The Timeline for Post Quantum Cryptographic Migration

A Position Paper on the Financial Sector's Global Transition

Produced in collaboration by the FS-ISAC Post Quantum Cryptography Working Group, members of the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), and the Quantum Safe Financial Forum

FS-ISAC

Post Quantum Cryptography Timelines

Contents

Contributors

Lead: Jaime Gómez García
Banco Santander and Chair of the Quantum Safe Financial Forum

Support: Dr. Kenneth Giuliani, CIBC, and Mike Silverman, FS-ISAC

- Peter Bordow, Wells Fargo
- Jelena Zelenovic Matone, European Investment Bank
- Ivan Makarov, TD Bank
- Mark Paulsen, TD Bank
- Oscar Covers, Dutch Banking Association (NVB)
- Dr. Thibaud Ecarot, National Bank of Canada
- Rebecca Gibergues, FS-ISAC
- Dr. Leila Taghizadeh, Allianz SE
- Imran Khan, Bank of Montreal
- Dr. Robby Burko, Scotiabank
- Ivan Soto, Bank of Spain
- Tapan Ghosh, Mizuho Americas
- Members of the FS-ISAC Post Quantum Cryptography Working Group
- Members of the Quantum Safe Financial Forum
- Members of the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

Executive Summary

This white paper provides insights for regulators, supervisors, and financial institutions on the significance of establishing a **global transition timeline** for the financial sector's migration to post quantum cryptography (PQC), along with key considerations for its implementation. It is the belief of the authors that coordinated, proactive planning will enable a more efficient transition.

Written by a team of experts in multiple organizations and countries, the white paper describes the **risks of delay** in detail, covers the sector's **critical dependencies and stakeholders**, and discusses **existing regulations**. It outlines the key outcomes of a phased approach and explains why **consensus is currently limited** around the target dates.

The goals of the white paper are to:

- Promote consensus within the financial sector on the need for coordinated action among key stakeholders.
- Establish agreement on the steps needed to develop such coordination.
- Foster and facilitate collaboration by identifying the interdependencies and complexities of the migration and building a framework for collective, proactive engagement.

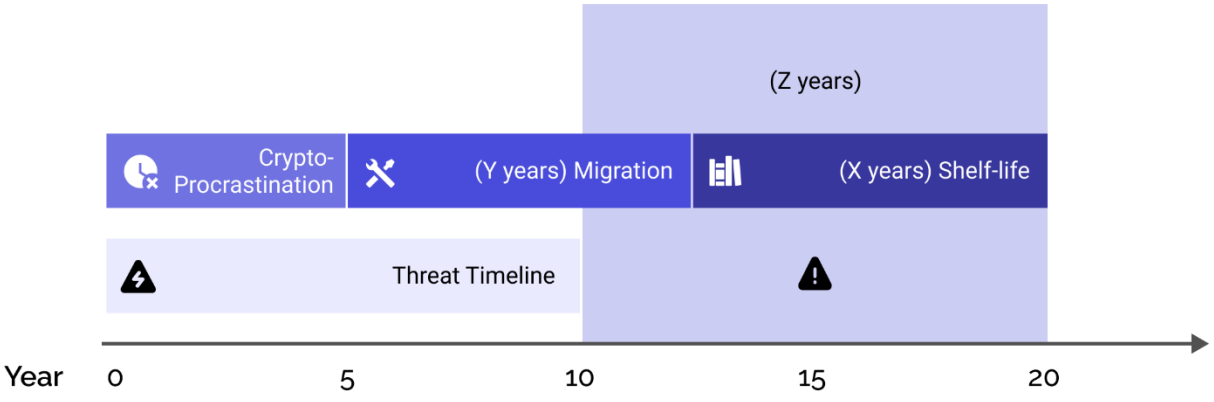
The time to prepare for quantum computing is arguably growing shorter, and the risks to security and resilience are clear. The migration to post quantum cryptography will not be simple – but the insights in this work will help the financial services sector make the transition with fewer challenges and more efficiency.

