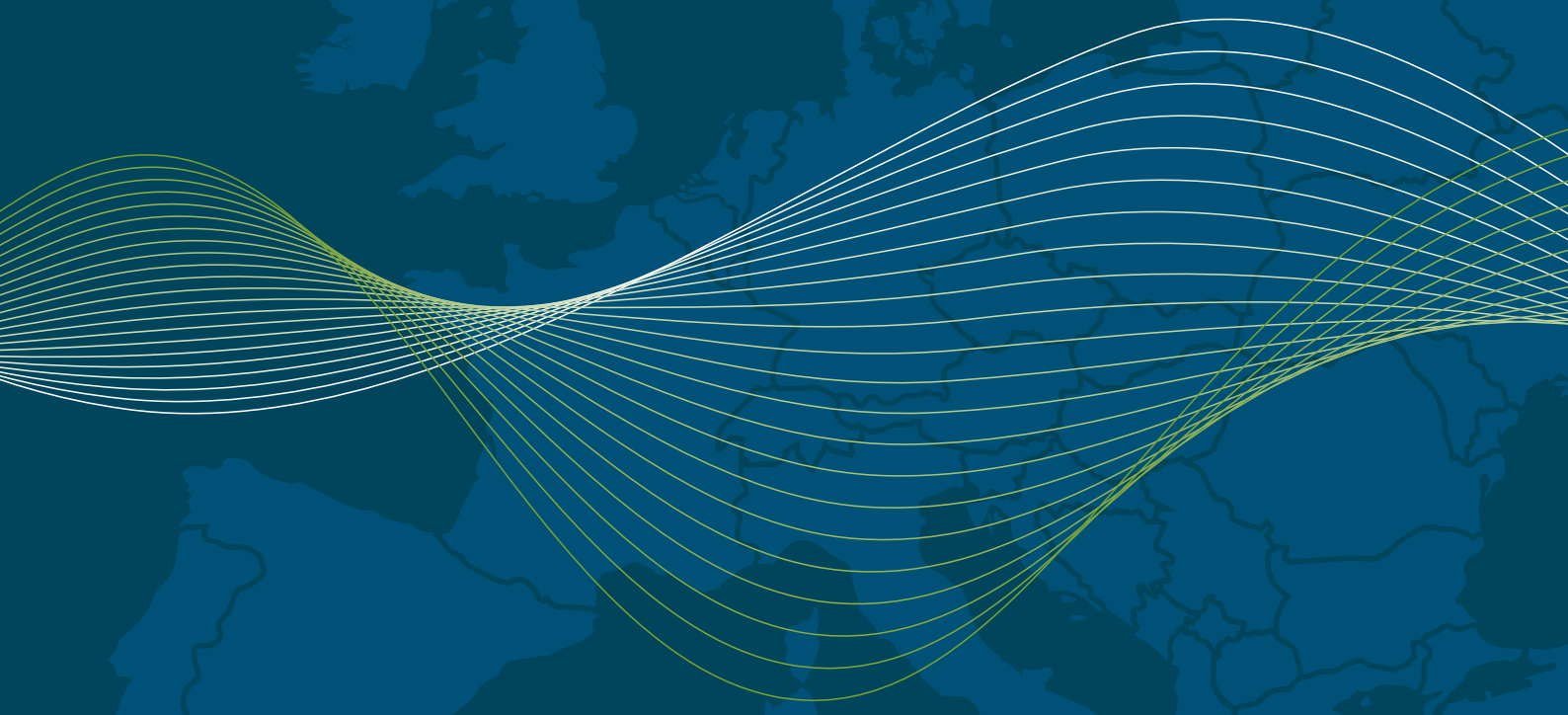
gfma afme/ asifma sifma

Quantum Migration: Mapping the Emerging Landscape

October 2025



Foreword

The advent of quantum computing represents a paradigm shift for cybersecurity in the financial sector. The potential for existing encryption methods to be compromised within the next 5 – 10 years has already catalysed concern and action across a number of financial entities, global regulatory, and industry bodies. For every financial entity, the threat quantum computers present to encryption raises urgent questions regarding data protection, the risk of disruption to critical operations, and the resilience of the sector overall in an increasingly digitised financial ecosystem. Without action, banks will undoubtedly be caught out by the advent of cryptographically-relevant quantum computers and its inevitable misuse by malicious actors to break encryption to access sensitive data. To mitigate this risk, financial entities must prepare by transitioning to post-quantum cryptography.

In response, GFMA have convened a series of expert-led roundtables, to draw out and map the activities of institutions including the US National Institute of Standards and Technology (NIST), the Financial Conduct Authority (FCA), the World Economic Forum (WEF), the Bank of England's Cross Market Operational Resilience Group (CMORG), and the Quantum Safe Financial Forum (QSFF). We recognise other bodies, such as FS-ISAC[1], are also active in this space.

