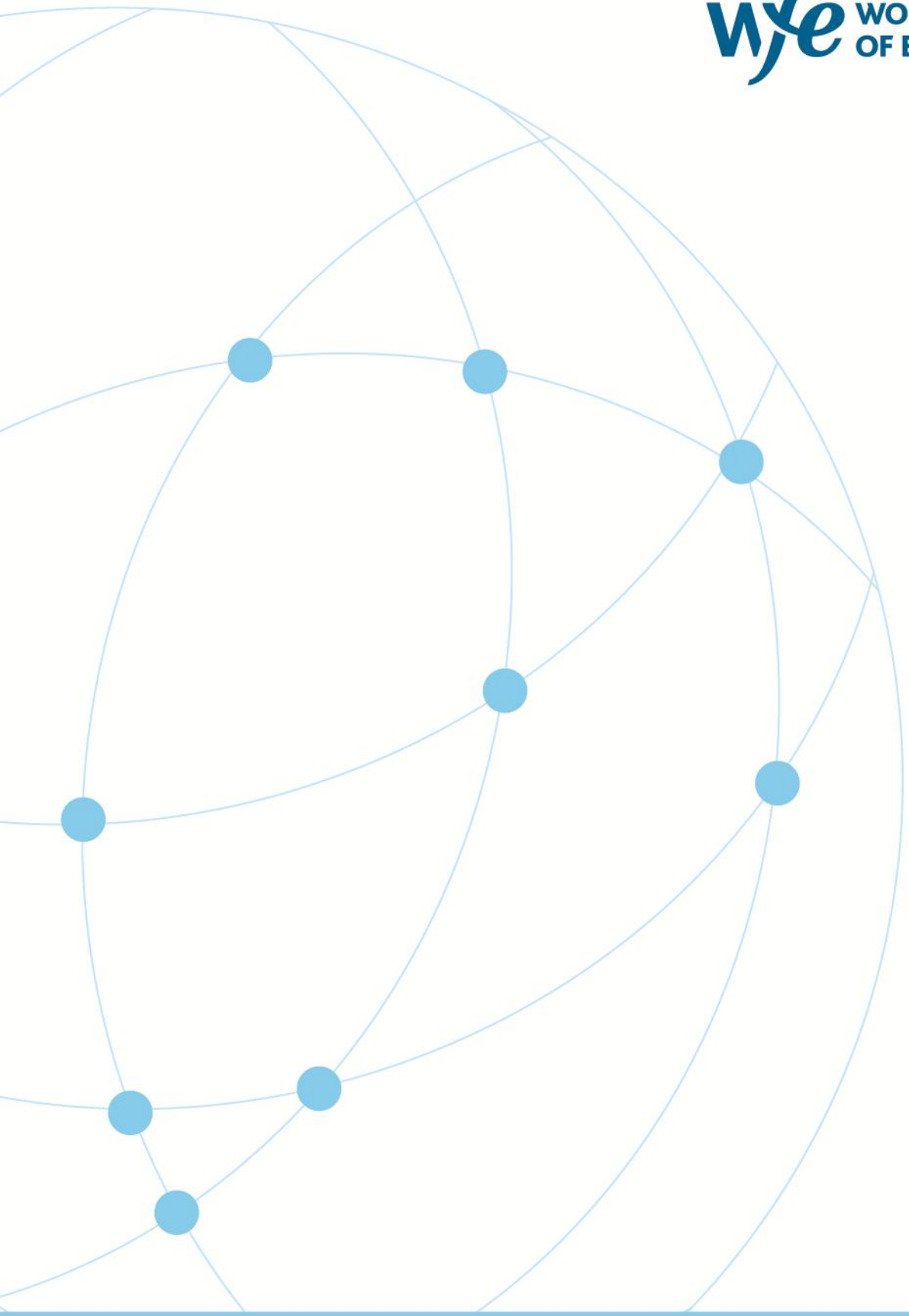
WORLD FEDERATION OF EXCHANGES



Regulatory Signals and Industry Perspectives on Quantum Computing Preparedness

January 2026

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents over 250 market infrastructure providers, including standalone CCPs that are not part of exchange groups. Of our members, 37% are in Asia-Pacific, 44% in EMEA and 19% in the Americas. WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. WFE exchanges, together with other exchanges feeding into our database, are home to over 51,000 listed companies, and the market capitalisation of these entities is over $110 trillion; around $140 trillion (EOB) in trading annually passes through WFE members (at end 2024).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policymakers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policymakers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Regulatory Affairs Manager: csinha@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org

1. Introduction

Global regulators are intensifying their calls for early quantum preparation, though some of this pressure may be premature given the current state of the technology. While Quantum Computing readiness is undoubtedly important, the migration to post-quantum cryptography (PQC) remains a long-term undertaking, and the practical groundwork—planning, asset mapping, and vendor coordination—should be paced appropriately.

From an industry perspective, the approach remains practical: quantum risk is acknowledged as important, but it must be balanced against more immediate operational challenges such as AI-related threats and broader cyber-resilience demands. Even so, WFE members have already begun laying essential groundwork by tracking regulatory developments, engaging with vendors, and starting to assess their cryptographic environments.

This report summarises: (1) the regulatory signals reflected in recent global publications, (2) industry views on practicality and concerns around Quantum Computing preparedness, (3) the challenges to transitioning into a quantum-safe environment, and (4) actions taken by WFE members to date.

2. Regulatory Signals

Major public authorities, standards bodies, and cross-border policy groups have begun issuing guidance, calling for early preparation and coordinated migration to post-quantum cryptography (PQC).

