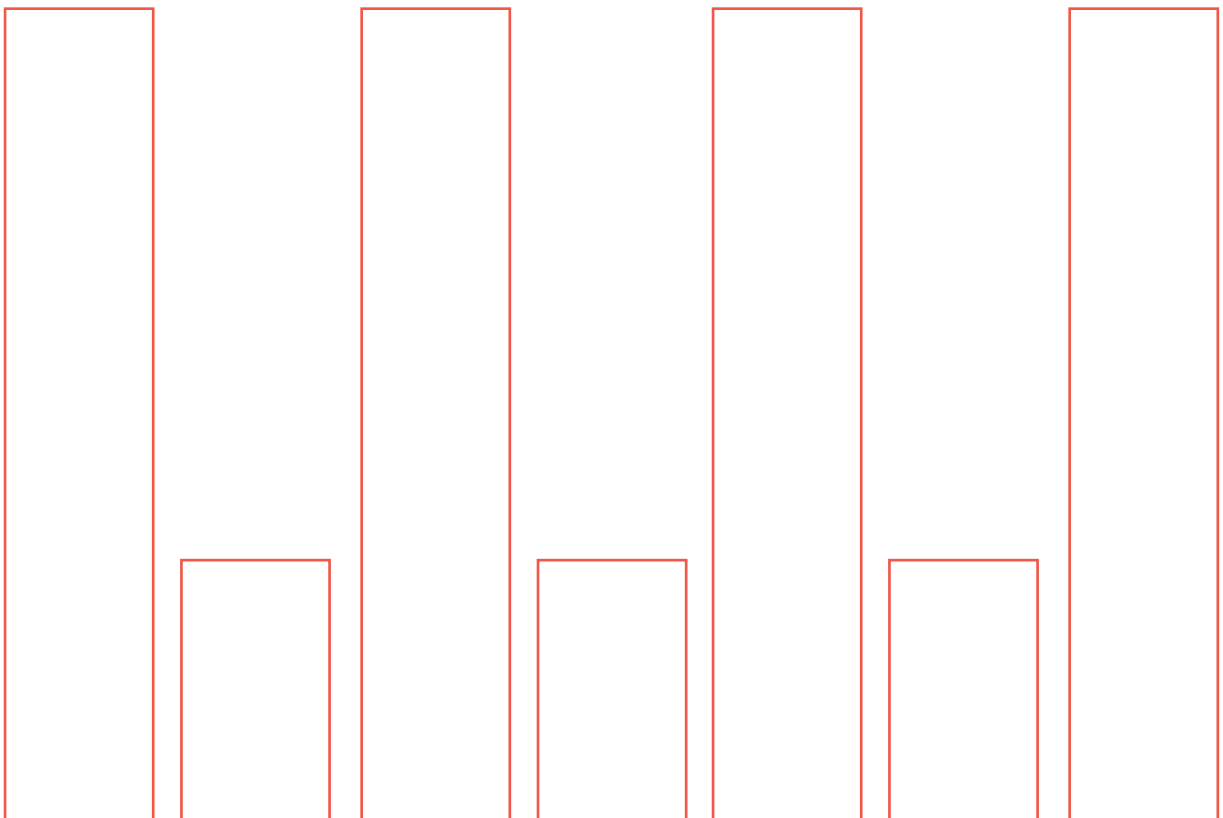
CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

GUIDANCE FOR POST-QUANTUM CRYPTOGRAPHY

CYBER COORDINATION GROUP

VERSION 1.0 | APRIL 2025 | TLP CLEAR



CONTENTS

FOREWORD FROM THE U.S. FINANCIAL SERVICES SECTOR COORDINATING COUNCIL (FSSCC)

The U.S. Financial Services Sector Coordinating Council (FSSCC) was established in 2002 by financial institutions to collaborate with government agencies on protecting the United States' financial infrastructure. As an industry-led non-profit, our mission is to enhance the sector's resilience to a wide range of risks -- from natural disasters to cyber threats -- by fostering public-private coordination.

We are grateful to the UK Cross Market Operational Resilience Group (CMORG) for the opportunity to contribute this foreword on an important paper on addressing quantum threat. The need to modernize cryptographic infrastructure is both urgent and global. The FSSCC supports this work as a part of its broader commitment to strengthening the security and operational resilience of the financial system.