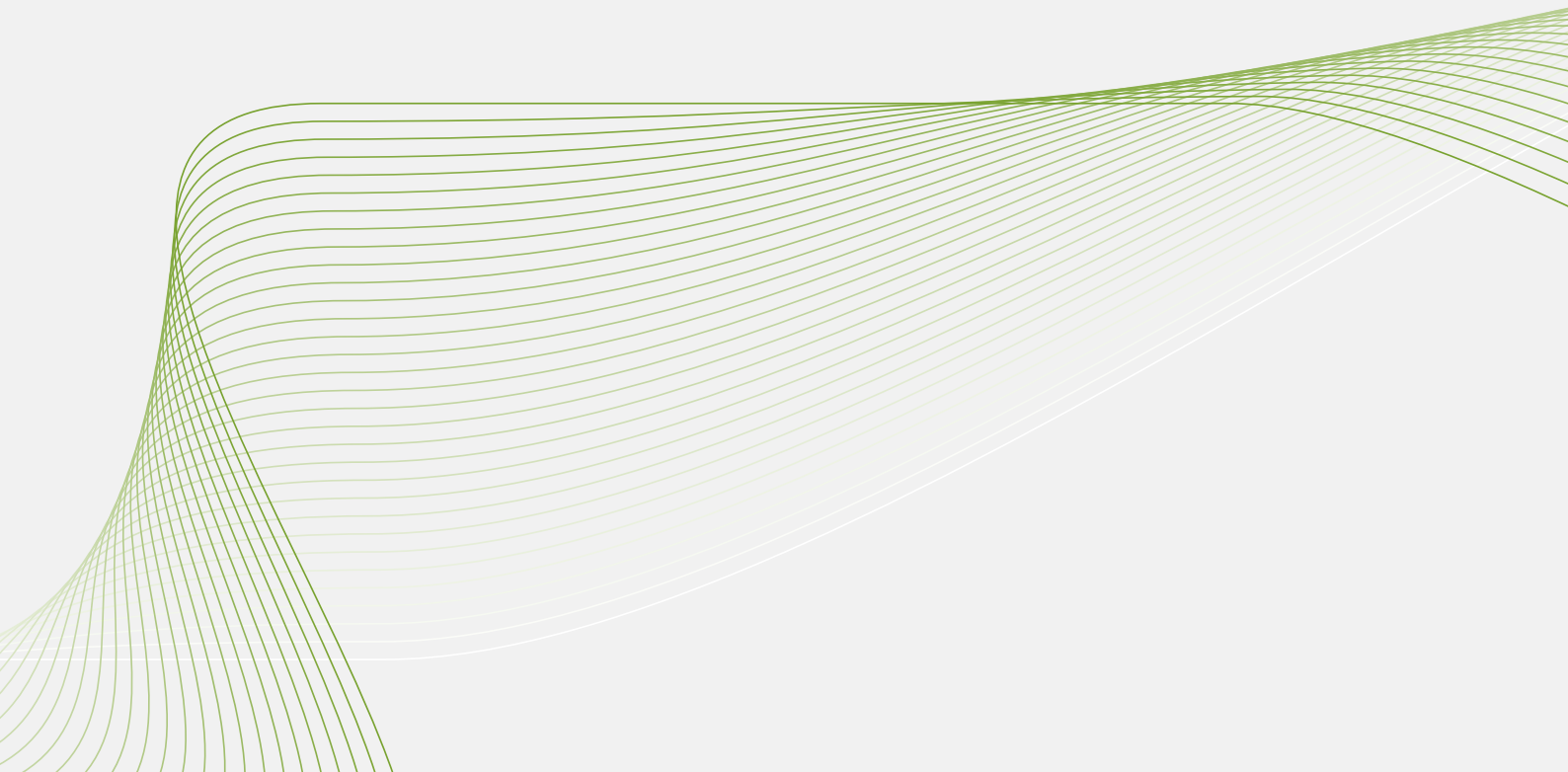
This paper is intended to serve as an educational tool for circulation among non-quantum experts within financial entities. It provides a summary of the emerging landscape and proposes a set of collective next steps as financial entities endeavour to understand, prepare for, and ultimately transition to systems that are resistant to quantum attacks. The recommendations outlined herein reflect both the publicly available guidance, and the industry concerns shared during the GFMA sessions on preparing for quantum readiness.

[1] FS-ISAC, Post Quantum Cryptography ; Post Quantum Cryptography Resources

Summary

Financial services must start preparing for a post-Quantum future now, not when the technology arrives at scale. Multiple authorities signal the **2030–2035** window as the period when **Cryptographically Relevant Quantum Computing risk** becomes operationally material. For banks, this necessitates that mitigation planning be largely complete within the next 2-3 years to ensure that vulnerable systems are fully upgraded in time, with critical systems transitioned several years earlier. Failure to act promptly risks exposing banks' digital infrastructures to both future and retrospective breaches.

Positively, although the technology is still evolving, there is increasing clarity on how financial services should approach the transition to post-quantum cryptography. This paper serves as an educational tool to raise internal awareness across banks' operations, business lines, and management levels. It identifies the key risks that quantum computers could pose to cryptography, the timeframes by which these risks are expected to materialise, and how public sector bodies are collaborating with industry to ensure a successful migration.