This is driven by two core concerns: (a) long lead times required to upgrade cryptographic systems; and (b) the "harvest now, decrypt later" threat where attackers steal (harvest) encrypted data today to unlock (decrypt) it in a future once more powerful technologies become available to break the encryption.

A summary of the main developments is provided below:

United States – NIST Standards: NIST finalised its first PQC standards in August 2024, including ML-KEM: A public key encapsulation mechanism for **secure key exchanges**.

ML-DSA: A digital signature scheme designed for **secure authentication**, and SLH-DSA: **An additional digital signature scheme** that uses a stateless hash-based signature scheme.[1]

Europe – NCSC, ANSSI, BSI, EU: European authorities advise early preparation and a harmonised approach to PQC migration.[2]

[1] **NIST Releases First 3 Finalized Post-Quantum Encryption Standards**

[2] United Kingdom: National Cyber Security Centre (NCSC) Migrating to Post-Quantum Cryptography (PQC). National Cyber Security Centre ; EU: security agencies of eighteen EU member states released a joint statement Securing Tomorrow, Today: Transitioning to PostQuantum Cryptography urging organisations to transition to international standards such as the NIST algorithms; France: Agence nationale de la sécurité des systèmes d'information (ANSSI) has initiated studies on the

Global Authorities – G7, BIS, WEF, Europol: These bodies emphasise coordinated action, crypto-agility, and risk assessments, signalling growing regulatory impatience.[3]

3. Industry perspectives on practical Quantum Computing preparedness

Feedback from WFE members reveals a substantial gap between regulatory expectations and industry expectations. The WFE Global Cybersecurity working group recently conducted a preliminary survey on the Quantum Computing Preparedness and the results show **competing priorities.** In particular:

- **Generative AI risks** are viewed as far more urgent and immediate, consuming most organisational attention and investment.
- Quantum Computing is seen as a **longer-term threat**, with many firms hesitant to commit resources until clearer timelines or stable standards emerge.

Most of our members estimate a **5–10+ year window** before cryptographically relevant quantum computers (CRQCs) emerge. Several members plan more active assessments next year, once vendor landscapes, tooling, and standards mature. However, some participants note expert opinions warning that quantum capabilities may arrive **earlier than commonly assumed**, prompting earlier preparatory steps.