The Risks of Crypto-Procrastination

The transition to quantum-resistant cryptography is a global challenge that demands strong focus and coordination, particularly in the financial sector. Despite increasing awareness, many organizations have yet to define or apply resources adequately supporting quantum-resistant projects. This delay (what we call crypto-procrastination) threatens the overall migration roadmap by compressing future implementation tasks into unrealistically short timeframes.

Mosca's Theorem, below, illustrates the issue. In short, Mosca's Theorem posits that if the amount of time that data must remain secure (X years) plus the time it takes to upgrade cryptographic systems (Y years) overlaps with the arrival of cryptographically-relevant quantum computers (Z years), financial services firms will run out of time to implement crypto-resilient algorithms. The effective migration window should be adjusted according to data sensitivity, system lifecycles, and the development of available post-quantum solutions.

Augmented Mosca's Theorem



Three key factors typically contribute to crypto-procrastination:[i]

1. Underestimating the impact
2. Misunderstanding the complexity of migration
3. Deferring the quantum threat as a future risk

Financial services' complex, systemic, and interconnected ecosystem means the sector has critical dependencies and sequencing considerations that hamper individual progress and coordination. Those dependencies and considerations include:

- **Peer financial institutions:** There are significant dependencies between regulated firms for delivery of services, including financial market infrastructure such as Central Counterparties (CCPs) and Central Securities Depository (CSDs). Eliminating quantum-vulnerable cryptography may be delayed by the need to support slow movers.
- **Publicly owned financial market infrastructure:** Some of the most critical financial services institutions are highly dependent on financial market infrastructure (e.g., payments and settlement systems) owned and operated by the public sector (e.g., national central banks). These services must also migrate within the necessary timelines. We recognize that private and public networks have different risk profiles. Private networks are out of scope for this document but should be considered by the sector in the future.
- **Critical infrastructure organizations:** Financial institutions rely on the services of other sectors, such as telecoms and energy. For financial institutions to be resilient, those sectors will also need to become quantum secure.
- **Technology and service providers:** Financial institutions are heavily dependent on third parties to provide mature, quantum-safe products and services. Due to the criticality of financial systems, institutions will require more time than other businesses to update third-party products to mitigate the risk of instability or security vulnerabilities.
- **Standards/governing bodies:** Financial systems and their service providers are connected through technical standards and similar bodies. Systems and suppliers need to coordinate with these often cross-sector entities to ensure successful upgrades to crypto-resilient products, both within the financial services sector and across all ecosystems.

CCPs are guarantors of trades between buyers and sellers

CSDs allow the transfer of securities through a book entry rather than physical certificates

- **Budget timelines:** Financial institution investment cycles can be several years long. Budget decisions need to be sequenced and planned with sufficient — often lengthy — timelines to accommodate the investments.

For guidance on managing the risks of post-quantum cryptography and crypto-procrastination, see the Post Quantum Cryptography Working Group's other white papers.

- Current State (Crypto Agility) Technical Paper
- Future State Technical Paper
- Infrastructure Inventory Technical Paper

The Need for Global Coordination

Faced with uncertainty about future standards of algorithms, certificates, and other cryptographic infrastructure, and considering the continuing maturity of post-quantum algorithms, institutions need to plan migration using a cryptographically agile approach. This involves adopting architectures that allow for algorithm changes without major redeployment, separating business logic from cryptographic primitives, and maintaining a cryptographic inventory that provides the firm with information on its level of agility.

Given the financial sector's extensive interconnectivity, a synchronized migration strategy would streamline the transition by addressing key bottlenecks, including the following.

The Existing Recommendations and Timelines section offers more considerations for resolving the challenges of confusion and insights on regulation.