Key points include:

- **Quantum technologies are already presenting financial entities with new forms of risk**: "Harvest Now, Decrypt Later" attacks are on the rise, putting today's data at risk of future exposure, and requiring a proactive cryptographic migration.
- **Timelines for quantum transition are tighter than many suspect:** Some regulators are warning publicly that firms should have already started their implementation of PQC, with all advising that migration planning should be completed by either 2027 or 2028.
- **Firm's encryption protections need to be overhauled to remain intact for PQC**: A phased, risk-based approach, supported by standards like NIST FIPS 203 – 205 (ML-KEM, ML-DSA and SLH-DSA) and aligned with global protocols, is emerging as the widely accepted best practice across jurisdictions.
- **Financial entities often operate within intricate and multifaceted environments:** These environments include a wide array of systems, applications, and platforms, each with its own set of cryptographic protocols and requirements. Mapping out all these components to create a comprehensive inventory is a detailed and labour-intensive task.
- **Many financial entities rely on third party vendors and suppliers for various services**: Ensuring that these external partners are aligned with the institution's cryptographic standards and are prepared for the quantum transition requires thorough communication and coordination.
- **There are a number of initiatives supporting industry to put their migration plans into practice:** GFMA will continue supporting members by coordinating shared learning, monitoring regulatory developments, and showcasing implementation tools.
- **Regulatory pressure can help drive forward the industry as a whole**: we stress however this should not take the form of new regulation, but rather supervisory attention during resilience testing, in IT Questionnaires and in ongoing inspections.

Part A: The Risks of Quantum

Understanding the Threat Landscape

Quantum Computing represents a milestone in computing technologies. The modern concept of quantum mechanics in physics was first introduced in 1901 by physicist Max Planck. Unlike classical computing, which relies on electric signals and binary bits to perform calculations, quantum computing uses the properties of subatomic particles and quantum bits (qubits).

Qubits can exist as a conventional binary state, either 0 or 1, but can also occupy as a superposition, where it simultaneously represents both 0 and 1. Combined with quantum entanglement, where multiple qubits are correlated within a register, this dramatically enhances computational power. Consequently, quantum computers are capable of performing complex calculations at speeds far beyond classical or today's computers. This capability enables systems, and those who manage them, to process vastly greater volumes of data, at unrivalled speeds, to solve problems across multiple levels in parallel.

These advances will deliver significant benefits for industry, from the speed and efficiencies of enhanced computational capabilities to the optimisation of data handling[2]. However, the broader adoption of quantum technologies will also introduce risks, particularly through their potential misuse by cyber criminals and other malicious actors. Quantum technology will enable such actors to circumvent existing risk management safeguards and protections, access sensitive systems and databases, and decrypt previously encrypted information, rendering current cryptographic methods largely obsolete.

To illustrate the scale of the threat, the US National Institute of Standards and Technology (NIST) has warned that Cryptographic Relevant Quantum Computers (CRQC) will be capable of breaking widely deployed public key cryptosystems, such as RSA (Rivest–Shamir-Adleman encryption algorithm) and ECC (Elliptic Curve Cryptography)[3]. These cryptographic protocols are foundational to securing modern digital communications and are used extensively across industries.

In practical terms, the Quantum Safe Financial Forum (QSFF – the joint EU industry forum with Europol) has highlighted that this will result in a range of new attacks vectors for banks[4]. Cyber criminals and malicious actors may exploit quantum computing's ability to break cryptographic protections to:

- Recover private authentication keys
- Create fake credentials
- Sign malicious code
- Manipulate signed documents
- Create fake documents with valid signatures

What is more, quantum technologies pose a risk of long-standing digital infrastructures to both future and retrospective breaches. A notable example is the threat of "*Harvest Now,*

[2] WEF: Quantum Technologies Key Strategies and Opportunities for Financial Services Leaders, 2025
[3] NIST, p.10. Available at: https://doi.org/10.6028/NIST.IR.8547.ipd
[4] Quantum Safe Financial Forum - A call to action | Europol, February 2025

Decrypt Later" (HNDL) attacks, in which encrypted data is stolen today with the intention of decrypting it once quantum capabilities become available.

Further, the risks associated with quantum computing have wider repercussions. As financial institutions increasingly rely on technology providers as suppliers, the threat can present itself both directly at the bank and indirectly, through the supply chain. Of particular concern, recent surveys[5] indicate that many providers are underestimating the threats emanating from quantum technologies.

Being aware that the clock is ticking.

Predicting when malicious actors will begin to harness and deploy quantum technologies at scale is, arguably, more of an art than a science. Yet, there is growing consensus among US, EU and UK authorities (see figure below) that 2035 is the point by which, the risks will have matured to the extent that traditional encryption of at-risk systems and databases will be largely insufficient. This deadline originated in the work of the US NIST[6] and underscores that the challenge facing industry will materialise in the short–medium term, and is not a longer-term pitfall that is sometimes anticipated.

In part, the perception of quantum computing as a longer-term challenge is the varying timeframes by which most banks are seeking to internally adopt these technologies. Typically, the sector views quantum computing as an opportunity which will not materialise for 10 years or longer. Yet, this trajectory is not the one which firms must bear in mind when considering the risks to encryption realized by CRQCs and the speed with which to manage its risks. The upgrades associated with migrating to a quantum-safe environment is a process which demands a much earlier starting point, and significant action in the short term.