Across the industry, the prevailing view is that:

- Awareness is improving,
- Deep technical preparedness is limited, and
- Resourcing remains proportionate to a long-term, not imminent, risk.

integration of post-quantum cryptography in protocols, and reflections on recommendations regarding crypto-agility. ANSSI views on the Post-Quantum Cryptography transition. Also refers to NIST
Germany (BSI): Federal Office for Information Security (BSI): Guidance on Quantum technologies and post-quantum cryptography

[3] **BIS Paper**: Quantum computing and the financial system: opportunities and risks October 2024; **G7 Cyber Expert Group**: G7 Cyber Expert Group recommends action to combat financial sector risks from quantum computing; **World Economic Forum**: Quantum-secure financial sector: 4 principles to inform global regulatory approaches Jan, 2024; **Europol** on 7th February 2025 hosted a Quantum Safe Financial Forum (QSFF) event, during which the QSFF has issued a call for action for financial institutions and policymakers, urging them to prioritise the transition to quantum-safe cryptography.

4. Challenges in transitioning to a Post-Quantum-Safe Environment

The transition to PQC is not a simple software upgrade. Industry discussions highlight several structural challenges:

- **Hidden Cryptography and System Complexity:** Most organisations underestimate where encryption is embedded—within databases, file systems, APIs, messaging layers, and legacy systems. Creating a **complete cryptographic inventory** is a nontrivial task and the foundational step regulators expect.
- **Long-Lived Assets and Data Retention:** FMIs operate long-lived systems and retain sensitive data for decades. This amplifies the "harvest now, decrypt later" risk and increases the need for early migration planning.
- **Vendor and Supply-Chain Dependencies:** A critical bottleneck is reliance on external cloud providers, software vendors, and market data suppliers. Even with internal readiness, **weak links in third parties** could compromise security.
- **Algorithm Maturity and Crypto-Agility:** PQC algorithms are still evolving. Organisations fear premature adoption of technologies that may later be deprecated. Ensuring **crypto-agility**—the ability to swap algorithms without major redesign—is essential but costly.
- **Competing Budgetary Pressures**: Operational risks linked to AI, cyber resiliency, ransomware, and cloud dependency often take precedence over quantum investment.

5. Actions by WFE Members to date

Although full-scale migration has not begun, several WFE members have taken early steps:

- **Awareness, Monitoring, and Governance:** Many exchanges are actively monitoring regulatory guidance, vendor progress, and developments in NIST standardisation. Several are incorporating Quantum Computing discussions into **risk committees and cyber governance forums**.
- **Early Risk Assessments:** A minority of members have started preliminary **quantum risk assessments**, typically focusing on long-term data confidentiality and areas with high regulatory exposure.
- **Vendor Engagement:** Some members have begun including **quantum-safe encryption criteria** in procurement and vendor evaluation cycles.
- **Planning for Cryptographic Inventories:** A few exchanges are considering projects to map existing cryptographic assets, recognising this as the first step in any migration roadmap.
- **Collaborative Discussions:** Through the WFE working group, members identified the need for a deeper study on quantum computing's implications for exchanges, a WFE best-practice guide on quantum transition, and a structured roadmap for market infrastructures.

6. Conclusion

Regulators worldwide are issuing increasingly clear and coordinated calls for action on quantum preparedness. While full transition to PQC may be years away, the planning, asset mapping, and vendor engagement required are substantial and long-term.

Industry views reflect a pragmatic stance: Quantum Computing is recognised as a meaningful risk, but one that competes with more immediate operational concerns such as AI-driven threats and cyber resiliency. Nonetheless, WFE members have begun taking foundational steps, including monitoring regulatory expectations, initiating vendor conversations, and exploring cryptographic inventories.

A structured, industry-wide approach—supported by WFE guidance, surveys, and best-practice materials—will be crucial in ensuring the sector transitions to a quantum-safe environment in a coordinated, efficient, and timely manner.