. Protocol

specifications, certificate formats, and supervisory guidance (e.g., TLS profiles, EMVCo and PCI SSC requirements) evolve gradually, and firms often hesitate to commit to large-scale PQC rollouts until these frameworks converge [3,5]. Finally, the capital planning cycles of large financial institutions can themselves impede rapid change. Security investment is often sequenced over multi-year horizons, and competing priorities may delay PQC adoption even once the threat is recognized.

These combined dynamics explain why migration timelines frequently exceed initial estimates, creating a dangerous gap if quantum capabilities arrive sooner than anticipated. Addressing these obstacles requires more than technical readiness alone: it demands sector-wide coordination, proactive engagement with vendors and infrastructure providers, and clearer regulatory and standards-based roadmaps to reduce uncertainty, synchronize migration schedules, and ensure end-to-end quantum resilience.

3. Historical and Technical Lessons from Cryptographic Transitions

Web security standards have evolved progressively over more than two decades (Figure 4), with the most notable changes occurring in the last ten years. Transport Layer Security (TLS) was introduced as a successor to the original Secure Sockets Layer (SSL) protocols during the late 1990s, with TLS 1.0 standardized in 1999 and TLS 1.1 following in 2006 [24]. TLS 1.2, released in 2008, became the dominant version throughout the 2010s, gradually replacing older and less secure versions such as SSLv2 and SSLv3, which were formally deprecated in 2011 and 2015, respectively [25,26].

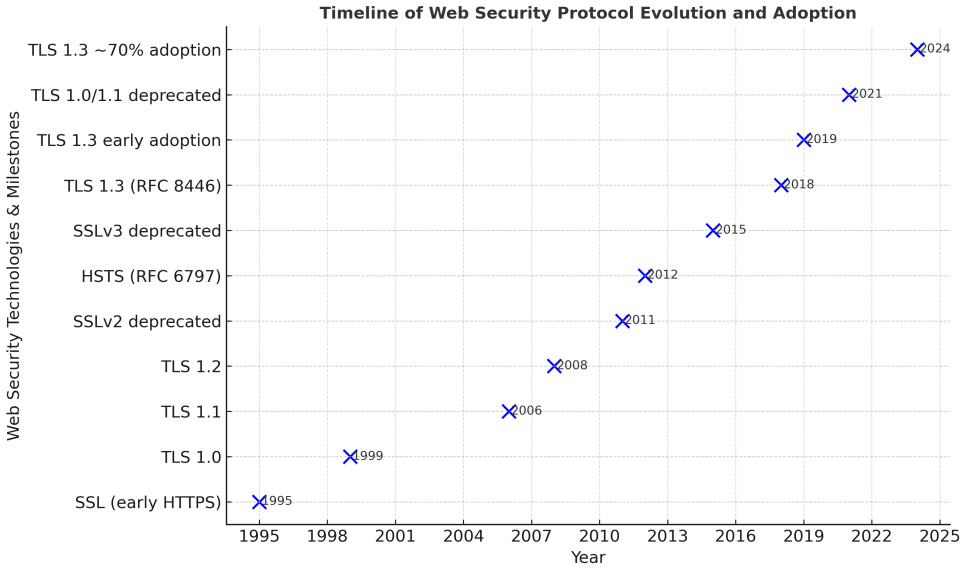


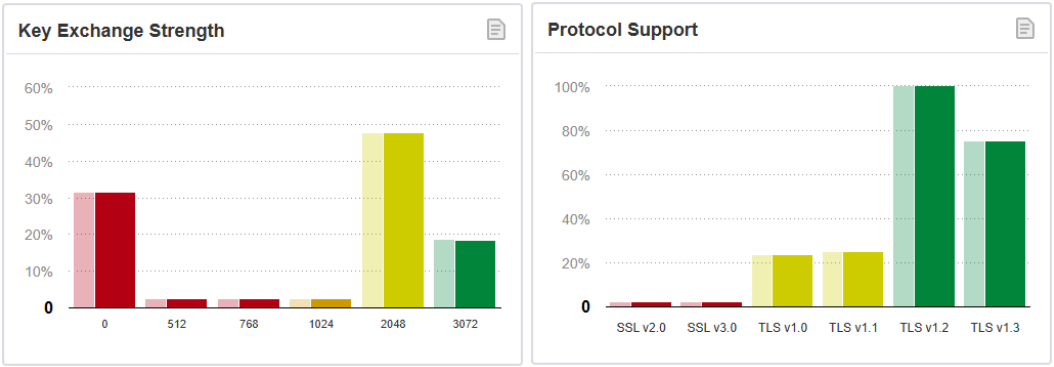
Figure 4. Timeline of web security protocol evolution and adoption, highlighting key milestones such as the introduction and deprecation of SSL/TLS versions, the standardization of HTTP Strict Transport Security (HSTS), and the progressive adoption of TLS 1.3 leading to 70% deployment by 2024.

The introduction of TLS 1.3 in August 2018 represented a major leap forward in both security and efficiency; within one year, major browsers and large service providers enabled it by default, and by 2024 adoption reached approximately seventy percent of surveyed websites, while TLS 1.2 remained almost universally supported [27–29]. Most websites now use TLS 1.2 or newer as shown in Table 2, and a large proportion (about seventy-nine percent) have already moved to TLS 1.3. TLS 1.3 is faster and more secure; for example, when you connect to a modern banking website such as HSBC or Revolut, TLS 1.3 ensures that your data is encrypted with the latest protocols. TLS 1.2 is still widely present (around

ninety-nine percent) and remains secure, but it is gradually being phased out as TLS 1.3 adoption grows as shown in Figure 5.

Table 2. Current SSL/TLS Security Landscape (Qualys SSL Pulse) [30].

Security Feature	% of Top Sites	Why It Matters
TLS 1.3	~79%	The newest and most secure TLS version—faster, stronger encryption, better privacy.
TLS 1.2	~99%	Still secure and widely supported—acts as a fallback when TLS 1.3 is unavailable.
Forward Secrecy (FS)	~89%	Protects past sessions even if the site's private key is compromised later.
HSTS (Strict Transport Security)	~26%	Forces browsers to use HTTPS, preventing downgrade attacks and mixed content.
Strong Keys (≥2048-bit RSA/ECDSA)	~98%	Strong cryptographic keys make breaking encryption computationally infeasible.
HTTP/2 Support	~56%	Enables faster, more efficient, and secure page loading over HTTPS.
Weak Ciphers (RC4, 3DES, etc.)	< 0.1%	Nearly extinct—indicates modern and safe cipher suites.
Certificate Chain Issues	~3%	Misconfigurations can trigger browser security warnings or failed connections.
Legacy SSLv3/SSLv2	<1%	Very rare now—important because these protocols are obsolete and insecure.



(**a**) (**b**)

Figure 5. Analysis of web encryption practices (from Qualys SSL Pulse [30]): (**a**) distribution of key exchange strengths used in secure connections; (**b**) support levels for different SSL/TLS protocol versions. The data highlights the shift toward stronger cryptographic parameters and the increasing adoption of TLS 1.2 and TLS 1.3.

Alongside TLS version evolution, the adoption of Forward Secrecy (FS)—ensuring that session keys cannot be retroactively decrypted—grew substantially during the 2010s as ephemeral Diffie–Hellman and Elliptic Curve Diffie–Hellman (ECDHE) became default in mainstream server configurations, with current deployment estimates approaching ninety percent [28]. Roughly eighty-nine percent of sites implement this, which means even if someone manages to steal a site's private encryption key in the future, they cannot go back and decrypt your previous sessions. For example, when using services like Gmail, your old emails remain protected because FS prevents retrospective decryption. Key lengths have also been strengthened; by the early 2020s, nearly all publicly trusted certificates used

RSA or ECDSA keys of at least 2048 bits, a requirement driven by certificate authority and browser policy enforcement [25].

Despite significant progress, several protective mechanisms remain underused. HTTP Strict Transport Security (HSTS), standardized in 2012, appears on only about one quarter of active domains, in part due to deployment complexity and misconfiguration risk [27]. Although automated issuance platforms like Let's Encrypt have improved certificate chain management, roughly three percent of sites still present trust chain errors [27]. In contrast to foundational improvements such as TLS 1.3 and forward secrecy—which achieved mainstream adoption within five to seven years—HSTS uptake has lagged more than a decade after introduction. HSTS instructs browsers to always use HTTPS, preventing downgrade and interception via unsecured versions of a site. While large platforms (e.g., Facebook, Twitter) enforce HSTS, many smaller e-commerce sites still do not, leaving users exposed.

Nevertheless, some weaknesses persist. Approximately three percent of sites still have certificate chain problems — an issue that can lead to browsers displaying "Not Secure" warnings. For example, if a smaller business incorrectly configures their SSL certificate, users may see trust warnings when visiting their site. A critical determinant for post-quantum readiness is not the nominal cryptographic key or certificate lifetime, which is often long, but the effective migration time—how long it actually takes to replace vulnerable primitives across complex ecosystems. Historical evidence shows that cryptographic transitions are protracted and uneven, especially on the public internet and in enterprise back-ends [31,32]. Legacy and insecure cryptographic technologies have almost disappeared. Fewer than one in a thousand sites still support weak ciphers like RC4, and SSLv3 or SSLv2 are nearly eradicated. This shows great progress in retiring old, vulnerable technologies.

3.1. Timelines in Past Cryptographic Transitions

Past cryptographic transitions provide important lessons for understanding the likely pace and complexity of migration to post-quantum cryptography. Several historical transitions illustrate the persistent operational inertia and long-tail coexistence that arise even when new algorithms are well justified and formally standardised.

First, the transition from 3DES to AES was motivated by both security margin and performance considerations, formalised through NIST's AES competition and standardisation in 2001. Despite clear technical superiority, 3DES remained widely deployed for more than a decade due to legacy hardware, protocol dependencies, and certification cycles, prompting NIST to designate 3DES for eventual deprecation only in 2017 [33,34].

Second, the move from RSA-1024 to RSA-2048 demonstrates similar inertia. Although the cryptographic community recognised already by the mid-2000s that 1024-bit RSA offered only an 80-bit security level, public-key infrastructures continued issuing 1024-bit certificates well into the 2010s. Major browser vendors announced coordinated deprecation only between 2013–2015, and long-lived certificates resulted in extended dual-stack periods where RSA-1024 and RSA-2048 coexisted [35,36].

Third, the SHA-1 to SHA-2 transition highlights the difficulty of retiring a widely embedded primitive. NIST recommended SHA-1's phase-out beginning in 2011, yet SHA-1 persisted across enterprise systems until at least 2017, when browser vendors enforced hard deprecation following published collision attacks [37,38]. Even then, internal enterprise infrastructures, firmware, and archival systems continued to rely on SHA-1 for years due to compatibility and lifecycle constraints.