Post Quantum Cryptography Timelines

Existing regulations, such as DORA,[ii] or obligations, such as PCI-DSS,[iii] require organizations to prevent future challenges to cryptography. However, a global action plan and timeline are essential to help prevent crypto-procrastination and ensure an orderly transition. Many institutions have identified the need for coordination. Banca d'Italia, for example, stated that "despite growing awareness of the quantum threat, a comprehensive and widely shared action plan in this area remains elusive. The lack of such a plan concerning the transition to a quantum-safe world may induce protracted inertia in the financial system's migration efforts."[iv]

The positive impact of influential timelines was demonstrated by the first version of the US National Security Agency's (NSA) transition plan, Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), published in 2022.[v]

By publishing its internal transition timeline, the US government and its NSA achieved three key goals:

1. Provided public visibility of their roadmap.
2. Established milestones for national security system administrators.
3. Informed its vendors and service providers of what the US government will expect from them.

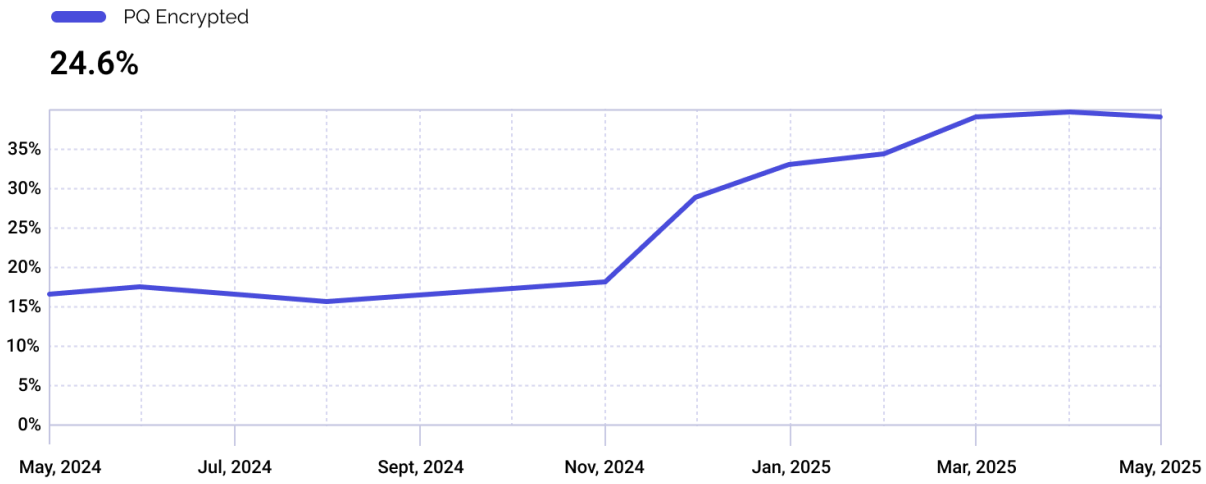
In practical terms, the CNSA 2.0 timeline helped relevant IT vendors prioritize PCQ activities and product roadmaps in 2022, 2023, and 2024 to prepare for future integration of PQC. As of today, leading internet browsers like Chrome and Edge, cryptographic libraries like OpenSSL,[vi] and content delivery networks like Cloudflare[vii] have begun supporting hybrid and classical post-quantum key establishment that protects web browsers.

According to Cloudflare Radar,[viii] a sizeable portion of today's internet traffic is already protected by quantum-resistant encryption. It can be inferred from Cloudflare's data that an equivalent proportion of traffic is likewise protected.

Post-quantum key exchange algorithms establish a shared secret key between two parties that can be used to protect confidentiality with symmetric encryption algorithms (like AES).

Post-Quantum Encryption Adoption

Post-quantum encrypted share of HTTPS request traffic



Source: Cloudflare's adoption and usage dashboard

Existing Recommendations and Timelines

The authors believe that global coordination is necessary to create consistent timelines for transition activities – in our sector and overall – and that the financial services ecosystem should be working towards a common end-date. However, to date, we have observed a lack of consistency in activities or timelines in industry-agnostic publications and in financial services-specific publications. The sector must align across jurisdictions, or the ecosystem will not be able to come together to achieve the goals.