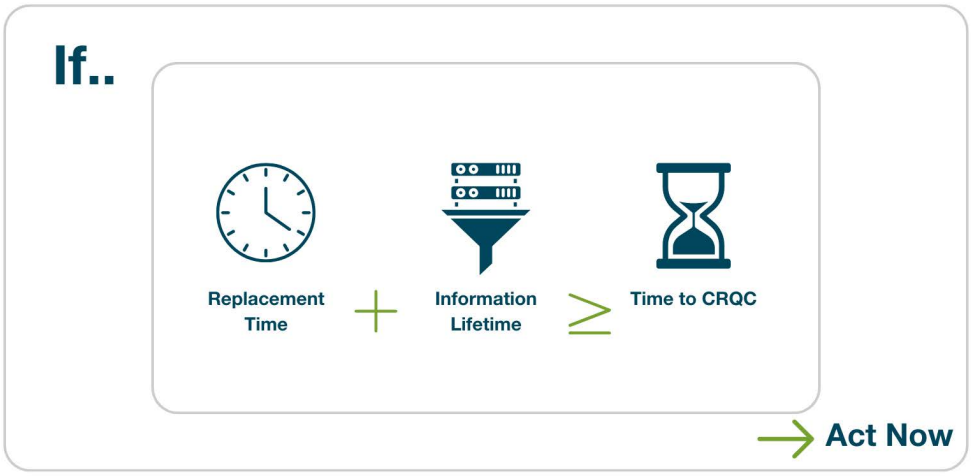
Mosca's Theorem[7]

This is where Mosca's Theorem becomes particularly relevant. The theorem provides a useful framework for assessing when to begin mitigating quantum risks. It states that organisations must act well before a quantum computer is capable of breaking today's encryption. Suggesting that if the sum of the time it takes to replace vulnerable systems plus the timeframe by which data needs to remain secure, exceeds the estimated time to Cryptographically Relevant Quantum Computers, then action must begin now.

[5] Fischer, H.-P., Hagemeier, D. H., Damm, D. F., & Lochter, D. M. (2023). Market Survey on Cryptography and Quantum Computing [Review of *Market Survey on Cryptography and Quantum Computing*]; BSI Bund & KPMG, Market Survey on Cryptography and Quantum Computing, 2023 *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.pdf?__blob=publicationFile&v=3*

[6] Moody (n 1) 20

[7] Michelle Mosca, professor of University of Waterloo, Canada



For banks, this has profound implications: proactive migration to quantum-safe architectures is not a future problem but a present operational necessity. Inaction during this window could compromise sensitive data and lead to systemic cryptographic failure across critical infrastructures. This has led to the emerging plethora of quantum migrations plans which set out step-by-step how best to approach the transition:

- WEF/FCA 2024: Joint Publication on a Quantum Security for the Financial Sector[8]
- The CMORG *Guidance for post quantum cryptography*[9]
- The QSFF/Europol *Call for Action*[10]
- UK NCSC *Timelines for migration to post-Quantum cryptography*[11]

[8] Beato, F., Moschetta, G., Avramovic, P. and Markha, C. (2024). *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*. [online] WEF in collaboration with the FCA. Available at: https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

[9] https://www.cmorg.org.uk/sites/default/files/2025-06/CMORG%20-%20Guidance%20for%20Post-Quantum%20Cryptography%20-%20April%202025%20-%20TLP%20CLEAR%20%281%29.pdf

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf

[11] UK NCSC *Timelines for migration to post-Quantum cryptography*; https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

Part B: Migrating to Quantum Readiness

The transition to PQC has led to policymakers both identifying a set of principles which should guide the industry a whole and developing a set of practical next steps and recommended actions to be taken by individual entities. Collectively these efforts provide the baseline for firms' future quantum migration plans.

Migration Principles

The joint work of the World Economic Forum and the UK's Financial Conduct Authority has significantly shaped the financial services sector's outlook on quantum. In a joint report published in 2024[12], the WEF and FCA identified four key principles to guide the overall approach:

- **Reuse and Repurpose:**
  Leverage existing tools, frameworks, and governance mechanisms, such as current cryptographic management systems, rather than building new infrastructures from scratch.
- **Establish Non-Negotiables:**
  Define clear, baseline requirements that are customer-centric, technology-neutral, and outcome-focused to ensure systemic security and interoperability.
- **Increase Transparency:**
  Encourage open sharing of strategies, threat intelligence, best practices, and evidence-based insights among financial institutions, regulators, and stakeholders.
- **Avoid Fragmentation:**
  Promote harmonised global approaches to regulation and industry practices to prevent inconsistencies across jurisdictions.

In addition, the report emphasised that PQC migration should mirror well established best practices from broader cyber risk management. This includes the need to identify internal vulnerabilities, engage with external partners on interdependencies, leverage technical standard setters and view the migration process as an iterative process which must be monitored and enhanced on an on-going basis.