Across these transitions plotted in Figure 6, several structural patterns emerge: (i) transitions typically require 5–15 years; (ii) dual-algorithm coexistence is unavoidable, as

seen in SHA-1/SHA-2 and RSA-1024/RSA-2048 eras; (iii) ecosystem-wide coordination—particularly among certificate authorities, browser vendors, protocol designers, and hardware suppliers—is often the primary bottleneck; and (iv) certificate validity periods, hardware replacement cycles, and certification requirements significantly slow adoption.

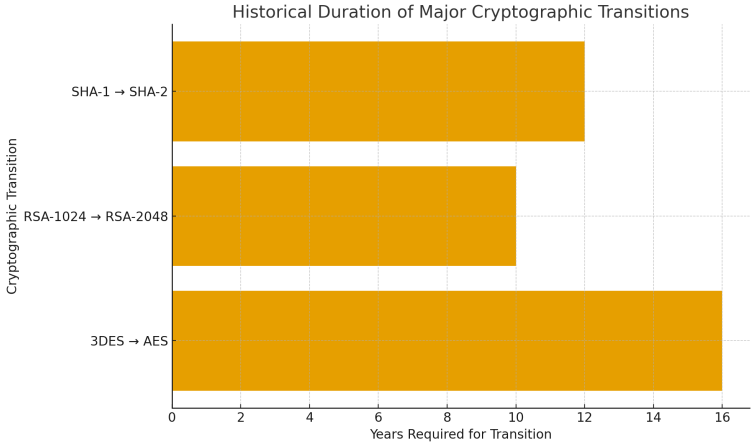


Figure 6. Approximate duration of major historical cryptographic transitions. The transition from 3DES to AES required more than 15 years due to legacy hardware and certification constraints; RSA-1024 to RSA-2048 took roughly a decade, driven by PKI inertia and certificate lifecycles; and the deprecation of SHA-1 required more than 12 years despite well-known weaknesses. These timelines illustrate the structural delays and dual-stack coexistence that inform expectations for post-quantum cryptographic migration.

These historical observations directly inform the PQC migration challenge. The need for hybrid classical–post-quantum deployments mirrors past dual-stack periods; the long lifetime of certificates and embedded systems predicts a multi-year coexistence of classical and PQC schemes; and structural dependencies in financial and payment infrastructures—much deeper than in previous transitions—suggest that PQC migration will face even stronger headwinds. Integrating these lessons strengthens the case that PQC adoption must begin early, coordinated across ecosystems, and supported by crypto-agility engineering from the outset.

3.2. Migration Timelines and Long-Tail Inertia

Financial sector organizations face a uniquely complex set of challenges and interdependencies that slow the migration to post-quantum cryptography (PQC). Unlike isolated IT environments, payment systems, clearing networks, card schemes, and cross-border settlement platforms form tightly coupled ecosystems in which even minor cryptographic changes must remain interoperable across issuers, acquirers, processors, and network operators. Legacy hardware security modules, long-lived certificates, hard-coded protocol assumptions, and vendor-managed components introduce dependencies that cannot be upgraded unilaterally. Additionally, regulatory obligations, certification cycles, and third-party risk-management frameworks require institutions to coordinate changes with external partners and supervisory bodies. These interdependencies create operational bottlenecks that make PQC transition slower and more resource-intensive than in other sectors, reinforcing the need for coordinated and phased migration strategies.

Cryptography migration typically spans decades, and obsolete or vulnerable cryptography is still seen in production environments [39–41]. Transport Layer Security (TLS) provides a salient example. Despite well-documented vulnerabilities in SSLv3/TLS 1.0/1.1 and formal deprecations by major standards bodies and browsers, measurable fractions of internet-facing services continued to support or negotiate obsolete versions years after

deprecation [30,32,42]. TLS 1.3, standardized in 2018 [43], is a prerequisite for several practical post-quantum deployment paths (for example, hybrid key exchanges in TLS 1.3 extensions and KEM-based handshakes), yet global adoption has progressed more slowly than hoped, with substantial long-tail inertia due to legacy stacks, middleboxes, compliance constraints, and operational risk aversion [44–46].

This inertia implies that configurations in the field remain old for long periods: outdated protocol versions, unpatched libraries, and appliances that are difficult to upgrade [32,47]. Consequently, under realistic operational assumptions, industry-wide quantum-safe migration is unlikely to complete quickly. Multiple governmental and industry analyses converge on a five- to ten-year horizon for substantial migration—conditional on early planning, inventory, and coordinated execution—rather than a "lift-and-shift" in a handful of years [48–50].

Since 2025, several cross-sector recommendations have elevated quantum-safe cryptography from a niche planning item to a mainstream cyber risk priority. For instance, major cloud and platform providers have published roadmaps, deployment guidance, and early hybrid deployments to accelerate readiness [51,52]. The Bank for International Settlements (BIS) has addressed systemic and macro-financial dimensions, including potential economic impact in terms of fractions of GDP under scenarios where cryptographic breaks cause widespread operational disruption, as well as a staged roadmap for financial market infrastructures [53,54].

Cost assessments by governments suggest that, for non–national-security systems, the transition costs may amount to roughly one percent of annual IT budgets, depending on asset inventories, cryptographic agility, and integration complexity [55,56]. Such figures underscore that the principal risks are not purely algorithmic but operational: asset discovery, protocol and product dependencies, certification and compliance updates, third-party risk, and the need for extensive testing in hybrid modes before cutting over to fully post-quantum suites [23,49,50]. Although this manuscript does not attempt a full economic model of post-quantum cryptography (PQC) migration, it is important to acknowledge that costs will meaningfully shape institutional transition roadmaps. According to a recent governmental estimate, migrating to PQC for U.S. Federal agencies alone is projected to cost approximately USD $7.1 billion between 2025 and 2035, excluding national-security systems. This estimate reflects expenses for cryptographic asset inventories, replacement or upgrading of legacy systems, vendor coordination, and testing and certification cycles [57]. As discussed in Section 3, real costs vary significantly across institutions due to differences in legacy architectures, regulatory obligations, system criticality, and supply-chain dependencies. For this reason, the "pragmatic playbook" proposed in this paper adopts a cost-agnostic, principle-based structure — crypto-agility, risk-prioritised scoping, hybrid deployment, vendor alignment, and supervisory engagement — designed to help institutions manage and contain migration costs even in the absence of precise sector-wide cost models.

To strengthen the operational guidance for stakeholders, a prescriptive migration framework can be incorporated that defines clear, phase-wise indicators and controls. Such a framework would outline:

- **Initial discovery and assessment KPIs:** cryptographic asset inventory coverage and dependency mapping.
- **Intermediate compliance milestones:** hybrid-PQC enablement, vendor-aligned upgrades, and certification updates aligned with NIST and sector-specific guidelines.
- **Technical risk scores:** quantifying exposure based on algorithm lifetime, data sensitivity, retention periods, and interoperability constraints across payment and financial infrastructures.

Embedding these structured metrics enables financial institutions to prioritise resources, evaluate progress objectively, and coordinate migration activities across complex ecosystems.

In summary, the limiting factor is migration time. Without deliberate, resourced programs—covering inventories, crypto-agility engineering, vendor coordination, and staged hybrid deployments—the sector is unlikely to achieve broad post-quantum coverage within five to ten years. The historical TLS experience, the current state of TLS 1.3 penetration, and recent macro-level risk and cost analyses all point to the same conclusion: plan early, run hybrids, and prioritize critical dependencies first [23,42,43,53].

4. Complexity and Underestimation of PQC Migration

4.1. Beyond Simple Algorithm Replacement

The transition from classical public-key cryptography to post-quantum cryptographic (PQC) systems is frequently underestimated in both complexity and duration. A common misconception is that it is a matter of swapping out algorithms, but in reality it is a multi-decadal, infrastructure-wide transformation that requires coordination across standards bodies, software ecosystems, hardware platforms, and legacy systems.

First, the uncertainty of when sufficiently powerful quantum computers capable of breaking RSA or ECC will actually appear aggravates planning: if organizations believe that quantum computing is still far off, then they may delay action, yet the "harvest now, decrypt later" strategy enables adversaries to capture encrypted data today in anticipation of future decryption capabilities [58,59].

4.2. Organizational and Ecosystem Barriers

Second, the complexity of integrating PQC into existing systems is high: most software, firmware, and network stacks assume fixed key sizes, fixed performance characteristics, and minimal cryptographic overhead, whereas PQC introduces larger keys and ciphertexts, different performance trade-offs, and subtle algorithmic differences that may break assumptions or lead to new vulnerabilities in side channels or protocol compatibility [60–62].

Third, organizational and institutional constraints slow adoption: not all vendors or systems can be upgraded simultaneously, and many systems are mission-critical or embedded, making patching or replacement risky. Indeed, a recent systematic review found that migrations toward PQC across software systems remain largely experimental, with terminological ambiguity, high realization effort, and heterogeneity of approaches persisting across the literature [62].

4.3. Standardization and Tooling Lag

Fourth, the standardization timeline and algorithm selection process itself took many years: the NIST PQC effort began soliciting proposals in 2016 and only finalized the first three FIPS standards (for key encapsulation and signatures) in August 2024, with further algorithmic work continuing [39,63]. Because these standards are relatively recent, the cryptographic libraries, hardware modules, and validation infrastructures (e.g., FIPS 140/CMVP) are still catching up, and many widely used software libraries have partial or preliminary support for PQC even in 2025 [64].

4.4. Realistic Migration Horizons

Another misconception is that the full transition can be completed quickly once standards exist; in practice, NIST and various agencies suggest a phased migration period extending to 2030 or even 2035 for full deprecation of legacy algorithms [59,65,66]. This mismatch in perceived and actual timelines leads many stakeholders to misjudge the urgency and difficulty of migration. Additionally, Mosca's "theorem" warns that one must

budget for the sum of the (unknown) quantum arrival time plus the (lengthy) migration time, because if the migration time exceeds the interval until the threat becomes viable, the window for securing data is lost [2].

In sum, misunderstanding the PQC transition as a short or mechanical upgrade risks severe strategic and operational failures; instead it should be viewed as an epochal overhaul of cryptographic infrastructure, likely spanning one or more decades of phased adoption, testing, fallback, hybrid operation, and gradual decommissioning of legacy systems.