We recognize the reasonable consensus of 2035 in government timelines as an end date. Institutions such as the Europol Quantum Safe Financial Forum,[ix] FS-ISAC,[x] the UK's Cross Market Operational Resilience Group (CMORG),[xi] the Canadian Forum for Digital Infrastructure Resilience,[xii] the G7 Cyber Experts Working Group,[xiii] the World Economic Forum,[xiv] the US's Bank Policy Institute,[xv] and the Bank for International Settlement[xvi] recommend that financial institutions start the migration effort to post quantum cryptography as soon as possible.

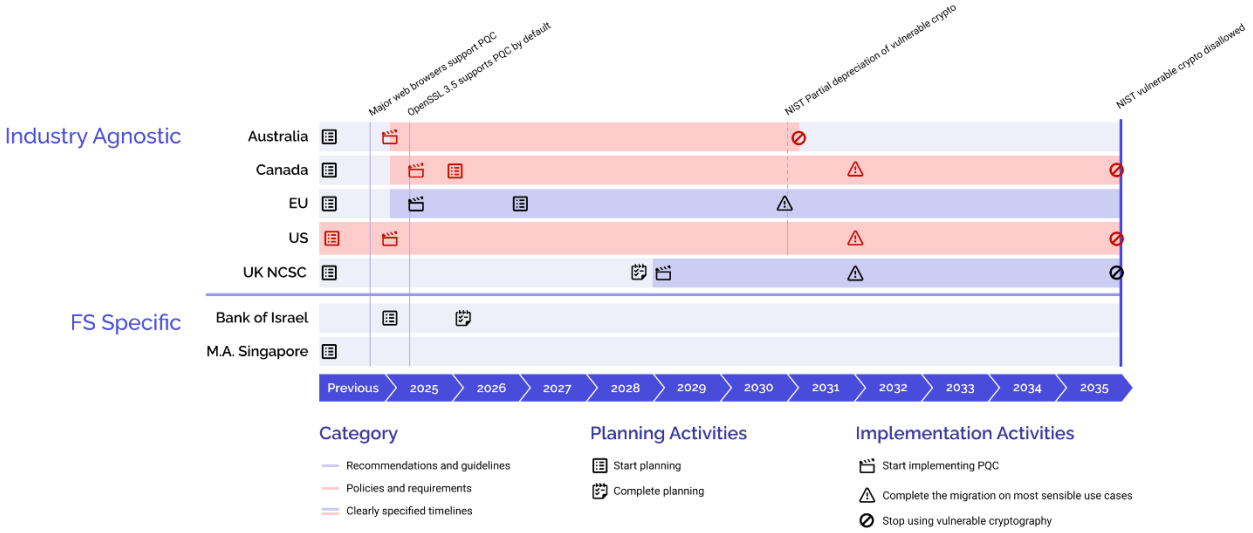
However, these recommendations have not translated into tactical action plans by financial services firms. Though some guidance has been published that could be prescriptive in certain environments (largely government and national security systems), most publications related to the financial sector lack detail and are unlikely to drive global alignment effectively.

Some key publications provide relevant insights into the financial sector's window:

- The Australian Cyber Security Centre[xvii] and the US NSA[xviii] published mandatory timelines and policies (the NSA's CNSA 2.0, an update of the 2022 version, is less detailed in use cases but offers a shorter final deadline).
- The UK National Cyber Security Centre published guidance on migration timelines for organizations.[xix]
- The European Commission has published *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography,*[xx] and agencies from 18 EU member states published a joint statement.[xxi]
- The US National Institute of Standards and Technology (NIST) announced its intention to deprecate the use of normal security configurations of quantum-vulnerable cryptography (like RSA-2048) by 2030 and disallow the use of all classical public key cryptography by 2035.[xxii] The NIST timeline decouples the transition timeline from the expectation of a Cryptographically Relevant Quantum Computer (CRQC), especially in the financial sector, in which organizations are required to comply with standards for security and interoperability reasons. This is recognized as a general indicator or standard for the industry. The financial services sector must decide how to incorporate these standards into its guidelines.
- In February 2024, the Monetary Authority of Singapore published a circular to all financial institutions under its jurisdiction with recommendations to address the cybersecurity risks associated with quantum.[xxiii]
- In January 2025, the Bank of Israel published a directive requiring banking corporations and licensed payment service providers to develop an initial preparedness plan.[xxiv]