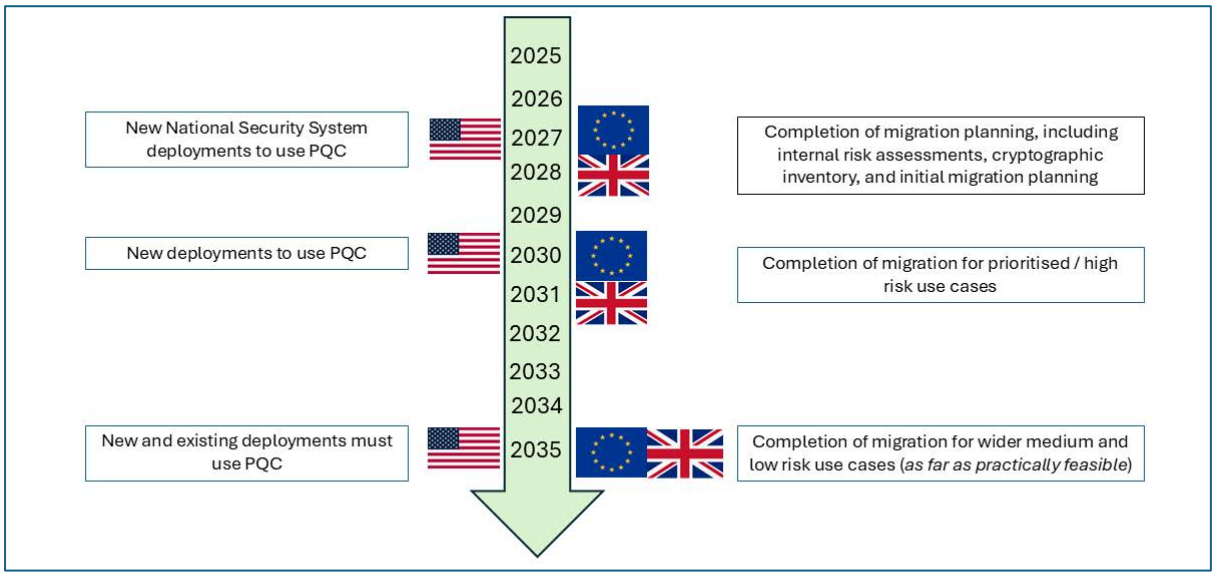
Entity Level Migration Plans

The above principles-based guidance provides the basis for each financial entity to establish their own PQC migration plans, and such extensions have again been the focus of recent collaboration between industry and public authorities. Overall, a phased, risk-based approach is emerging as recommended best practice, with several agencies and bodies coalescing around the following timeframes as the key transition milestones:

---

[12] Beato, F., Moschetta, G., Avramovic, P. and Markha, C. (2024). *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*. [online] WEF in collaboration with the FCA, p.9. Available at: https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

EU/UK/US Timeframes for Quantum Migration[13]



The milestones typically culminate in financial institutions completing their transition plans to PQC by 2035, and such a timeline again illustrates the growing awareness of the need to confront now the future world of quantum threats.

The recent work by industry and public bodies has also helped to extrapolate the individual steps for firms and identified a general prioritisation. Partnerships such as the UK's Cross Market Operational Resilience Group (CMORG) and the EU-backed Quantum Safe Financial Forum (QSFF) have built out the necessary steps for individual banks, covering:

1. **Cryptographic Inventories:** Identification of quantum-vulnerable systems and databases, maintaining the inventory as part of general IT asset management. The operational burden behind this step should not be underestimated and is likely to take years to fully complete. Further, in order to undertake the inventory, financial entities must scope and define a set of internal parameters given that no inventory can provide 100% coverage. Awareness of how peer banks across the industry are approaching their own inventories can be valuable to ensure that no major gaps are at risk of emerging.

2. **Risk Assessments;** Development of internal frameworks by which to rank the level of risk, for example depending on the value of the underlying data. It is recommended firms build upon existing cyber risk mapping efforts, in line with WEF/FCA *Reuse and Repurpose* principle. This should recognise that data sensitivity can be time-variant, with long-lived confidential data likely to require periodic re-classifications. Part of the challenge for financial entities will also be identifying legal friction points which could impact the risk weighting, for example the impact of GDPR obligations on certain types of data.

[13] QSFF /Europol Call for Action 2025: https://www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf

3. **Prioritisation of quantum upgrades:** This is in line with the WEF/FCA timeframes for the sector, which identified 2030/31 as the cut-off for high priority, critical functions, and 2035 as the date for all other upgrades. With many jurisdictions creating enhanced operational resilience requirements around the criticality of the functions or data, the roll out of quantum upgrades should likewise be made on a phased, risk-based approach.

4. **Remediation**: including coordination of the different stakeholders, across financial institution group structures and the vendor supply chain. The latter represents a major concern, given how early market research suggests a very low level of awareness of quantum risk across many tech suppliers and other supply chain providers[14]. This backdrop will require sustained cross-industry action to meaningfully shift the dial and ensure a fully resilient ecosystem with no potentially exposed underbellies.

One of the more complex early steps lies in the discovery and inventorying of cryptographic assets. Without full visibility of the systems and data which rely on at-risk encryption protections, mitigation efforts may be partial and ineffective, especially given the legacy infrastructure and deeply interlinked infrastructure typical across a financial institutions' group structures. This foundational step sets the stage for structured migration planning.