5. Quantum Threats and Regulatory Drivers for Payment Security

5.1. Cryptographic Foundations and Emerging Quantum Risks

The implications for payment security are immediate. Financial institutions and payment processors worldwide rely on public-key cryptography systems such as RSA and elliptic-curve cryptography (ECC) to secure transactions, protect sensitive customer data, and authenticate users. Payment ecosystems widely deploy 2048-bit RSA and standardized elliptic curves (e.g., NIST P-256) in TLS, EMV back-end services, HSM-based key management, tokenization services, and APIs across acquirers, issuers, and processors. The security of these systems rests on the computational hardness of number-theoretic problems, notably integer factorization for RSA and the discrete logarithm problem (over finite fields or elliptic curves) for Diffie–Hellman and ECDSA/ECDH [67,68]. Classically, the best-known algorithms achieve only sub-exponential performance—e.g., the Number Field Sieve for integer factorization runs in expected time

$$\exp\Big((1.923 + o(1))(\log N)^{1/3}(\log\log N)^{2/3}\Big), \tag{2}$$

rendering 2048-bit RSA infeasible to break with current and foreseeable classical resources [65,69].

Quantum computing upends this foundation. Shor's polynomial-time quantum algorithm for integer factorization and discrete logarithms [15] shows that a sufficiently large, fault-tolerant quantum computer can break RSA and ECC in time roughly cubic in the bit-length of the modulus (up to polylogarithmic factors), i.e., $O((\log N)^3)$. This asymptotic separation implies that cryptosystems long considered secure could become tractable to compromise once quantum hardware attains the necessary scale and error-correction overheads.

5.2. Regulatory Pressures and Migration Imperatives

Encouragingly, sector-specific regulations are beginning to address cryptographic resilience, particularly in the payment system. The European Union's Digital Operational Resilience Act (DORA) and the Payment Card Industry Data Security Standard (PCI DSS) both require financial institutions to strengthen how they manage and update cryptographic systems. Although the term "quantum" is sometimes mentioned in introductory notes or guidance, it is often absent from the binding requirements themselves, as these frameworks focus on overall cryptographic governance, lifecycle management, and operational resilience rather than quantum computing alone. For instance, Article 6(4) of DORA stipulates that "financial entities shall include provisions to update or change the cryptographic technology to ensure they remain resilient against cyber threats" [70]. This effectively mandates *cryptographic agility*—the ability to replace or upgrade algorithms and keys when threats evolve—a concept increasingly emphasized in discussions on migrating to quantum-safe cryptography [23,71].

Risk assessments provide an additional lens. Several expert elicitations and industry analyses have estimated non-trivial probabilities that a cryptographically relevant quantum

computer could emerge in the mid-2030s (e.g., on the order of ∼20–30%) [72,73]. If the potential impact is measured in percentage points of global GDP or systemic operational risk, even a 26% tail-risk is difficult to accept from an enterprise risk management perspective. However, it is crucial to decouple the rationale for action from speculative timelines for quantum capability. The near-term driver is compliance and resilience engineering, not predictions about when a particular quantum threshold will be crossed.

In this regard, policy and standards signals have crystallized. Following NIST's selection of post-quantum cryptographic (PQC) algorithms and the publication of FIPS 203 (ML-KEM, based on CRYSTALS-Kyber) and FIPS 204 (ML-DSA, based on CRYSTALS-Dilithium), U.S. federal guidance has set migration milestones via OMB Memorandum M-23-02, with discovery and inventory deadlines starting in 2023 and phased adoption progressing through the early 2030s [74–76]. In parallel, the U.S. National Security Memorandum-10 (NSM-10) mandates a government-wide transition, and NIST SP 800-208/800-56C and migration guidance outline hybrid modes and key establishment transitions [48,77,78]. Internationally, ETSI has produced a rich corpus on quantum-safe migration and crypto-agility patterns, and ISO/IEC JTC 1 SC 27 is standardizing PQC profiles and key management updates [71,79,80].

Practically, for highly regulated sectors such as financial services, the immediate mandate is to implement crypto lifecycle management with agility: maintain cryptographic inventories, assess algorithm/dependency exposure, enable configuration-driven swaps of algorithms and parameters, adopt vetted PQC algorithms and hybrid modes where appropriate, and plan for certificate, protocol, and hardware upgrades across distributed systems [3,23,79]. The relevant timeline is now anchored by compliance and standardization milestones. In effect, the question is no longer whether quantum computers arrive "on time"; it is whether organizations can meet the regulatory and interoperability deadlines that deprecate certain classical public-key schemes and require PQC adoption in the 2030–2035 window [48,74–76].

6. Global Policy and Compliance Landscape

6.1. Emerging Quantum Risk and Regulatory Drivers

Organizations face a narrowing window to prepare for post-quantum cryptography (PQC) due to the confluence of HNDL threats, expected compliance deadlines, and the long lead times required for cryptographic discovery, inventory, remediation, and coordinated migration across distributed systems and vendors. Deferring PQC programs effectively compresses migration timelines, which increases both execution risk and cost. While some quantum-enabled decryption risks may materialize in the mid-2030s, regulatory and supervisory expectations for readiness will emerge earlier—many signals indicate material compliance scrutiny by or before 2030 [3,48,78,81]. Therefore, firms should treat quantum risk as an emerging risk now, not a distant one [49,82,83].

A consistent theme across guidance is that quantum readiness is primarily a cryptographic management challenge rather than a purely quantum technology problem. Core workstreams include: establishing governance, creating and maintaining a comprehensive crypto-asset inventory, prioritizing use cases by business impact and data sensitivity, ensuring vendor and supply-chain alignment, and enabling crypto-agility so that algorithms and parameters can be swapped with minimal disruption [82–85]. Crypto-agility must blend technical and business perspectives, since cryptography ultimately supports business objectives and legal obligations around confidentiality, integrity, availability, and non-repudiation [82,86].

7. Government-Led Post-Quantum Cryptography (PQC) Roadmaps

Government-led strategies in Canada, the European Union (EU), the United States (US), the United Kingdom (UK), Australia, and several Asian jurisdictions are shaping the global transition to post-quantum cryptography (PQC) listed in Figure 7. These initiatives provide timelines, set expectations for industry and government systems, and influence both regulatory frameworks and practical implementation. Although the approaches differ in prescriptiveness and pace, they collectively indicate an accelerating shift away from classical public-key cryptography.

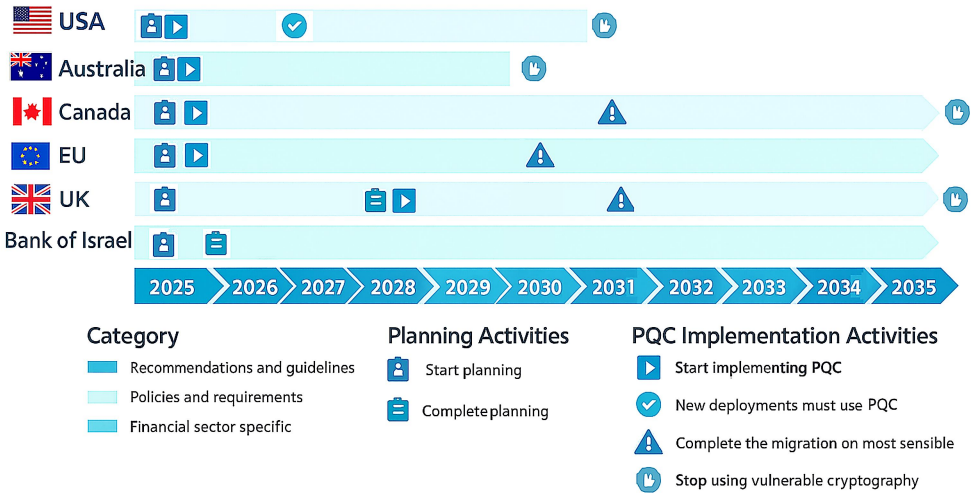


Figure 7. Synthesis of government-led post-quantum cryptography (PQC) roadmaps and transition milestones. The timeline consolidates published guidance from NIST's PQC standardization and NSA's CNSA 2.0 deadlines [21], CSE (Canada) [87], ENISA and EU coordinated implementation roadmaps [3], and national guidance from NCSC (UK) [18], ASD (Australia) [88], and other authorities cited in Section 7. The figure provides a unified visual summary derived from these cited sources.

In the United States, the combination of policy direction and technical standardization has driven early momentum. The National Security Agency (NSA) released the *Commercial National Security Algorithm Suite 2.0* (CNSA 2.0) in 2022, providing clear migration milestones and compliance deadlines [89]. By publicly sharing its internal schedule, the U.S. government gave national security system administrators, IT vendors, and service providers a structured roadmap and increased transparency, allowing product plans to align with PQC requirements across 2022–2024. The National Institute of Standards and Technology (NIST) subsequently announced the deprecation of RSA-2048 by 2030 and the prohibition of all classical public-key cryptography by 2035 [39]. Crucially, these deadlines are decoupled from predictions about the arrival of cryptographically relevant quantum computers (CRQCs), signaling the need for proactive transition in sensitive sectors such as finance and critical infrastructure. NIST has finalized the first PQC standards, including *FIPS 203 (ML-KEM)* and *FIPS 204 (ML-DSA)*, with migration guidance through NISTIR 8425 and the SP series [90]. Policy momentum has been reinforced by the White House Office of Science and Technology Policy (OSTP), which directed federal PQC readiness, and by the Cybersecurity and Infrastructure Security Agency (CISA), which published critical-infrastructure transition roadmaps [91,92]. These combined actions have triggered rapid industry uptake: major browsers such as Chrome and Edge, cryptographic libraries like OpenSSL and BoringSSL, and large content delivery networks (CDNs) including Cloudflare, AWS, and Akamai introduced support for hybrid PQC key exchange during 2024–2025 [93–99].

Canada has taken a similarly structured but nationally focused approach. The Communications Security Establishment (CSE) published a PQC roadmap emphasizing the

need to conduct cryptographic inventories, prioritize vulnerable systems, and plan migration sequencing across government and critical sectors [87]. This framework aims to prepare both public and private infrastructures for the adoption of PQC technologies while maintaining alignment with international cryptographic standards.

Within the European Union, PQC transition is advancing through coordinated policy efforts and sectoral guidance. The European Commission released *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, aiming to harmonize member states' strategies [100]. This initiative was supported by a joint statement from agencies representing 18 EU countries [101]. Complementing this work, the European Union Agency for Cybersecurity (ENISA) has published sector-agnostic migration recommendations, and the Eurosystem has set expectations for financial market infrastructures (FMIs) [3,102]. PQC considerations have also been integrated into the transposition of the *NIS2 Directive* and related supervisory frameworks [103]. Although the EU encourages prioritization of high-risk use cases by 2030–2031 and aims for widespread adoption by the mid-2030s, its guidance remains primarily advisory, giving member states and sectors some flexibility in how they adapt to emerging risks.

The United Kingdom's National Cyber Security Centre (NCSC) has issued guidance to encourage near-term planning and crypto-agility across critical sectors. Current recommendations advise organizations to prepare through the late 2020s, with migration of essential systems to PQC technologies suggested after 2028 [104]. While this approach offers clear strategic direction, it remains non-mandatory and could compress migration timelines for organizations facing stricter deadlines set elsewhere.