Quantum computers will soon pose profound and complex risk to data protection across all industries. Once scaled, these technologies could render today's public-key encryption obsolete. It is imperative that financial institutions inventory their data, analyze and prioritize it by risk, and begin transitioning to quantum resistant cryptography.

Thankfully, both the processes to conduct this migration and the algorithms required are well known and available. Industry groups such as the Financial Services – Information Sharing Analysis Center (FS-ISAC) and World Economic Forum, and government agencies such as the National Institute of Standards and Technology (NIST) and National Security Agency (in the U.S.) and National Cyber Security Centre (in the UK) have laid out considerations for conducting enterprise level migrations. In 2024, NIST released the first set of quantum resistant cryptography. More will follow from NIST and other technical standards setters.

For the financial sector, this transition is especially challenging. Success will require early action, multi-year planning, and broad alignment across institutions, vendors, and regulators. In fact, regulatory agencies have a significant role to play. Not just in establishing common expectations for regulated entities, but in conducting their own post-quantum transition to protect the data and systems that they manage.

Two factors heighten the urgency:

1. **Interconnected Risk:** No single firm can secure the sector alone. Widespread adoption of quantum-safe cryptography is essential for systemic resilience.

2. **Technology Dependencies:** Financial institutions rely on a vast ecosystem of third-party providers who must deliver quantum-safe solutions well in advance of sector deadlines to enable testing, integration, and deployment.

The FSSCC endorses the core premise of this paper: the time to act is now. A coordinated, forward-leaning response is essential to protect the integrity of the global financial system.

FSSCC Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

Debbie Guild, FSSCC Chair
Executive Vice President and Head of Technology, The PNC Financial Services Group

1 EXECUTIVE SUMMARY

Quantum computers pose risks to cryptographic mechanisms that safeguard critical data and systems in the financial sector. This threat necessitates immediate attention and action through a strategic, phased modernisation of cryptographic infrastructure. Financial institutions (also referred to as 'firms') should begin uplift efforts by establishing comprehensive cryptographic inventories and developing transition roadmaps. A notable consideration in this transition is vendor readiness. Given financial institutions' reliance on third-party solutions, it is imperative to assess and align vendors' capabilities with quantum-resistant standards to facilitate a seamless transition. Banks, as critical national infrastructure (CNI), alongside industry partners and government agencies must act decisively now to promote and adopt quantum resistant cryptographic solutions.

This paper emphasises the urgency of managing quantum risk and aligns with the UK National Cyber Security Centre's (NCSC) guidance[1] for the financial sector to begin transitioning towards quantum-safe cryptographic practices. NCSC states unequivocally that 'the scale of the effort means that work to prepare [migration to Post-Quantum Cryptography] is a priority now.' In other words, the challenge is significant in scope and complexity, and waiting until quantum attacks are imminent is not an option. By enhancing cryptographic inventory capabilities and building a structured migration roadmap, institutions can bolster the resilience of their operations against quantum computing's inevitable impact.

2 BACKGROUND ON QUANTUM COMPUTING

Quantum computing leverages the unique principles of quantum mechanics to perform computations that are infeasible for today's classical computers. While classical bits exist in a state of 0 or 1, quantum bits (qubits) can exist in superposition – essentially being 0, 1, or both simultaneously, This allows quantum computers to process vast combinations of states in parallel. For example, Shor's algorithms for integer factorisation can theoretically run in polynomial time on a sufficiently powerful computer, whereas classical computers would require exponential time.[2] This dramatic increase in potential computing power means quantum computers will be able to tackle complex problems (like factoring large numbers or decrypting certain cryptographic schemes) that are currently considered practically impossible.

3 IMPACT TO CRYPTOGRAPHY

The advent of large-scale quantum computing would pose significant challenges to current encryption and authentication techniques. Modern public-key cryptography, which underpins secure banking transactions, internet-based communications and digital signatures, relies on complex mathematical problems that are effectively unsolvable with today's computing power. A future quantum computer, however, could solve these problems in a reasonable timeframe, breaking algorithms like RSA and elliptic curve cryptography (ECC) that are widely used across the financial industry. In essence, once a

[1] National Cyber Security Centre. (n.d.). Migrating to Post-Quantum Cryptography (PQC). Retrieved from https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[2] Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5), 1484-1509. Retrieved from https://arxiv.org/pdf/quant-ph/9508027

cryptographically relevant quantum computer (CRQC) is available, an adversary could defeat the cryptography protecting sensitive financial data and transactions.