There is also important advice for financial entities regarding the governance to oversee and drive forward the migration plan as a comprehensive programme (see section on *Immediate next steps*).

[14]BSI Bund & KPMG, Market Survey on Cryptography and Quantum Computing, 2023 *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.pdf?__blob=publicationFile&v=3*

Leveraging the Emerging Global Standards

The use of global standards presents a vital opportunity to build consistency and efficiency into the migration, especially with regards to the above Step 3. The NIST PQC suite offers the foundation for technical implementation, while international coordination efforts, such as those led by Interpol and ISO help create an aligned global approach. Financial institutions are encouraged to integrate these standards into their planning to reduce fragmentation and accelerate transition readiness.

Given the scale of the challenge, firms are particularly encouraged to take account of the PQC standards being driven by the US NIST, including FIPS 203, 204, and 205 which were all published in 2024[15]:

- *FIPS 203: CRYSTALS-Kyber (ML-KEM)*
  A key encapsulation mechanism (KEM) for secure key exchange, intended to replace RSA (Rivest - Shamir - Adleman) as one of the most widely used public-key cryptographic algorithms) and Elliptic Curve Diffie-Hellman (ECDH).
- *FIPS 204: CRYSTALS-Dilithium (ML-DSA)*
  A digital signature scheme offering strong security and efficiency; designed to replace current standards like RSA and ECDSA (Elliptic Curve Digital Signature Algorithm).
- *FIPS 205: SLH-DSA (SPHINCS+)*
  A stateless hash-based digital signature algorithm which serves as a conservative backup with different cryptographic assumptions.

These standards, which are only the first batch from NIST, and which can be adopted as hybrid cryptographic algorithms will likely form the basis of future global alignment efforts, and early adoption may reduce the burden of compliance.

[15] https://csrc.nist.gov/news/2024/postQuantum-cryptography-fips-approved

Part C: Next Steps for Financial Entities and Priorities for Cross Industry Action in 2025/6

In order to take forward and implement the Quantum Migration Plans set out in Part B, a number of practical steps have been identified by GFMA as part of a mini-series of roundtables with the stakeholders on Page 6 of this report. These can be broadly divided into:

A. Immediate next steps for firms before initiating any migration
B. Collective priorities for cross industry action.

Immediate Next Steps for Financial Entities

There is growing consensus amongst policymakers and industry groups that there are at least three immediate next steps for financial entities, which can be undertaken as procedural points of process in order to unlock the above substantive components of Quantum Migration:

- Governance
- Education & Awareness
- Contingency Planning

1. Governance

First and foremost is the issue of governance. Institutions are encouraged to establish internal accountability mechanisms for quantum migration, supported by cross-functional leadership and reporting. The WEF and FCA highlight that leveraging existing cybersecurity oversight mechanisms, rather than creating new governance layers, supports smoother implementation and executive visibility[16]. Repurposing existing cyber resilience and governance frameworks to incorporate PQC migration efforts also minimises new overhead while maintaining regulatory confidence. To ensure internal traction, secure funding and executive sponsorship, it is recommended this is also framed in business terms, leaving executives with a clear understanding of why these matters and the cost of inaction.

Strong governance can further help ensure that the migration to PQC does not become a tick box compliance but an opportunity to future-proof financial entities' infrastructure. The financial services information sharing and analysis centre (FS-ISAC)[17] flags that key

[16] Beato, F., Moschetta, G., Avramovic, P. and Markha, C. (2024). *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*. [online] WEF in collaboration with the FCA, p.9. Available at: https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

[17] *Building Cryptoagility in the Financial Sector*. [online] FS-ISAC. Available at: https://www.fsisac.com/typ-pqc-crypto-agility-paper?submissionGuid=5056d751-52bc-4ac0-b37c-46d11b984d95.

to this is building broader cryptographic agility into quantum planning, for example embedding within this process post quantum authentication.

In addition, regulatory frameworks such as the EU's Digital Operational Resilience Act (DORA) and PCI DSS 4.0 (which comes into force in 2025), are already raising expectations for cryptographic governance. Embedding quantum readiness into these ongoing compliance efforts can reduce duplication and ensure firms stay ahead of emerging supervisory expectations.

2. Education & Awareness

Going forward, senior leadership must additionally ensure that there is internal education across the wider workforce of both the risks and the implementation of transition measures. The topic to date has often been framed as theoretical or academic, which can hinder executive engagement and resourcing.

A layered approach, proportionate to the technical expertise of the team or function in question, is key. Bodies such as the UK's CMORG and QSFF have been encouraging industry to build different levels of awareness - from high-level strategic understanding for senior management, to more technical readiness for IT, risk, and compliance teams. Such an approach will help secure early buy-in, reduce friction during implementation, and position the organisation to respond confidently to regulatory nudges or supply chain pressures.

Without early exposure to available tools and approaches, firms risk delays in planning, vendor selection, and implementation when cryptographic transition pressure intensifies. Cryptographic migrations have historically taken decades, for example, even now, only around 70% of internet traffic is TLS 1.3 compliant[18]. Addressing this behavioural and operational inertia will require ongoing communication, targeted education, and strong leadership commitment.