Australia stands out for its comparatively prescriptive approach. The Australian Signals Directorate (ASD) recommends avoiding reliance on classical public-key cryptography beyond 2030 in government systems [88], while the Australian Cyber Security Centre (ACSC) has issued mandatory cryptographic transition guidelines for both government and critical infrastructure operators [105]. These measures create one of the most clearly defined national migration horizons and send a strong signal to industries that rely on long-term cryptographic planning.

In Asia, regulatory action is emerging, particularly within the financial sector. The Monetary Authority of Singapore (MAS) issued an advisory in 2024 requiring financial institutions to assess and mitigate quantum-related cybersecurity risks [106]. The Bank of Israel (BoI) has gone further, mandating that banks and licensed payment service providers submit quantum transition preparedness plans by early 2026 [107,108]. This early regulatory posture is among the most stringent globally and may influence peer financial regulators in the region and beyond.

Across these jurisdictions, there is a growing but imperfect alignment around key milestones. Many authorities, including NIST and ENISA, identify 2030–2031 as the critical period to complete the transition for high-risk use cases and anticipate that by around 2035 most environments should have moved away from classical public-key cryptography [3,90,92,102]. Nonetheless, divergent timelines create practical uncertainty for multinational institutions. For example, the UK allows critical system migration to begin after 2028 [49], whereas Australia expects full avoidance of classical public-key algorithms by 2030 [88]. This misalignment complicates decisions about algorithm selection, hybrid versus pure PQC deployment, and the sequencing of compliance efforts across multiple legal frameworks [109].

Meanwhile, market momentum is reinforcing the policy direction. Major browsers and large-scale internet infrastructure providers have already introduced hybrid PQC key exchange for TLS 1.3, beginning in late 2024 [93–95,98,99]. Widely used cryptographic libraries, including OpenSSL and BoringSSL, now provide default PQC support [96,97].

Independent internet measurements confirm that a growing share of global web traffic is already being negotiated using hybrid post-quantum key exchanges [110]. This early adoption underscores that the transition is not merely theoretical but actively underway, further aligning industry with the forward-looking roadmaps of national and regional authorities.

7.1. Sector Guidance and Ecosystem Coordination

Sector initiatives underscore this shift from awareness to execution. The Institute of International Finance (IIF) and other sector bodies have convened multi-day programs on quantum safety, reflecting growing board- and CRO-level attention [111]. Financial-sector collaboration forums (e.g., regional quantum financial working groups, FS-ISAC workstreams) are sharing migration practices, timelines, and definitions—such as practical definitions of crypto-agility that integrate business impact with technical feasibility—to avoid duplicated efforts and accelerate alignment [112,113]. Recommendations from these bodies broadly align: make PQC a strategic priority; identify and coordinate dependencies early; prefer guidance and sector alignment over premature prescriptive regulation; and frame the transition as a program of continuous cryptographic management improvement, not a one-off project [81,83–85].

8. From Policy to Practice: Migration Priorities

8.1. Near-Term Measures to Reduce Long-Tail Exposure

Risk triage also affects near-term prioritization. While a headline "thesis of fire" in 2025 specifically due to the lack of PQC is unlikely, data of long-term sensitivity is already at risk from harvesting by capable adversaries; ransomware and classical cyber threats will continue to dominate incident reports meanwhile [114,115]. This dichotomy often diverts resources toward urgent threats at the expense of strategic PQC programs, resulting in experts lacking organizational support to drive meaningful action. Clear executive sponsorship, cross-functional governance, and strong external collaboration can counteract this tendency and ensure that PQC migration proceeds in parallel with other cyber priorities [48,83,112].

In short, the capability to act is a present requirement even if the most severe quantum decryption impacts arrive later. Treating quantum risk as an emerging risk now, institutionalizing crypto-agility, and participating in sector alignment efforts are foundational to reducing cost, risk, and disruption as PQC standards and implementations are operationalized [78,83,116]. For instance, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has addressed concrete payment-system use cases in recent sector guidance, highlighting key considerations when preparing for major transitions in payment card services [117,118]. Beyond FS-ISAC, several bodies have issued targeted guidance for payments modernization and adjacent risk domains, including SWIFT on ISO 20022 adoption and best practices, CPMI on cross-border migration lessons, and the ECB on Eurosystem implementation [119–121]. There has also been a proliferation of recommendations and position papers from global and regional standard-setters on operational resilience, third-party risk, and cyber transitions affecting payments (e.g., FSB, EBA on DORA implementation, UK authorities on operational resilience) [109,122,123].

However, as noted by a Deputy Governor of Banca d'Italia in remarks delivered in Rome in September 2024, despite growing awareness, a clear unified action plan to ensure a smooth and secure transition remains lacking [124]. Some supervisory expectations are becoming more concrete. For example, the Bank of Israel moved beyond non-binding recommendations and required supervised institutions to submit their transition plans, a model other authorities may adopt [107]. In parallel, high-level G7 finance track com-

muniqués have referenced timelines and priority workstreams published this year, yet fragmentation persists across sectors and jurisdictions [125,126].

In domains tightly coupled to payment security, additional transition agendas underscore the breadth of change facing the ecosystem: NIST and ENISA on migration to post-quantum cryptography (PQC), Eurosystem expectations on cryptographic agility for FMIs, and PCI SSC's evolving standards for the payment card environment [3,90,102,127]. Major market infrastructures and central banks have also documented ISO 20022 migration outcomes and forward plans (e.g., Bank of England CHAPS) and real-time gross settlement renewals (e.g., T2/T2S consolidation), which provide practical transition playbooks and risk mitigants relevant across jurisdictions [121,128]. Together, these sources show growing momentum in guidance and requirements, but also illustrate the need for coordinated, end-to-end roadmaps to avoid fragmented implementation and residual operational risk [109,120,125].

8.2. Hybrid Cryptography and the Internet Edge

Reality on the internet edge has advanced quickly: major browsers, TLS libraries, and CDNs have enabled hybrid KEM key agreement at scale, meaning much of the world's web traffic is already protected, at least for confidentiality during transit, by a combination of classical elliptic-curve cryptography and post-quantum algorithms [93,96,98].

This discussion synthesizes cross-national roadmaps and sector-specific expectations, contrasts binding requirements and voluntary guidance, and highlights the operationalization gap between policy timelines and live deployment. It argues that the financial sector can mitigate cross-border misalignment through a principle-based adoption playbook built on cryptographic agility, risk-prioritized scoping, independent verification and testing, and supply-chain alignment.

9. Financial-Sector Modernization and Dependencies

9.1. Lessons from Payment System Migrations

The financial sector's crypto transition is intertwined with existing modernization programmes. ISO 20022 adoption across RTGS and correspondent networks has already stressed change-management processes and vendor alignment. Lessons from CPMI on cross-border ISO 20022 migration and ECB's T2/T2S consolidation underscore the importance of multi-year planning, industry-wide testing, and cutover risk governance [120,121]. These experiences translate directly into PQC migration, where cryptographic upgrades must be coordinated across payment rails, market data feeds, custodial services, and cross-border gateways. The FSB's cross-border payments agenda and work on operational resilience provide governance scaffolding—defining roles for standard-setters, supervisors, and industry associations to harmonize minimum expectations and testing regimes [109,126].

9.2. Payment Standards and Supervisory Signals

Security standards in the payment card ecosystem (e.g., PCI SSC) continue to evolve, and while PCI DSS primarily governs cardholder data protection and controls rather than algorithmic mandates, PCI-aligned guidance will influence implementation constraints and validation practices for PQC adoption in payment flows and merchant ecosystems [127]. Similarly, national cybersecurity authorities (ENISA, NCSC, ASD) provide reference migration patterns that, when contextualized for financial services, offer a stable base for supervisory dialogue and auditability [3,88,129]. For FMIs, the Eurosystem's expectation that operators institutionalize cryptographic agility and plan PQC preparedness is a critical

signal: it elevates crypto lifecycle management from engineering practice to governance mandate [102].

The operational reality has, in some respects, outpaced policy. Beginning in late 2024 and continuing through 2025, major browsers initiated support for hybrid key agreement in TLS 1.3, typically combining X25519 with the NIST-selected Kyber KEM (ML-KEM) [93–95]. OpenSSL and BoringSSL integrated hybrid KEM mechanisms, enabling server-side adoption at scale and forming the substrate for cloud providers and CDNs to offer hybrid PQC as default or opt-in [96,97]. AWS CloudFront and Akamai documented production rollouts, signaling that high-volume web traffic now benefits from hybrid confidentiality protections against HNDL risks [98,99]. Independent measurements report significant penetration of hybrid PQC across top websites, demonstrating rapid diffusion into the broader ecosystem [110].

For the financial sector, early adopters include banks and payment brands enabling hybrid PQC on public web properties and APIs—both as a signal of readiness and as a risk-mitigating measure for high-value, confidentiality-sensitive sessions. Openbank (a Santander brand) publicly noted support for hybrid PQC in customer web sessions, pairing elliptic-curve methods with a quantum-resistant KEM to ensure confidentiality remains robust even under future quantum adversaries [130]. These deployments, while primarily focused on transport confidentiality, create momentum and practical learning for deeper migrations within internal messaging, interbank connectivity, and workload-to-workload cryptography.

9.3. Dependencies

The timeline for PQC migration must account for a range of interconnected dependencies and anticipate how to influence external stakeholders to achieve coherent sector-wide change. At the ecosystem level, it is essential to coordinate transitions across all critical interoperability platforms in the financial sector so that payments networks, markets and exchanges, central banks, clearinghouses, and other infrastructures advance in step and avoid fragmentation or systemic risk. Technology and service providers represent another key dependency, as many financial institutions also serve as vendors to others; migration planning should therefore include strategies to influence vendor roadmaps, ensure PQC readiness in supplied products and services, and embed post-quantum requirements into procurement and contractual obligations. Beyond vendors, dependencies extend to standards development: firms must align with the evolving roadmaps of influential bodies such as the Internet Engineering Task Force (IETF) [45] and industry groups like the X9 Financial PKI [131], which are shaping updates to protocols (e.g., TLS, IPsec, SSH), certificate formats and signature algorithms, and interim constructs like hybrid certificates that enable controlled, phased adoption. Finally, success depends on robust governance and regulatory alignment; institutions need mechanisms to comply with current and emerging cryptography management or quantum-safety regulations while maintaining clear communication of milestones and expectations to customers, partners, and supervisors to support trust and auditability throughout the transition.