Post Quantum Cryptography Timelines

Compared Transition Timelines



[xxv] *National security systems have different timelines dictated by CNSSP 15*
[xxvi] *Please see the References and Resources section for source publications.*

A comparative analysis of these publications shows a strong consensus: firms must create a quantum threat program as soon as possible to initiate planning and improve cryptographic management maturity (which is also required by policies like DORA in the EU or PCI-DSS in 2025).

It also shows how the period 2030-2031 represents a key milestone, when algorithms like RSA-2048 will be deprecated. National cybersecurity organizations (such as those in Australia and the US) recommend that institutions have either completed the migration to PQC or have migrated critical use cases by then.

However, agreement or convergence among most financial institutions towards this target date remains limited. Though quantum-resistant solutions are expected to become available starting as early as 2026 (if not actively used already), most statements specific to the financial sector only recommend that planning should begin. For instance, the UK NCSC recommends starting the migration of critical use cases after 2028, giving firms just two years to meet the Australian requirement and ignoring the current availability of quantum-resistant solutions for some key use cases, such as critical websites.

Considerations for a Global Timeline

Transition Phases

The authors understand that a phased transition approach mitigates many of the risks of rolling out PQC. Financial institutions believe that by prioritizing the high- and medium-risk use cases first, many of the biggest concerns in transitioning from quantum-vulnerable algorithms will be mitigated, helping them ensure all appropriate resources are prioritized and deadlines are met.

At a very high-level, phasing should consider at least:

1. The initiation of a focused transition program, which would include:
   - Incorporating quantum resistance into the organization's risk framework and culture
   - Estimating and securing needed resources and budgets
2. **A discovery and inventory phase,** through which financial institutions should:
   - Inventory their dependencies on quantum-vulnerable algorithms, prioritizing high-risk portions of their architectures that are easily identified
   - Continue to gather data and apply prioritization for all business use cases in the remainder of the ecosystem.
3. **A deployment phase**
   - Remediate all high- and medium-risk use cases of quantum-vulnerable algorithms and have plans for the remainder
   - Begin to disallow connections using quantum-vulnerable algorithms
4. **An exit phase**, during which financial institutions should:
   - Disallow all quantum-vulnerable algorithms
   - Embrace cryptographic agility, so they can change algorithms (and hybrids of algorithms) as needed
   - Conduct an audit to ensure there are no hidden dependencies on quantum-vulnerable cryptography
   - Measure, attest, and report on the continued compliance with policy and regulatory requirements.

A key output of this phase is an initial action plan with adequate organizational accountability and leadership.

Post Quantum Cryptography Timelines

The timelines published by relevant standards organizations and national security agencies will help inform the timing of the key milestones in this phased approach. For instance, the exit phase should end by 2035 to meet currently published recommendations from security agencies.

Dependencies

The timeline needs to consider a number of dependencies and identify ways to influence external stakeholders. Specifically:

Ecosystem dependencies: The timeline should ensure all existing interoperability platforms in the financial sector transition in coordination. This could include how the timelines affect payments networks, markets/exchanges, central banks, clearinghouses, etc.

Vendor dependencies:[xxvii] As it relates to technology and service providers, the timeline should note that some financial institutions are also vendors to others. It should identify ways to influence the vendors' roadmaps.