3. Contingency planning

The word of warning from all authorities active in this space has been that, drawing on past experiences such as Y2K, indications are it will take banks longer than anticipated to transition, and that this should be seen as an iterative process, with no end-date to enhancements. Even with early preparation, the scale of remediation, interdependencies, and third-party reliance means transition timelines will be pressured. Institutions should consider interim risk mitigation measures, in parallel with their long-term migration planning.

[18] https://www.ssllabs.com/ssl-pulse/

Priorities for cross industry action in 2025/26

As the transition to post-quantum cryptography moves from identification of the migration plans to its implementation, it is clear that several core roadblocks or common challenges will require cross-industry action, and potentially central leadership. While some of these may only emerge over time, as PQC transitions mature, a number of issues have already come to light.

Drawing on the guidance on PQC migration set out in Part B, it is clear that cross-industry work and coordination will be required on at least the following areas:

- **Alignment in Inventorying At-Risk Systems and Algorithms:** Ensuring industry is aligned in the inventorying of systems and algorithms vulnerable to quantum threats, in order to prevent the emergence of gaps.

- **Facilitation of Statutory Requirements:** Determining how financial institutions are meeting statutory requirements, particularly regarding sensitive data, as part of internal risk assessments.

- **Regulatory Divergence on Critical Functions:** Assessing the extent to which differences in regulatory definitions of critical functions is impeding firms in upgrading their systems based on their criticality.

- **Engagement with Technology Providers and Subcontractors:** Evaluating how the sector's technology providers and subcontractors are addressing quantum security, and identifying further steps to galvanise action in sub-sectors that are progressing too slowly, or are especially critical due to interdependencies.

GFMA remains confident that the bulk of the above challenges can be redressed through public-private collaboration, but there may be times where regulatory "nudges" may be required or could play a useful role in accelerating adoption, particularly in systemically important areas such as payments infrastructure. It is stressed though this does *not* amount to new regulations, as the existing frameworks provide the tools required. Recent experience from the EU AI Act demonstrates the risks in creating new technology-specific regulation which cuts across and duplicates existing obligations. Instead, authorities should adapt and apply those existing risk management tools, such as IT questionnaires, resilience testing and supervisory inspections, to ensure that there is ownership on common pain points and interdependencies. In assessing whether industry participants are progressing with sufficient pace, any supervisory action should focus on the maturity of a firm's documented path towards PQC, rather than binary "compliant"/"non-compliant" judgements.

The challenge for bodies such as GFMA will be in ensuring these nudges are risk-based and proportionate, and that there is alignment, if not standardisation, across international jurisdictions, especially on the interim steps that take us to 2035. This will be the basis of our future engagement with supervisors and regulators in order to avoid a mixture of standards and approaches across different markets or jurisdictions. We look forward to working with policymakers and leveraging their role as a convenor for wider industry action.

Conclusion

The window to act is narrowing. Even though the real impact of quantum computing still lies ahead, financial institutions need to engage meaningfully in the very near future. Those who do so will not just mitigate future risk but tackle threats already in play. Firms that begin early will be better placed to influence emerging standards, shape vendor relationships, and embed cryptographic agility at the heart of their systems.

This paper has mapped out the foundations for sector- wide transition, grounded in various public-private collaborations and shared learnings. The alignment across policymakers and industry demonstrates how the steps for financial entities are now well documented and widely recognised but further exploration can identify how and where each side can continue to help driving emerging practice.

Appendix – Checklist of Actions for Financial Entities

Immediate Next Steps

1. **Establish governance and ownership**
    - ✓ Appoint a lead function or taskforce to oversee quantum readiness efforts.
2. **Educate internal teams and raise awareness**
    - ✓ Provide awareness training for security architects, IT ops, and compliance teams.
    - ✓ Involve legal, compliance, risk, and technology teams and senior management.
3. **Understand regulatory expectations as baseline for contingency planning**
    - ✓ Monitor updates from authoritative bodies and standard setters on post-quantum cryptography (PQC) transition.
    - ✓ Map readiness against operational resilience and DORA/GDPR principles.

Mapping your Migration Plan

4. **Conduct a cryptographic inventory**
    - ✓ Identify where and how cryptographic algorithms are used across systems, applications, and data flows.
    - ✓ Classify cryptographic assets based on sensitivity and lifespan (e.g. long-term confidentiality needs).
5. **Rank critical assets and data**
    - ✓ Highlight systems handling sensitive, high-value, or long-retention-period data.
    - ✓ Evaluate exposure to "harvest now, decrypt later" scenarios.

Implementing your Migration Plan

6. **Deliver a PQC transition plan, based on the criticality assessments**
    - ✓ Set timelines, milestones, and budget for phased migration, prioritising critical functions first.
7. **Leverage technical standards**
    - ✓ Use the work of the NIST and other standard setters as part of the upgrades to encryptions

8. **Assess third-party dependencies**

   - ✓ Catalogue vendors, platforms, and outsourced services that use or manage cryptography.
   - ✓ Include cloud providers, software vendors, (third parties) etc

9. **Identify opportunities to embed crypto-agility mechanisms**

   - ✓ Ensure systems can switch cryptographic algorithms without major redesign. (In line with Reuse and Repurpose Principle mentioned previously).