While private key cryptography, such as the Advanced Encryption Standard (AES), is theoretically vulnerable to quantum attacks via Grover's algorithm, the practical risk is considered low.[3] Grover's algorithm would require doubling the key length to maintain security, but due to implementation complexities, this attack does not scale to a level that poses an immediate threat. Therefore, the focus remains on addressing the vulnerabilities in public key cryptography as the primary concern for post-quantum cryptography (PQC).

The timeline for the first CRQC remains uncertain, but many experts estimate it within the next decade.[4] Critically, even if we assume we have 7-10 years, the extensive effort required to migrate systems means organisations cannot wait. Any delay increases the risk that the quantum threat will materialise before defences are in place. Moreover, adversaries may "store now and decrypt later," by intercepting and saving encrypted data today in hopes of decrypting it once they have quantum capabilities. This means long-lived sensitive data (e.g., confidential records, keys that secure historical transactions, etc.) could be retroactively compromised. The bottom line is that quantum threats are inevitable, and proactive risk mitigation is essential to preserve the confidentiality and integrity of financial information.

4 POST-QUANTUM CRYPTOGRAPHY REVIEW

In response to the looming quantum threat, global efforts to develop quantum-resistant cryptographic algorithms have accelerated. The National Institute of Standards and Technology (NIST) initiated its post-quantum cryptography project in 2016 and continues to evaluate and release new algorithms. In August 2024, NIST finalised its first set of PQC algorithms designed to withstand quantum attacks, marking a significant milestone in the journey to securing digital infrastructure. These algorithms include:

- ML-KEM: A public key encapsulation mechanism for secure key exchanges.
- ML-DSA: A digital signature scheme designed for secure authentication.
- SLH-DSA: An additional digital signature scheme that uses a stateless hash-based mechanism.

These algorithms are now recommended for implementation and NIST encourages organisations to begin integrating them immediately to mitigate future risks. To support this transition, NIST established a project at the National Cybersecurity Center of Excellence (NCCoE) that will publish guidelines to assist organisations in their PQC migration strategies.

NIST's efforts were reflected in developments in the UK, where the NCSC updated its guidance to align with these PQC standards. The NCSC also supports the use of hybrid cryptographic solutions, which combine classical and PQC algorithms to facilitate a smoother transition to quantum safe systems.

Additionally, other jurisdictions across the globe continue to evaluate further candidates, including Germany and France. More standardised algorithms provide further options for organisations to evaluate and select for migration. In December 2024, security agencies of eighteen EU member states

[3] ETSI. (2015). Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/quantumsafewhitepaper.pdf
[4] Global Risk Institute. (2023). Quantum Threat Timeline Report. Retrieved from https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

released a joint statement urging organisations to transition to international standards such as the NIST algorithms. The below table provides a high-level summary of jurisdictional activities related to PQC standardisation.

Country/Agency	**Recommended PQC Algorithms or Actions**
United Kingdom (NCSC)	Advises preparation for the transition to quantum-safe algorithms, aligning with international standards such as NIST.[5]
France (ANSSI)	Transition Strategy: Advocates progressive increase of assurance on new post-quantum algorithms without introducing vulnerabilities. Specific algorithm recommendations are to be detailed in forthcoming guidelines.[6]
Germany (BSI)	General Guidance: Emphasises the importance of migrating to PQC and support the adoption of algorithms selected by NIST. Specific algorithm recommendations are to be detailed in forthcoming guidelines.[7]

5 CMORG PQC ROADMAP

Transitioning to post-quantum cryptography (PQC) is a complex and time-consuming process, as evidenced by industry experiences. Many organisations have found that upgrading cryptographic infrastructure involves significant challenges, including the need for extensive planning, resource allocation, and coordination with various stakeholders. The time involved in this transition underscores the urgency for financial institutions to begin the process if they haven't already, to ensure they are prepared for a quantum-safe future.