10. A Pragmatic Playbook for Cross-Border Transition

The analysis in earlier sections showed that post-quantum migration in finance is shaped by three persistent forces: (i) legacy technical architectures across FMIs and payment infrastructures, (ii) jurisdictional divergence in regulatory expectations; as reflected in NIST, ENISA, and ECB migration guidance [3,90,102]; and (iii) vendor and interoperability dependencies documented in cross-border policy work [109]. To convert these findings into actionable guidance, we define a **pragmatic, principle-based playbook** as a structured

decision framework that translates regulatory, technical, and operational insights into practical, repeatable migration actions for multinational financial institutions (shown in Figure 8). Rather than reproducing public guidelines, the playbook below synthesises the evidence developed in this paper into six coordinated principles, each supported by concrete operational steps.

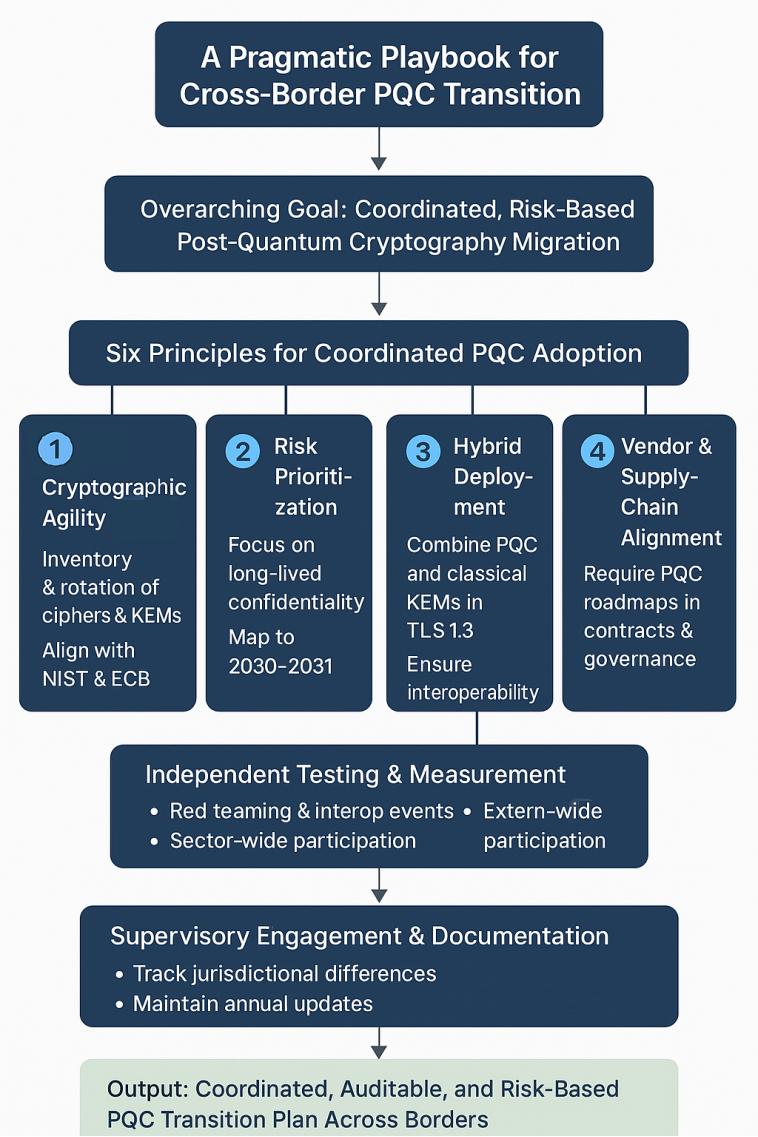


Figure 8. A pragmatic playbook for cross-border post-quantum cryptography (PQC) transition. The framework outlines a coordinated, risk-based migration strategy, guided by six principles — cryptographic agility, risk prioritization, hybrid deployment, vendor and supply-chain alignment, independent testing and measurement, and supervisory engagement — to enable secure, auditable, and interoperable PQC adoption across jurisdictions.

10.1. Principles for Coordinated PQC Adoption

Principle 1 — Crypto-Agility as Foundational Engineering and Governance.

Historical cryptographic transitions—including the depreciation of SHA-1, RC4, and TLS 1.0—demonstrated that institutions lacking crypto-agility required multi-year remediation cycles. Contemporary supervisory expectations, such as ECB guidance for FMIs and NIST migration strategy [90,102], similarly identify crypto-agility as the foundation for timely PQC adoption.

- Define upgrade-safe interfaces between business logic and cryptographic implementations.
- Decouple cryptographic libraries from application code using abstraction layers.
- Implement protocol-level algorithm negotiation (e.g., flexible KEM identifiers in TLS 1.3).
- Maintain centralised, continuously updated inventories of keys, ciphers, and KEM deployments.

Principle 2 — Risk-Prioritised Scoping for Financial Stability and HNDL Mitigation.

Analysis in preceding sections showed that confidentiality lifetimes in finance are unevenly distributed: long-lived datasets, interbank links, and high-value messaging interfaces face the highest "harvest-now, decrypt-later" exposure. Cybersecurity agencies emphasise early protection of these classes, including CISA and ENISA migration priorities for 2030–2031 [3,92].

- Classify systems and datasets by confidentiality lifetime, systemic importance, and cross-border visibility.
- Prioritise long-lived data stores, high-value messaging flows, and authentication/signature systems.
- Map prioritised assets to 2030–2031 transition milestones [3,90,92].
- Place these systems in early PQC pilots or hybrid-based transitional deployments.

Principle 3 — Hybrid Deployment Patterns to Manage Interoperability Constraints.

The technical evidence presented earlier—including PQC-enabled TLS 1.3 rollouts in Chrome, OpenSSL, and major CDNs [93,96,98]—shows hybrid KEM as the only widely interoperable near-term migration pathway. Hybridisation therefore acts as a transitional control that preserves internet-scale compatibility while enabling PQC adoption.

- Deploy hybrid KEM in TLS 1.3 where supported (OpenSSL, BoringSSL, CloudFront).
- Measure latency, handshake success rates, and throughput impacts across payment, messaging, and API systems.
- Use hybrid signatures internally where backward compatibility requirements persist.
- Sequence deployments to align with the readiness of third-party infrastructure, vendors, and counterparties.

Principle 4 — Vendor and Supply-Chain Alignment Across Borders.

Earlier regulatory analyses, including cross-border financial sector studies [109], emphasise that PQC readiness depends strongly on vendor timelines, particularly HSMs, TLS terminators, API gateways, and core-banking platforms. Without coordination, such dependencies create systematic misalignments across jurisdictions.

- Request PQC enablement roadmaps from HSM, network security, banking platform, and API vendors.
- Embed crypto-agility and PQC milestones into procurement cycles and contractual acceptance criteria.
- Require demonstrable PQC capability (e.g., hybrid KEM support) for new deployments beyond 2025.
- Conduct joint pilot migrations with critical third-party service providers.

Principle 5 — Independent Testing, Measurement, and Sector-Wide Validation.

Interoperability risks identified in earlier sections cannot be mitigated by institutions acting alone. Independent validation mechanisms—such as interoperability events ref-

erenced by CPMI and FSB [120,126]—enable harmonised testing across infrastructures, vendors, and jurisdictions.

- Participate in PQC interoperability and conformance testing exercises hosted by standards bodies or supervisors.
- Use external scanning, red-teaming, and penetration testing to verify hybrid and transitional deployments.
- Benchmark performance impacts (latency, CPU cost, handshake reliability) across representative workloads.
- Share anonymised test and pilot results with sector-wide working groups to support ecosystem alignment.

Principle 6 — Proactive Supervisory Engagement and Traceable Decision-Making.

Divergent regulatory timelines (e.g., Bank of Israel vs. UK expectations [107,129]) amplify uncertainty for multinational institutions. As shown in earlier sections, supervisory engagement is essential to coordinate sequencing, validate transitional approaches, and justify risk-based prioritisation.

- Document and justify migration sequencing when regulatory requirements differ across jurisdictions.
- Maintain audit-ready migration plans with at least annual refresh cycles.
- Provide evidence that interim controls (e.g., hybrid modes) reduce HNDL exposure.
- Establish early, recurring communication channels with supervisors to validate approaches and timelines.

This playbook synthesises the technical, operational, and policy analysis developed throughout this paper into six coherent principles and actionable steps. It provides institutions with a defensible, audit-ready migration structure while accelerating the security benefits achievable through hybrid deployments, prioritised migrations, and coordinated vendor alignment.

10.2. Coalescing on Migration Timelines

Despite misalignments in form and specificity, a consensus contour is emerging: authorities increasingly identify 2030–2031 as the critical milestone for transitioning high-risk use cases, with a broader horizon near 2035 for full migration [3,90,92]. This aligns with observed timelines for standardisation (FIPS finalisation), vendor enablement (libraries, HSMs, network devices), and internet-scale pilots [93,96,98]. These migration contours reinforce the necessity of the structured principles above: without coordinated sequencing, cross-border inconsistencies will compound rather than diminish.

11. Discussion

In summary, the transition to post-quantum cryptography (PQC) is no longer hypothetical; it is underway today [78,116]. Nevertheless, awareness and action remain uneven across sectors. Many organizations still assume that migration can be deferred, as though the "race" to quantum safety has yet to begin, shown in Figure 9. In reality, the starting signal has already sounded: major standards bodies have finalized the first PQC algorithms, and leading vendors and infrastructures have begun adopting hybrid classical–post-quantum mechanisms [93,116].

A critical risk in the current landscape is the danger of a *dual-speed transition*. Early adopters that migrate to PQC ahead of the broader ecosystem will still need to maintain classical cryptographic capabilities to interoperate with slower movers. This backward compatibility can expand the attack surface and extend the lifetime of vulnerable primitives [83,115]. Avoiding a fragmented transition requires cross-sector alignment so that

critical systems reach cryptographic parity rather than leaving laggards connected to quantum-safe networks.