Engage with peers on a quantum ready ecosystem

10. **Participate in industry collaboration**

    - ✓ Engage with industry groups, regulators, and tech providers on joint readiness efforts to understand if you are aligned in the inventorying of systems and algorithms at risk from quantum
    - ✓ Undertake a collective push with tech providers and subcontractors to ensure quantum-safe supply chains

11. **Support industry-wide efforts to standardise regulatory interventions**

    - ✓ Join industry conversations on managing regulatory divergence for example over the definition of critical functions and the need for regulatory nudges within resilience testing.

Contacts

Allison Parent
Executive Director
GFMA
aparent@global.gfma.org

Marcus Corry
Director
AFME
marcus.corry@afme.eu

The GFMA represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The Global Financial Markets Association ("GFMA") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe ("AFME") in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association ("ASIFMA") in Hong Kong and Singapore, and the Securities Industry and Financial Markets Association ("SIFMA") in New York and Washington are, respectively, the European, Asian and North American members of GFMA.

afme/

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

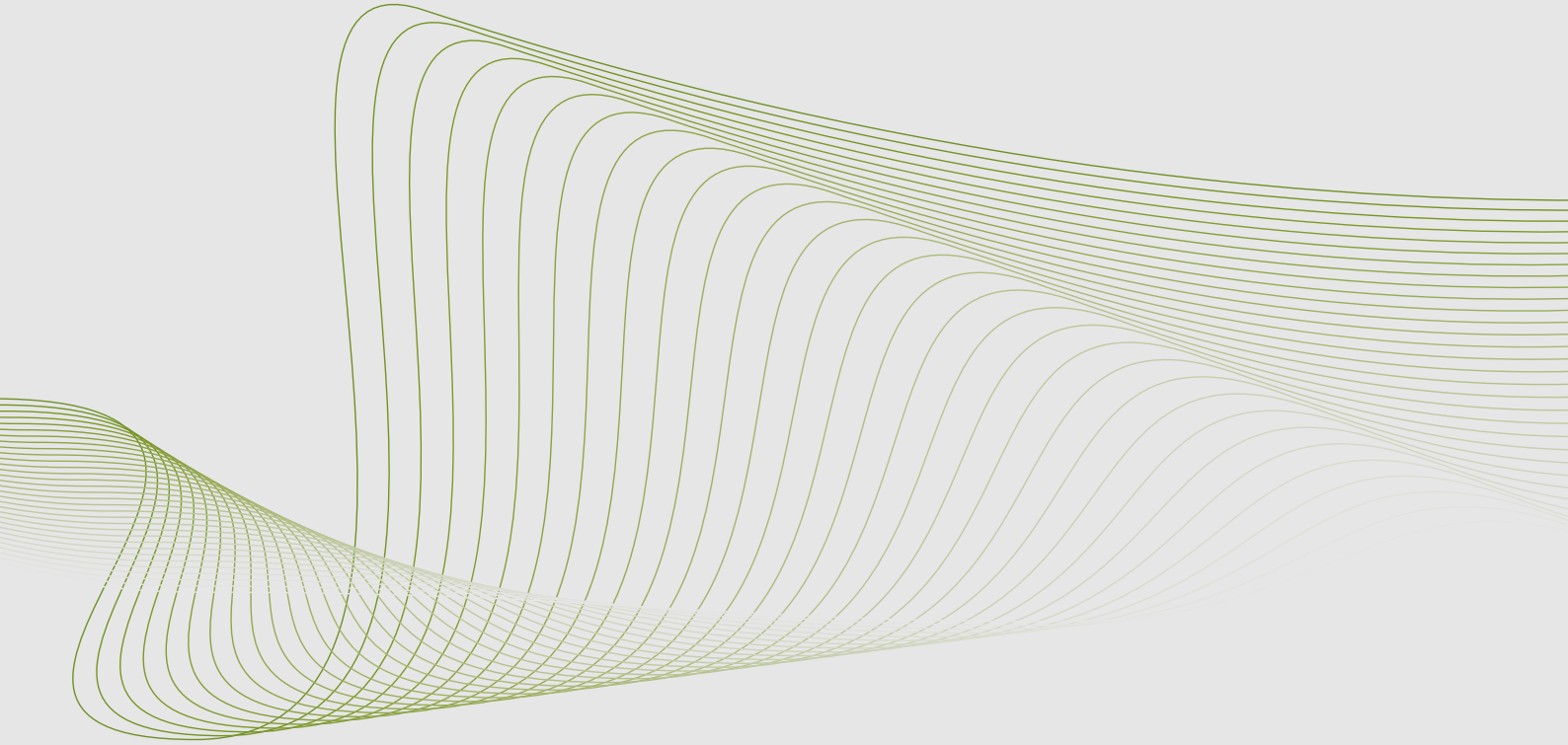
Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)



London Office
Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Press enquiries
Rebecca Hansford
Head of Communications
and Marketing
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Frankfurt Office
Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

AFME is registered on the
EU Transparency Register,
registration number
65110063986-76

www.afme.eu