There are many resources being developed by industry and governmental bodies, to aid organisations' migration strategies and roadmaps to transition to PQC systems. To prepare for a quantum-safe future, financial institutions must adopt a proactive, structured approach to upgrade their cryptographic infrastructure.

The Cross Market Operational Resilience Group (CMORG) aligns with industry best practices as highlighted in the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and federal partners' publication, *Quantum Readiness: Migration to PQC,*[8] and NCSC's PQC White paper,[9] that are further

[5] National Cyber Security Centre. Migrating to Post-Quantum Cryptography (PQC). National Cyber Security Centre, n.d. https://www.ncsc.gov.uk/pdfs/blog-post/migrating-to-post-quantum-cryptography-pqc.pdf.
[6] Agence nationale de la sécurité des systèmes d'information (ANSSI). (n.d.). ANSSI views on the post-quantum cryptography transition. https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
[7] Federal Office for Information Security (BSI). (n.d.). Quantum technologies and post-quantum cryptography. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html
[8] Cybersecurity and Infrastructure Security Agency. (2023, August). Quantum readiness: Final report. https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf
[9] National Cyber Security Centre. (n.d.). Next steps: Preparing for post-quantum cryptography. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

reflected within sector considerations represented in the Financial Sector Information Sharing and Analysis Center (FS-ISAC)'s publication, *Preparing for a Post-Quantum World by Managing Cryptographic Risk.*[10]

1. Cryptographic Inventory

Financial Institutions should create a comprehensive inventory of all cryptographic assets within their organisation. This involves identifying where cryptography (encryption, digital signature) is used across data-in-transit, data-at-rest, and data-in-use. The inventory should not only track cryptographic algorithm and keys, but also capture metadata like ownership, usage, and lifecycle management. By documenting both known assets and conducting detailed scans, institutions can ensure they have a full picture of their cryptographic landscape, preparing for eventual quantum-resistant updates.

2. Risk Assessment

Next, a risk assessment should be conducted to evaluate the quantum vulnerability of each cryptographic asset. This process should account for variability in timelines across different algorithms, as quantum threats may emerge sooner for some than others. Factors to consider include the shelf life of encrypted data and the timeline for quantum computers becoming capable of breaking current cryptographic algorithms. Institutions should use frameworks that incorporate data longevity, migration timelines, and the urgency of adopting PQC.

3. Prioritisation

Given that the timelines for quantum threats may differ significantly across algorithms, high-risk areas where data has long-term value or where cryptographic mechanisms are critical to operations should be prioritised. Systems that protect long-lived, sensitive data or have extensive third party dependencies may also require more immediate attention. Developing a prioritisation framework helps in managing resources effectively and ensuring that the most critical vulnerabilities are addressed first.

4. Remediation

Remediation involves the migration of systems to quantum-safe algorithms. Institutions should implement the new internationally recognised standards, like the NIST algorithms and other emerging options in other jurisdictions. Additionally, financial institutions must ensure they have crypto-agile systems that can quickly adapt to future cryptographic requirements and quantum threat. Collaboration with vendors and implementing a phased approach for integrating PQC will be key to minimising disruptions while securing critical systems against future quantum threats.

6 VENDOR READINESS INCORPORATED INTO PLANNING

As financial institutions prepare for the quantum future, vendor readiness plays a crucial role in the successful transition to PQC. Given the interconnected nature of modern systems, dependencies on third party vendors - ranging from cloud providers to software developers - are growing. Ensuring that these vendors are quantum-ready is essential for a seamless transition. Where possible, firms should

[10] FS-ISAC. (n.d.). Preparing for a post-quantum world by managing cryptographic risk. https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForAPostQuantumWorldByManagingCryptographicRisk.pdf

engage in dialogue with key vendors to encourage the acceleration of PQC in their offerings. Many large technology providers are already working on quantum-safe updates, but their timelines might not align with those of the financial sector unless demand is signalled.

Firms should assess each vendor's cryptographic protocols, their ability to support new PQC standards, and their readiness to adopt quantum-resistant algorithms. This assessment should consider various types of vendors, including Software as a Service (SaaS) providers, cloud service providers, and hardware manufacturers, as each may have different considerations and timelines for implementing PQC. Establishing clear communication channels with vendors is crucial, as is reviewing their roadmaps for cryptographic updates. Additionally, firms should consider incorporating requirements for PQC in new contracts and service-level agreements to ensure all vendor relationships align with their quantum migration strategies.