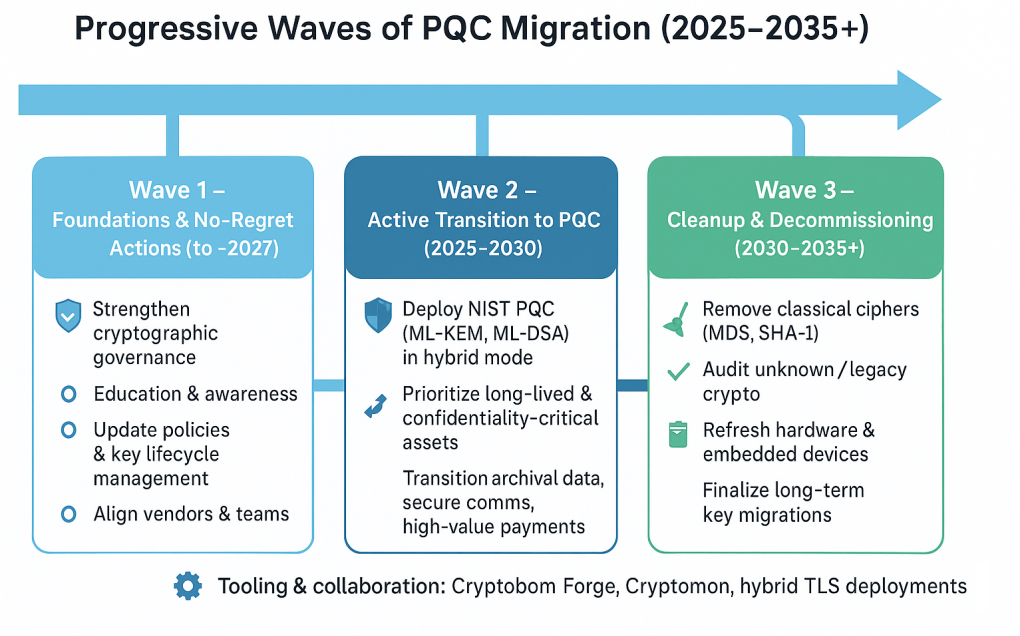


Figure 9. Progressive waves of post-quantum cryptography (PQC) migration from 2025 to 2035 and beyond. The roadmap outlines three phases: Wave 1—establishing governance, awareness, and foundational policy updates; Wave 2—active transition to NIST PQC algorithms in hybrid deployments, prioritizing long-lived and confidentiality-critical assets; and Wave 3—decommissioning legacy cryptography, auditing unknown systems, and completing long-term key migrations.

11.1. Recommended Migration Phases

Consistent with emerging guidance [82,85,115], migration to PQC can be conceptualized in three progressive waves:

Wave 1—Foundations and No-Regret Actions (to ~2027).

This phase focuses on strengthening cryptographic governance and preparing the enterprise for change. Organizations should establish education and awareness programs, formalize governance models, and build comprehensive cryptographic inventories. It is often more important to discover and classify cryptographic *use cases* than merely to list keys or algorithms. Key actions include updating cryptographic policies, consolidating diverse signing practices, improving key lifecycle management, and aligning internal teams and vendors [82,85]. No post-quantum primitives need be deployed here; the emphasis is on gaining control and visibility.

Wave 2—Active Transition to PQC (2025–2030).

Organizations begin implementing NIST-standardized PQC algorithms (e.g., ML-KEM, ML-DSA) [116], typically in hybrid mode alongside established elliptic-curve or RSA methods for interoperability. During this period, the most confidentiality-critical and long-lived assets should transition first, including sensitive archival data, secure communications, and interbank or high-value payment links. By 2030, many infrastructures are expected to default to quantum-resistant algorithms.

Wave 3—Cleanup and Decommissioning of Classical Cryptography (2030–2035+).

Once PQC is broadly deployed and trusted, the goal is to eliminate residual dependencies on classical algorithms and address complex edge cases (e.g., global hardware

refresh of point-of-sale terminals, replacement of long-lived embedded devices). This phase involves auditing for unknown or legacy cryptographic uses, removing obsolete ciphers (e.g., MD5, SHA-1), and finalizing key migration projects that require extended hardware and vendor coordination.

Practical readiness also depends on improved tooling and collaboration. Open-source cryptographic discovery tools such as *Cryptobomb Forge* (co-developed with Microsoft and GitHub) and *Cryptomon* can help identify algorithmic usage in codebases and network flows, supporting cryptographic quality assessment in development pipelines and runtime monitoring. Similarly, early deployments in Transport Layer Security (TLS) demonstrate how hybrid key exchange can be adopted using existing compliance and vulnerability management frameworks, without major infrastructure replacement.

Additional near-term enablers include post-quantum signatures with long-term validation timestamps and blockchain notarization of documents to provide quantum-safe proof of existence even before full PQC signature standards mature [83,115]. For many organizations, a pragmatic first use case is enabling confidentiality protection on public web endpoints: major browsers and TLS libraries already support hybrid PQC handshakes [93,96].

The transition to PQC is a current regulatory and operational imperative, independent of exactly when large-scale quantum computers arrive [78,83]. Enterprises should immediately strengthen cryptographic management and governance, inventory use cases and dependencies, and start controlled PQC adoption in well-supported areas (e.g., web confidentiality). At the same time, industry-wide and cross-sector coordination is essential to avoid a fragmented, dual-speed migration that would prolong vulnerability and raise systemic risk.

12. Conclusions

This paper reframes quantum readiness for finance as an immediate resilience and compliance priority rather than a distant technical challenge. We have shown that secure migration to post-quantum cryptography is complex and protracted, demanding early governance, discovery of cryptographic assets, and sustained cross-sector coordination. By learning from past transitions, adopting hybrid deployment patterns, and aligning with emerging regulatory milestones, financial institutions can reduce systemic risk and avoid dual-speed adoption traps. A pragmatic, principle-based playbook, which combines cryptographic agility, vendor alignment, independent testing, and supervisory engagement, offers a clear path to protect long-lived confidentiality and transaction integrity. As standards mature and hybrid implementations become mainstream, the opportunity to act decisively is now; delaying action will compress migration timelines, increase cost, and expose critical payment and settlement infrastructures to harvest-now-decrypt-later threats. Achieving quantum safety requires not only technical change but also strategic leadership and international collaboration to ensure that the financial system evolves in step with global cryptographic policy and technological innovation.

Author Contributions: Conceptualization, C.K.; methodology, C.K.; software, C.K.; validation, C.K.; formal analysis, C.K.; investigation, C.K.; resources, C.K.; data curation, C.K.; writing—original draft preparation, C.K.; writing—review and editing, C.K.; visualization, P.L.T.; supervision, S.M.; project administration, L.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F.G.; Buell, D.A.; et al. Quantum Supremacy Using a Programmable Superconducting Processor. *Nature* **2019**, *574*, 505–510.
2. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41.
3. European Union Agency for Cybersecurity (ENISA). Post-Quantum Cryptography: Current State and Quantum Mitigation. ENISA Report, 2022. Available online: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation (accessed on 2 October 2025).
4. National Institute of Standards and Technology (NIST). NISTIR 8413: Migration to Post-Quantum Cryptography—Guidance on Discovery and Remediation of Cryptographic Systems. NIST Interagency/Internal Report, 2024. Available online: https://csrc.nist.gov (accessed on 2 October 2025).
5. ETSI. Quantum-Safe Cryptography and Security (ETSI TR 103 619). ETSI Technical Report, 2020. Available online: https://www.etsi.org (accessed on 2 October 2025).
6. Dixit, S. The Impact of Quantum Supremacy on Cryptography: Implications for Secure Financial Transactions. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2020**, *6*, 611–637. https://doi.org/10.32628/cseit2064141.
7. Shaikh, F.; Sangole, M.; Pareek, V.; Patil, P.; Takale, D.; Gupta, S. Quantum Cryptographic Algorithms for Securing Financial Transactions. *Comput. Fraud Secur.* **2024**. https://doi.org/10.52710/cfs.32.
8. Joseph, D.; Misoczki, R.; Manzano, M.; Tricot, J.; Pinuaga, F.; Lacombe, O.; Leichenauer, S.; Hidary, J.; Venables, P.; Hansen, R. Transitioning organizations to post-quantum cryptography. *Nature* **2022**, *605*, 237–243. https://doi.org/10.1038/s41586-022-04623-2.
9. Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-Quantum Lattice-Based Cryptography Implementations. *ACM Comput. Surv.* **2019**, *51*, 1–41. https://doi.org/10.1145/3292548.
10. Li, S.; Chen, Y.; Chen, L.; Liao, J.; Kuang, C.; Li, K.; Liang, W.; Xiong, N. Post-Quantum Security: Opportunities and Challenges. *Sensors* **2023**, *23*, 8744. https://doi.org/10.3390/s23218744.
11. Xie, J.; Zhao, W.; Lee, H.; Roy, D.; Zhang, X. Hardware Circuits and Systems Design for Post-Quantum Cryptography—A Tutorial Brief. *IEEE Trans. Circuits Syst. II Express Briefs* **2024**, *71*, 1670–1676. https://doi.org/10.1109/TCSII.2024.3357836.
12. Sezer, B.; Akleylek, S.; Nuriyev, U. PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-Based Systems: A Systematization of Knowledge. *IEEE Access* **2025**, *13*, 41382–41405. https://doi.org/10.1109/ACCESS.2025.3545943.
13. Fernández-Caramés, T.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985.
14. Preethi, P.; Ulla, M.; Sapna, R.; Mohan, K. Implementing Post-Quantum Cryptography Algorithm in Blockchain. In *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*; IEEE: Karnataka, India, 2023; pp. 1–7. Available online: https://doi.org/10.1109/ICCAMS60113.2023.10525729 (accessed on 2 October 2025).
15. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Siam Rev.* **1996**, *41*, 303–332.
16. National Institute of Standards and Technology. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*; NIST: Gaithersburg, MD, USA, 2024. Available online: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (accessed on 2 October 2025).
17. Bernstein, D.J.; Buchmann, J.; Dahmen, E. Post-quantum cryptography. *Commun. ACM* **2023**, *66*, 30–32.
18. UK National Cyber Security Centre (NCSC) and National Physical Laboratory, with Partners (Including BSI, ANSSI). Next Steps in Quantum-Safe Cryptography. Whitepaper, 2022. Available online: https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography-guidance (accessed on 2 October 2025).
19. Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; (NISTIR 8105); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
20. NIST Computer Security Resource Center (CSRC). Post-Quantum Cryptography Standardization (Project Hub; Includes FIPS 203/204/205 and Ongoing Updates). Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (accessed on 2 October 2025).
21. U.S. National Security Agency (NSA). CNSA 2.0: Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ. Guidance on Migration Urgency, Timelines, and Interim Protections, 2022. Available online: https://media.defense.gov/2022/Sep/07/2003071687/-1/-1/0/CSA_CNSA_2.0_FACT_SHEET.PDF (accessed on 2 October 2025).
22. KPMG; Bundesamt für Sicherheit in der Informationstechnik (BSI). Quantum-Safe Cryptography: Readiness of German Enterprises. Survey Report, 2022. Available online: https://home.kpmg/de/en/home/insights/2022/11/quantum-safe-cryptography-study.html (accessed on 27 September 2025).
23. National Institute of Standards and Technology (NIST). Migration to Post-Quantum Cryptography: Guidance for Organizations. NIST (Landing and Working Guidance), 2024. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography (accessed on 27 September 2025).