Stakeholders

Several groups of constituents should be part of this coordinated timeline conversation and implementation:

- Supervisory and regulatory agencies
- Financial institutions
- Financial market infrastructure providers
- Operators of public sector financial market infrastructure

Other groups that should be consulted or involved:

- Working groups focused on the financial sector's quantum safety
- Vendors supplying functionality to financial institutions or their supply chain
- Standards bodies (e.g., IETF)
- The open-source community
- Managed service provider financial institutions
- Customers

Standards dependencies: Aside from PQC standards, firms have dependencies on the roadmaps of standardization bodies like the Internet Engineering Task Force (IETF)[xxviii] and industry collaborations, like the X9 Financial PKI.[xxix] For instance:

- Updates to protocols like TLS, IPSEC, and SSH
- Certificate standards, including signature and certificate construct standards.
- Definition of interoperability/interim protocols, such as hybrid certificates.

Governance and regulation dependencies: The success of the transition will require financial institutions to ensure they can define and implement methods and systems

for governance and ensure relevance and compliance with internal policies. For example:

- Complying with any current or future regulations on cryptography management or quantum safety
- Communicating relevant milestones and expectations with customers and partners

Conclusion

The global, interconnected, and interoperable nature of the financial ecosystem requires worldwide alignment on priorities and transition timelines across the sector. Constructs and guidance from authoritative and governmental agencies, such as CNSA 2.0 (which is specific to US agencies), should provide guidance, inform a coordinated global transition timeline, generate a top-down approach for financial institutions to initiate, and provide resources to transition programs.

This approach should align activities involving all relevant stakeholders, especially those providing technology products and services or managing interoperability platforms (like markets, payments, or messaging), through clear and reasonable milestones that:

- Enforce action.
- Facilitate compliance with local policies and regulations across jurisdictions.
- Reduce the need to maintain backward compatibility. Maintaining both quantum-vulnerable and quantum-resistant algorithms for long periods could be complex and cumbersome. Being clear on the timeline and when to deprecate older technologies reduces the complexity of operating in a bifurcated landscape.

A key aspect of achieving this goal is collaboration within the sector. Post quantum cryptographic resilience is not a competition, but a collaborative project.

References and Resources

[i] Etsi.org. (2025). *ETSI-QSC-Report-2025*. Available at: https://www.etsi.org/e-brochure/ETSI-QSC-Report-2025/mobile/index.html#p=7

[ii] Europa.eu. (2024). *Search results - EUR-Lex*. Available at: https://eur-lex.europa.eu/eli/reg_del/2024/1774/

[iii] PCI SSC (2024). *Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0.1*. Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf.

[iv] Steering the transition to a quantum-safe world. An internationally coordinated approach. (n.d.). Available at: https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2024/Perrazzelli-G7-conference-24092024.pdf?language_id=1

[v] National Security Agency/Central Security Service. (n.d.). *NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy*. Available at: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/ (https://web.archive.org/web/20220908002358/https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF), superseded by the 2024 version described later.

[vi] openssl (2025). *Releases · openssl/openssl*. GitHub. Available at: https://github.com/openssl/openssl/releases

[vii] Cloudflare Docs. (2024). *Post-quantum cryptography (PQC) · Cloudflare SSL/TLS docs*. Available at: https://developers.cloudflare.com/ssl/post-quantum-cryptography/

[viii] Cloudflare.com. (2025). *Adoption & Usage Worldwide | Cloudflare Radar*. Available at: https://radar.cloudflare.com/adoption-and-usage?dateRange=52w

[ix] Europol. (2022). *Quantum Safe Financial Forum - A call to action | Europol*. Available at: https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

[x] Preparing for a Post-Quantum World by Managing Cryptographic Risk. (2023). Available at: https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForA

[xi] CMORG. (2025). *Guidance for Post-Quantum Cryptography*. Available at: https://www.cmorg.org.uk/artefact/guidance-post-quantum-cryptography

[xii] Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR). (2024). Available at: https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