7 UK COMMITMENT TO PQC

NCSC has been a global leader in encouraging the public and private sector to consider quantum computing and to start the process of migrating to PQC. This includes two publications in 2020 on quantum security technologies[11] and preparing for quantum-safe cryptography.[12] In their publication on PQC, NCSC stated that firms "should factor quantum-safe transition into their long-term plans and conduct investigatory work to identify which of their systems will be high priority for transition." NCSC is clear that the migration to PQC is a "complex and expensive process that must be planned and managed with care," which is highly applicable to all financial institutions that are members of CMORG.

In August 2024, NCSC updated their PQC White Paper to endorse the NIST quantum-safe algorithms.[13] The UK was the first major regulatory jurisdiction to reflect NIST's algorithms and to embed them within their national advice. UK securities agencies additionally show growing focus on the topic, with the Financial Conduct Authority (FCA) collaborating within the World Economic Forum to publish a white paper on quantum security matters within the financial sector.[14]

8 CONCLUSION

Quantum computing may still be on the horizon, but the security implications are immediate. The inevitability of cryptographically relevant quantum computers – and the magnitude of effort required to defined against them- means that financial institutions must start preparing today, not years from now. This paper has outlined the key steps, from inventory and planning through to vendor engagement. By undertaking these preparations, financial institutions will greatly strengthen their resilience against future threats. Crucially, early movers will also minimise the risk of disruption to their

[11] National Cyber Security Centre. (n.d.). Quantum security technologies. Retrieved from https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[12] National Cyber Security Centre. (n.d.). Preparing for quantum-safe cryptography. Retrieved from https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

[13] National Cyber Security Centre. (n.d.). Migrating to Post-Quantum Cryptography (PQC). Retrieved from https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc

[14] World Economic Forum. (2024). *Quantum Security for the Financial Sector*. Retrieved from https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf

operations and customers by addressing challenges in a controlled, proactive manner instead of under duress.

In summary, the coming quantum era will transform the cybersecurity landscape, but with timely action and collaborative effort, the financial industry can stay one step ahead. The time to begin the post-quantum journey is now; the cost of waiting will be measured in lost trust, broken systems, and compromised data. Future-proofing our cryptography is not just a technical necessity, but a strategic imperative to ensure the safety and integrity of the financial system in the decades to come.

9 APPENDIX: SUGGESTED READING AND RESOURCES

Agence Nationale De La Sécurité Des Systèmes D'information (ANSSI)

- ANSSI views on the post-quantum cryptography transition, December 2023.

Cybersecurity and Infrastructure Security Agency (CISA)

- Quantum-Readiness: Migration To Post-Quantum Cryptography, August 2023.

European Telecommunications Standards Institute (ETSI)

- Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, June 2015
- TR 103 619: Migration strategies and recommendations to Quantum Safe schemes, July 2020.

Federal Office for Information Security (BSI)

- Quantum technologies and post-quantum cryptography, n.d.
- Securing Tomorrow, Today: Transition to Post-Quantum Cryptography, November 2024.

Financial Services Information Sharing and Analysis Center (FS-ISAC)

- Preparing for a post-quantum world by managing cryptographic risk, March 2023.
- Building Cryptographic Agility in the Financial Sector, October 2024.
- The Impact of Quantum Computing on the Payment Card Industry, February 2025.

Global Risk Institute

- Quantum Threat Timeline Report, December 2023.

National Cyber Security Centre (NCSC)

- Migrating to Post-Quantum Cryptography (PQC), n.d.
- Preparing for quantum-safe cryptography, n.d.
- Quantum security technologies, n.d.
- Timelines for migration to PQC Guidance, n.d.

National Institute of Standards and Technology (NIST)

- NIST SP 1800-38A: Executive Summary (Preliminary Draft), 2023-04
- NIST SP 1800-38B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools (Preliminary Draft), 2023-12
- NIST SP 1800-38C: Quantum-Resistant Cryptography Technology Interoperability and Performance Report (Preliminary Draft), 2023-12

World Economic Forum

- Quantum Security for the Financial Sector, 2024