24. FeistyDuck. SSL/TLS and PKI History. Available online: https://www.feistyduck.com/ssl-tls-and-pki-history/ (accessed on 3 October 2025).
25. The SSL Store. Celebrating 30 Years of SSL and TLS Versions. Available online: https://www.thesslstore.com/blog/ssl-and-tls-versions-celebrating-30-years-of-history/ (accessed on 3 October 2025).
26. Smitterhane, M. How TLS Was Born to Secure the Modern Internet Age. Available online: https://dev.to/smitterhane/how-tls-was-born-to-secure-modern-age-internet-45jb (accessed on 3 October 2025).
27. SSL Dragon. SSL Statistics and TLS Trends. Available online: https://www.ssldragon.com/blog/ssl-stats/ (accessed on 3 October 2025).
28. IETF. TLS 1.3 Adoption Update. Available online: https://www.ietf.org/blog/tls13-adoption/ (accessed on 3 October 2025).
29. Catchpoint. TLS 1.2 vs. TLS 1.3 Adoption Statistics. Available online: https://www.catchpoint.com/http2-vs-http3/tls1-2-vs-1-3 (accessed on 3 October 2025).
30. SSL Labs. SSL Pulse. Available online: https://www.ssllabs.com/ssl-pulse/ (accessed on 5 October 2025).
31. Anderson, R. *Security Engineering*, 2nd ed.; Wiley: New York, NY, USA, 2008; pp. 154–196.
32. Holz, R.; Braun, L.; Kammenhuber, N.; Carle, G. The SSL Landscape: A Thorough Analysis of the X.509 PKI Using Active and Passive Measurements. In *ICM'11: Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference (IMC), Berlin, Germany, 2–4 November 2011*; Association for Computing Machinery: New York, NY, USA, 2011; pp. 427–444.
33. NIST. *Recommendation for Key Management, Part 1: General (SP 800-57)*; NIST Special Publication; NIST: Gaithersburg, DC, USA, 2016.
34. Moore, J. The 3DES Deprecation Timeline and Its Impact. *Cryptogr. Eng. Rev.* **2017**.
35. Lenstra, A.; Verheul, E. Selecting Cryptographic Key Sizes. *J. Cryptol.* **2001**, *14*, 255–293.
36. Mozilla Security Team. *Deprecation of 1024-bit RSA Certificates*; Mozilla Security Bulletin; Mozilla Security Team: San Francisco, CA, USA, 2015.
37. NIST. *Announcing Approval of SHA-2 Family of Hash Functions. Federal Register*; NIST: Gaithersburg, DC, USA, 2011.
38. Stevens, M.; Bursztein, E.; Karpman, P.; Albertini, A.; Markov, Y. *The First Collision for SHA-1 and Implications for the Web PKI*; SHAttered Attack Report; Springer: Cham, Switzerland, 2017.
39. NIST. *Transition to Post-Quantum Cryptography; NIST Internal Report 8547*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf (accessed on 3 October 2025).
40. NIST. *Considerations for Achieving Crypto Agility; NIST Cybersecurity White Paper (CSWP) 39*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf (accessed on 3 October 2025).
41. Attema, T. *The PQC Migration Handbook*; TNO: The Hague, The Netherlands, 2023. Available online: https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf (accessed on 3 October 2025).
42. IETF. *Deprecating TLS 1.0 and TLS 1.1*; RFC 8996; IETF: Fremont, CA, USA, March 2021.
43. Rescorla, E. *The Transport Layer Security (TLS) Protocol Version 1.3*; RFC 8446, IETF: Fremont, CA, USA,, August 2018.
44. Akamai. The state of TLS 1.3 deployment. In *Akamai Security Intelligence Report*; Akamai Technologies: Cambridge, MA, USA, 2019; pp. 32–58.
45. Internet Engineering Task Force (IETF). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. Available online: https://datatracker.ietf.org/doc/html/rfc8446 (accessed on 27 September 2025).
46. APNIC Labs. Measuring the adoption of TLS 1.3. Available online: https://labs.apnic.net/ (accessed on 27 September 2025).
47. Seychelles, A.; Brown, P.; Kumar, R. Legacy cryptography and operational inertia in large-scale systems. *J. Cyber Risk* **2021**, *10*, 142–159.
48. United States National Security Council. *National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. The White House. (2022, May 4). Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/national-security-memorandum-10-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed on 27 September 2025).
49. UK National Cyber Security Centre. Preparing for Post-Quantum Cryptography: Guidance for Organizations. Available online: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography (accessed on 27 September 2025).
50. ENISA. *Post-Quantum Cryptography: Expected Impact and Preparedness*; European Union Agency for Cybersecurity: Athens, Greece, 2022; pp. 1–68.
51. Google. A Roadmap to Deploy Quantum-Resistant Cryptography at Scale. Available online: https://security.googleblog.com/ (accessed on 27 September 2025).
52. Cloudflare. Post-Quantum Cryptography Comes to Cloudflare's Network. Available online: https://blog.cloudflare.com/ (accessed on 27 September 2025).

53. Bank for International Settlements. *Roadmap for Quantum-Safe Cryptography in Financial Market Infrastructures*; BIS: Basel, Switzerland, 2025; pp. 1–56.
54. Bank for International Settlements. *Macro-Financial Risks from Cryptographic Disruption: Scenario Analysis*; BIS: Basel, Switzerland, 2025; pp. 10–24.
55. U.S. Office of Management and Budget. *Guidance on Budgeting for Post-Quantum Cryptography Transition*; Memorandum M-24-07; U.S. Office of Management and Budget: Washington, DC, USA, 2024; pp. 1–12.
56. U.S. Government Accountability Office. *Post-Quantum Cryptography: Federal Agencies Need to Plan for Transition Costs*; GAO-23; U.S. Government Accountability Office: Washington, DC, USA, 2023; pp. 1–40.
57. White House/Office of Management and Budget. *Report on Post-Quantum Cryptography Migration*. White House Report, 2024. Government-wide estimate of approximately USD $7.1 billion between 2025 and 2035 for PQC migration in non–national-security systems. Available online: https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/ (accessed on 11 December 2025).
58. Harvest Now, Decrypt Later. Available online: https://en.wikipedia.org/wiki/Harvest_now%2C_decrypt_later (accessed on 3 October 2025).
59. Cloudflare. Why Transition to Post-Quantum Cryptography and Why Now? Blog Post, 2025. Available online: https://blog.cloudflare.com/he-il/post-quantum-zero-trust/ (accessed on 3 October 2025).
60. F5. Understanding PQC Standards and Timelines. Available online: https://www.f5.com/company/blog/understanding-pqc-standards-and-timelines (accessed on 3 October 2025).
61. Stormshield. Preparing for the Digital Future: Post-Quantum Cryptography Challenges and Adoption in Companies. Available online: https://www.stormshield.com/news/preparing-for-the-digital-future-post-quantum-cryptography-challenges-and-adoption-in-companies/ (accessed on 3 October 2025).
62. Näther, C.; Herzinger, D.; Gazdag, S.-L.; Steghöfer, J.-P.; Daum, S.; Loebenberger, D. Migrating Software Systems towards Post-Quantum Cryptography — A Systematic Literature Review. *arXiv* **2024**. https://doi.org/10.48550/arXiv.2404.12854.
63. DigiCert. The Progress toward Post-Quantum Cryptography, 2025. Available online: https://www.digicert.com/blog/the-progress-toward-post-quantum-cryptography (accessed on 3 October 2025).
64. Ahmed, N.; Zhang, L.; Gangopadhyay, A. A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries. *arXiv* **2025**. https://doi.org/10.48550/arXiv.2508.16078.
65. PQShield. NIST Recommends Timelines for Transitioning Cryptographic Algorithms. Available online: https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/ (accessed on 3 October 2025).
66. CyberArk. NIST's New Timeline for Post-Quantum Encryption. Available online: https://www.cyberark.com/resources/blog/nist-s-new-timeline-for-post-quantum-encryption (accessed on 3 October 2025).
67. Menezes, A.; van Oorschot, P.; Vanstone, S. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996; pp. 1–780.
68. Hoffstein, J.; Pipher, J.; Silverman, J.H. *An Introduction to Mathematical Cryptography*, 2nd ed.; Springer: New York, NY, USA, 2014; pp. 1–538.
69. Lenstra, A.K.; Lenstra, H.W., Jr. (Eds.) *The Development of the Number Field Sieve*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 1–264.
70. European Union. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). *Off. J. Eur. Union*, **2022**. Available online: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed on 27 September 2025).
71. ETSI. Quantum-Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. ETSI White Paper No. 28, 2021. Available online: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP28_QSC_2021.pdf (accessed on 27 September 2025).
72. Gao, X.; Zhang, S.; et al. Expert Elicitation on Timelines for Cryptographically Relevant Quantum Computers. *arXiv* **2023**, arXiv:2304.XXXX, 2023. Available online: https://arxiv.org/ (accessed on 27 September 2025).
73. Metaculus Community Forecast. Date of First Cryptographically Relevant Quantum Computer. Available online: https://www.metaculus.com/questions/ (accessed on 27 September 2025).
74. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). 2024. Available online: https://csrc.nist.gov/publications/detail/fips/203/final (accessed on 27 September 2025).
75. NIST. FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA). 2024. Available online: https://csrc.nist.gov/publicaions/detail/fips/204/final (accessed on 27 September 2025).
76. U.S. Office of Management and Budget (OMB). Memorandum M-23-02: Migrating to Post-Quantum Cryptography. 2022. Available online: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-Migrating-to-Post-Quantum-Cryptography.pdf (accessed on 27 September 2025).
77. NIST. SP 800-56C Rev. 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes. 2020. Available online: https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final (accessed on 27 September 2025).