[xiii] *G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing*. (2024). Available at: https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

[xiv] World Economic Forum. (2024). *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*. [online] Available at: https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/

[xv] Bonner, W. (2024). *Quantum Computing: The Urgent Need to Transition to Quantum-Resistant Cryptography - Bank Policy Institute*. [online] Bank Policy Institute. Available at: https://bpi.com/quantum-computing-the-urgent-need-to-transition-to-quantum-resistant-cryptography/

[xvi] Auer, R., Dodson, D., Dupont, A., Haghighi, M., Margaine, N., Marsden, D., McCarthy, S. and Valko, A. (2025). *Quantum-readiness for the financial system: a roadmap*. Bis.org. Available at: https://www.bis.org/publ/bppdf/bispap158.htm

[xvii] Australian Signals Directorate (2025). *Guidelines for cryptography | Cyber.gov.au*. [online] Cyber.gov.au. Available at: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography

[xviii] National Security Agency/Central Security Service. (n.d.). *NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy*. Available at: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[xix] Ncsc.gov.uk. (2025). *Timelines for migration to post-quantum cryptography*. Available at: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[xx] Shaping Europe's digital future. (2025). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Available at: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[xxi] A joint statement from partners from 18 EU member states. (n.d.). Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

[xxii] NIST IR 8547 (2024). Available at: Transition to Post-Quantum Cryptography Standards. https://csrc.nist.gov/pubs/ir/8547/ipd

[xxiii] MAS/TCRS/2024/01. (2024). *MAS/TCRS/2024/01 : Advisory on Addressing the Cybersecurity Risks Associated with Quantum*. [online] Mas.gov.sg. Available at: https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

[xxiv] Boi.org.il. (2025). Available at: https://www.boi.org.il/en/economic-roles/supervision-and-regulation/letters/letter202501en

[xxv] CNSSP 15 states that by January 1, 2027, all brand-new acquisitions for NSS will be required to be CNSA 2.0 compliant

[xxvi] Sources for the Compared Transitions Timeline on page 9.

- Australian Signals Directorate (2025). *Guidelines for cryptography | Cyber.gov.au*. [Cyber.gov.au. Available at: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography.
- Roadmap for the migration to post- quantum cryptography for the Government of Canada (ITSM.40.001). (n.d.). Available at: https://www.cyber.gc.ca/sites/default/files/itsm.40.001-e.pdf
- Shaping Europe's digital future. (2025). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Available at: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- A joint statement from partners from 18 EU member states. (n.d.). Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5.
- European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms. (2025). Available at: https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-

890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf Ncsc.gov.uk. (2025). *Timelines for migration to post-quantum cryptography*. Available at: Ncsc.gov.uk. (2025). *Timelines for migration to post-quantum cryptography*. Available at: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

- National Security Agency/Central Security Service. (n.d.). *NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy*. Available at: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/
- NIST. Transition to Post-Quantum Cryptography Standards. (2024) https://csrc.nist.gov/pubs/ir/8547/ipd
- Bank of Israel. *Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities* (2025). Available at: https://www.boi.org.il/en/economic-roles/supervision-and-regulation/letters/letter202501en
  Monetary Authority of Singapore. *Advisory on Addressing the Cybersecurity Risks Associated with Quantum*. Mas.gov.sg. Available at: https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

[xxvii] A non-exhaustive list of the types of functionality and use cases that vendors provide includes: hardware / firmware (servers, workstations, networking equipment, HSMs, financial equipment (e.g., point of sale and mobile devices), telecomm providers, applications/development (open source software; browsers; office, financial and custom applications), operating systems, API security and gateways cloud service providers, content delivery networks, asset management systems

[xxviii] IETF (2019). *Home*. IETF. Available at: https://www.ietf.org/

[xxix] Accredited Standards Committee X9. (2025). *X9 Financial PKI Q&A - Accredited Standards Committee X9*. Available at: https://x9.org/x9-financial-pki-qa/