78. Barker, E.; Chen, L.; Barker, E.B.; Roginsky, A.L.; Davis, R. *SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes*; NIST Special Publication; NIST: Gaithersburg, DC, USA, 2020; pp. 1–50.
79. ETSI. Migration to Quantum-Safe Cryptography. ETSI GR QSC 001 and related TRs, 2022. Available online: https://www.etsi.org/committee/qsc (accessed on 27 September 2025).
80. ISO/IEC JTC 1 SC 27. Post-Quantum Cryptography Profiles and Guidelines (work items, including ISO/IEC 14888 updates and PQC profiles). 2024. Available online: https://www.iso.org/committee/45306.html (accessed on 27 September 2025).
81. Basel Committee on Banking Supervision. *Prudential Treatment of Risks from Quantum Computing to Cryptographic Systems: Supervisory Considerations*; BIS Publications; Basel Committee on Banking Supervision: Basel, Switzerland, 2023.
82. Barker, E.; Chen, L.; Cooper, D.; Moody, D.; Regenscheid, A.; Souppaya, M.; Newhouse, B.; Housley, R.; Turner, S.; Barker, W.; et al. *NISTIR 8240: Computing Environments for Cryptographic Algorithms—Crypto Agility Considerations*; NIST Interagency/Internal Reports; NIST: Gaithersburg, DC, USA,2020.
83. World Economic Forum. *Transitioning to a Quantum-Secure Economy: Practical Guidance for Organizations*; WEF Insight Report; World Economic Forum: Geneva, Switzerland, 2023.
84. Cloud Security Alliance. *Preparing Enterprises for the Quantum-Safe Future*; CSA Guidance; Cloud Security Alliance: Las Vegas, NV, USA, 2022.
85. Souppaya, M.; Scarfone, K.; Yeluri, R. *NISTIR 7966: Security of Interactive and Automated Access Management Using Secure Shell (SSH) and Lessons for Crypto-Agility*; NIST Interagency/Internal Reports; NIST: Gaithersburg, DC, USA, 2015; pp. 1–52.
86. *ISO/IEC 27002:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. International Organization for Standardization: Geneva, Switzerland, 2022.
87. Communications Security Establishment (CSE). Canada's Roadmap to Post-Quantum Cryptography. *Government of Canada Guidance*. 2024. Available online: https://www.cse-cst.gc.ca (accessed on 26 December 2025).
88. Australian Signals Directorate (ASD)/Australian Government. Planning for Post-Quantum Cryptography *Commonwealth of Australia* 2024. Available online: https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography (accessed on 5 October 2025).
89. National Security Agency (NSA). NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems. Available online: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/ (accessed on 30 September 2025).
90. National Institute of Standards and Technology (NIST). Considerations for Achieving Crypto Agility: Strategies and Practices (NIST CSWP 39). *NIST Cybersecurity White Paper*. 2025. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf (accessed on 30 September 2025).
91. White House Office of Science and Technology Policy (OSTP). Advancing Post-Quantum Cryptography Readiness in Federal Systems. *OSTP Memorandum* 2024. Available online: https://www.whitehouse.gov/ostp (accessed on 5 October 2025).
92. Cybersecurity and Infrastructure Security Agency (CISA). Post-Quantum Cryptography Migration: Roadmap for Critical Infrastructure. *CISA Guidance*. 2025. Available online: https://www.cisa.gov (accessed on 5 October 2025).
93. Google Chrome Team. Hybrid Post-Quantum Key Agreement in Chrome (X25519_Kyber Hybrid) Rollout Notes. *Chrome Platform Status/Security Blog*, 2024. Available online: https://chromestatus.com (accessed on 5 October 2025).
94. Mozilla Security Engineering. Post-Quantum and Hybrid KEM Support in Firefox/TLS. *Mozilla Security Blog/Release Notes*, 2025. Available online: https://security.mozilla.org (accessed on 5 October 2025).
95. Microsoft Edge Team. TLS Hybrid Post-Quantum Key Exchange Support in Edge. *Microsoft Security Blog / Edge Platform Status*, 2025. Available online: https://learn.microsoft.com (accessed on 5 October 2025).
96. OpenSSL Project. OpenSSL 3.x: Hybrid PQC (X25519+Kyber) in TLS 1.3–Implementation Notes. *Project Documentation*, 2024. Available online: https://www.openssl.org (accessed on 5 October 2025).
97. BoringSSL. Hybrid PQC Key Agreement Support for TLS 1.3. *Project Repository Documentation*, 2024. Available online: https://boringssl.googlesource.com/boringssl (accessed on 5 October 2025).
98. Amazon Web Services. AWS CloudFront: Hybrid Post-Quantum TLS Key Agreement (Kyber) Enablement. *AWS Security/CloudFront Blog*, 2024. Available online: https://aws.amazon.com/blogs/security (accessed on 5 October 2025).
99. Akamai. Enabling Hybrid Post-Quantum TLS at Scale. *Akamai Blog / Product Documentation*, 2025. Available online: https://www.akamai.com (accessed on 5 October 2025).
100. European Commission. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Available online: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (accessed on 30 September 2025).
101. A joint statement from 18 EU Member States' Agencies on Post-Quantum Cryptography Transition. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-jointstatement.pdf?__blob=publicationFile&v=5 (accessed on 30 September 2025).

102. Eurosystem. ECB Public Consultation on Cyber Resilience Oversight Expectations *Eurosystem Communication*, 2024. Available online: https://www.ecb.europa.eu/press/intro/cons/html/cyber_resilience_oversight_expectations.en.html (accessed on 30 September 2025).
103. European Union. NIS2 Implementation Guidance: Cryptographic Agility and PQC Considerations for Essential and Important Entities. *EU/NIS Cooperation Documents*, 2024. Available online: https://digital-strategy.ec.europa.eu (accessed on 30 September 2025).
104. NCSC (National Cyber Security Centre). Timelines for Migration to Post-Quantum Cryptography. 2025. Available online: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (accessed on 5 October 2025).
105. Australian Signals Directorate (ASD). Guidelines for Cryptography. Available online: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography (accessed on 30 September 2025).
106. Monetary Authority of Singapore (MAS). Advisory on Addressing the Cybersecurity Risks Associated with Quantum. Available online: https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum (accessed on 30 September 2025).
107. Bank of Israel, Banking Supervision Department. Supervisory Directive: Transition Planning Requirements for Banking Corporations. *Supervisory Directive*, 2024. Available online: https://www.boi.org.il (accessed on 5 October 2025).
108. Bank of Israel. Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities. 2025. Available online: https://www.boi.org.il/en/economic-roles/supervision-and-regulation/letters/letter202501en (accessed on 5 October 2025).
109. Financial Stability Board (FSB). FSB Chair Sets Out the FSB's Work to Maintain Financial Stability Amidst Technological Advancements.*FSB Publication*. 2024. Available online: https://www.fsb.org/2024/10/fsb-chair-sets-out-the-fsbs-work-to-maintain-financial-stability-amidst-technological-advancements/(accessed on 5 October 2025).
110. Apple WebKit/Research Community. Measuring Hybrid PQC Adoption in the Web Ecosystem (Top Sites, Traffic Shares). *Measurement Report/WebKit Blog* 2025. Available online: https://webkit.org/blog (accessed on 5 October 2025).
111. Institute of International Finance. Quantum Safety Boot Camp (3-Day Program), December 2024. *IIF Event Materials*, 2024. Available online: https://www.iif.com/ (accessed on 27 September 2025).
112. FS-ISAC Post-Quantum Working Group. *Defining Crypto-Agility and Sector Guidance for PQC Migration*; FS-ISAC Member Brief FS-ISAC: Reston, VA, USA, 2024.
113. European Quantum Financial Forum. Quantum Safe Financial Forum—A Call to Action. *European Cybercrime Centre (EC3), Europol*, 2025. Available online: https://www.europol.europa.eu (accessed on 27 September 2025).
114. UK National Cyber Security Centre. *Annual Cyber Threat Report 2024/25*; NCSC Report; UK National Cyber Security Centre: London, UK, 2025.
115. European Union Agency for Cybersecurity (ENISA). *Threat Landscape*, 2024. ENISA Report; ENISA: Athens, Greece, 2024.
116. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization: Selected Algorithms and Draft Standards. *NIST Cryptographic Standards and Guidelines*. 2024. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/selected-algorithms (accessed on 27 September 2025).
117. FS-ISAC. Emerging Threats to Payment Systems: Sector Brief. *FS-ISAC Report*. 2024. Navigating Cyber 2024: Annual Report on Emerging Threats and Operational Resilience in the Financial Services Ecosystem. Available online: https://www.fsisac.com/navigatingcyber2024 (accessed on 27 September 2025).
118. FS-ISAC. Navigating Operational Resilience in the Global Payments Ecosystem. *FS-ISAC Report*. 2023. Available online: https://www.fsisac.com/hubfs/NavigatingCyber-2023/NavigatingCyber2023-Final.pdf?hsLang=en (accessed on 27 September 2025).
119. Introduction to Post-Quantum Security: Understanding the Quantum Threat and Future Security Considerations in SWIFT Networks.2025. Available online: https://www.swift.com/myswift/services/training/swift-training-catalogue/browse-swift-training-catalogue/introduction-post-quantum-security (accessed on 5 October 2025).
120. Committee on Payments and Market Infrastructures (CPMI). *ISO 20022 Migration for Cross-Border Payments: Key Learnings and Next Steps*; Bank for International Settlements (BIS): Basel, Switzerland, 2023. Available online: https://www.bis.org/cpmi (accessed on 5 October 2025).
121. European Central Bank (ECB). TARGET Services Annual Report 2024: T2-T2S Consolidation and ISO 20022 Migration Insights.. *Annual Report*. 2024. Available online: https://www.ecb.europa.eu/press/targetservar/html/ecb.targetservar2024.en.htm (accessed on 2 October 2025).
122. European Banking Authority (EBA). Digital Operational Resilience Act (DORA): Overview and EBA Activities on ICT Risk Management and Operational Resilience. Available online: https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act (accessed on 2 October 2025).

123. Bank of England; Prudential Regulation Authority; Financial Conduct Authority. Operational Resilience: Final Rules and Updates. *UK Authorities Policy Materials*, 2021–2024. Available online: https://www.bankofengland.co.uk, https://www.fca.org.uk (accessed on 5 October 2025).
124. Banca d'Italia. *Remarks by the Deputy Governor on Transition Planning and Operational Resilience*; Banca d'Italia: Rome, Italy, September 2024. Available online: https://www.bancaditalia.it (accessed on 5 October 2025).
125. Group of Seven (G7). *Finance Ministers and Central Bank Governors' Communiqué*. Rome, 2024. Available online: https://www.g7italy.it (accessed on 5 October 2025).
126. Financial Stability Board (FSB). Enhancing Cross-Border Payments: 2024 Progress Report. *FSB Report*. 2024. Available online: https://www.fsb.org (accessed on 5 October 2025).
127. PCI Security Standards Council (PCI SSC). PCI DSS v4.0 and Related Guidance for the Payment Card Ecosystem. *PCI SSC Standards and Guidance*, 2024. Available online: https://www.pcisecuritystandards.org (accessed on 5 October 2025).
128. Bank of England. RTGS and CHAPS Annual Report 2024/25. *BoE Publication*. 2025. Available online: https://www.bankofengland.co.uk/report/2025/rtgs-and-chaps-annual-report-2024-2 (accessed on 5 October 2025).
129. UK National Cyber Security Centre (NCSC). Preparing for Post-Quantum Cryptography: Planning Expectations and Timelines. *NCSC Guidance*. 2024. Available online: https://www.ncsc.gov.uk (accessed on 5 October 2025).
130. Openbank (Grupo Santander). Openbank Enables Hybrid Post-Quantum TLS for Customer Web Sessions. *Engineering/Press Note*. 2025. Available online: https://www.openbank.es (accessed on 5 October 2025).
131. Accredited Standards Committee X9. X9 Financial PKI Q&A. Available online: https://x9.org/x9-financial-pki-qa/ (accessed on 5 October 2025).