# Following The Roadmap Toward Quantum Security

By **James Burns, Ferdisha Snagg and Andreas Wildner** (February 29, 2024)

James Burns

Ferdisha Snagg

Andreas Wildner

Last month, the World Economic Forum, together with the U.K. Financial Conduct Authority, published a white paper on quantum security for the financial sector.[1]

The white paper aims to inform global regulatory approaches by setting out a roadmap for transitioning to a quantum-secure financial sector.

This article sets out key considerations of the white paper and discusses the implications for firms and lawyers.

**What Is Quantum Computing?**

Quantum computers leverage principles of quantum mechanics to perform calculations or solve problems.

While traditional computers represent information in binary bits — characterized as 0 or 1 — quantum computers use quantum bits or qubits, which can represent both 0 and 1 at the same time. This phenomenon, known as superposition, allows quantum computers to process multiple possibilities at the same time.

Moreover, multiple qubits can exhibit quantum entanglement, a special connection whereby the changing state of one qubit affects others. This generates even more results through interaction of multiple qubits.

These capacities allow quantum computers to solve certain computational problems much more efficiently than traditional computers.

**Risk Inherent in New Technology**

Quantum technology has the potential for enormous benefits but equally represents a significant threat, especially in terms of cybersecurity. For example, quantum computing is expected to dramatically reduce the effectiveness of current encryption methods, especially asymmetric key cryptography.

That this is more than science fiction is apparent from lawmakers across the world, making quantum technologies a strategic priority. Firms in all industries should therefore start paying attention to the emerging regulatory agenda for this technology.

In the U.S., for example, the White House has emphasized in a national security memorandum the need for "a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum-resistant cryptography … mitigating as much of the quantum risk as is feasible by 2035."[2]

The EU too has designated quantum computing as a technology area that is critical for its

economic security.[3]

The European Commission's recent proposal for a new regulation on the screening of foreign investments includes quantum technologies in the list of technologies of particular importance for the security or public order interests of the EU, where foreign investment may affect security or public order through an EU target.[4]

The U.K. government has also emphasized the potential benefits and risks inherent in quantum technologies and has declared quantum technologies as a strategic priority.[5]

**Quantum Technology in the Financial Sector**

Like other information-driven industries, the financial sector safeguards confidential information through cryptography.

This way, firms ensure cybersecurity in their own data architecture, e.g., communications with customers or other firms, identity verification, and securing of stored data, as well as with regard to internet-based connections more broadly and in respect of blockchain platforms.

The mere promise of quantum technology and its ability to break present encryption methods is already incentivizing cyberattacks — so-called harvest now, decrypt later attacks, whereby data is being captured and stored now, to be decrypted later, when more advanced quantum algorithms are developed. Such attacks show that the intention to abuse quantum technology already exists.

The threat of future decryption of stolen data also raises questions about the extent of damages that may materialize at some point in the future, and the litigation risk that flows from that.

Apart from these obvious security concerns, the quantum transition also entails other more subtle challenges, such as skills and knowledge gaps, long-term cybersecurity priority management, and the high-resource intensity of migrating and upgrading complex financial infrastructure.

With a growing focus on these challenges, regulators across different jurisdictions — including the U.S. Financial Industry Regulatory Authority, the European Commission and the U.K. Financial Conduct Authority — have started to think about the implications of quantum computing for firms within their remit.[6]

**White Paper Guiding Principles for Quantum Transition**

The white paper sets out four guiding principles to inform global regulatory and industry approaches.

***Reuse and Repurpose***

Where possible, regulators should use existing tools, techniques and frameworks to address quantum-enabled cybersecurity risks. They should seek to clarify how current frameworks apply to cryptographic management and develop new regulation primarily where gaps are identified in current frameworks.

***Establish Nonnegotiables***

Regulators should lay down overarching requirements that all industry players should meet. These requirements should aim to be customer-focused, technologically neutral and outcome-based, and should allow for risk awareness and an agile approach to cryptography.

***Increase Transparency***

Industry players and regulators should exchange information on their strategies, best practices and approaches, as well as evidence-based, scientific communication about security threats and preventive mechanisms.

***Avoid Fragmentation***

Approaches to regulation and industry action should be globally coordinated, encompassing both mature and emerging markets, to ensure regulatory harmonization and interoperability.

These guiding principles are, of course, in no way binding. Nonetheless, reflecting on them provides important insights regarding possible regulatory developments that may have an impact on firms' operations.

The general approach of relying on an established framework, subject only to a set of nonnegotiable minimum standards, would result in a pragmatic, incremental approach to rulemaking.

A similar approach has been adopted by the U.K. with respect to artificial intelligence and, to some extent, also in the digital assets context.[7]

However, this approach might not suit each legal or regulatory system. For example, with regard to both digital assets and AI, the EU has opted to set up entirely new regulatory frameworks, rather than adjusting existing ones.

These examples show that different jurisdictions may have different levels of appetite for so-called reuse and repurpose approaches, or that such approaches may not be equally effective in all legal systems.

In addition, global regulatory coordination may be difficult to achieve, and therefore there is potential for regulatory fragmentation, cross-border inefficiencies and cybersecurity gaps.

Notably, in a world where data is fast becoming one of firms' most valuable assets, the sharing of insights into quantum technology and security both by public authorities and private actors because of, among other things, intellectual property rights and export and foreign investment restrictions, may not be a given.

That said, the white paper's guidelines are consistent with the regulators' first signals as to future regulation.

The U.S. Financial Industry Regulatory Authority, for example, has requested market participants within its remit to point out where it should offer guidance or modifications to its rules to address the adoption of quantum computing, and how it could foster greater crypto agility within firms to prepare for post-quantum cryptography.

To this end, it has sought input from market participants on the measures they are taking to

enhance safeguards on their encrypted data, including those for quantum resistance.[8]

What remains to be seen is how financial services regulators in other jurisdictions will address the looming quantum security risk, and how global coordination will evolve.

**Laying Out a Transition Roadmap**

The white paper also sets out a roadmap for transitioning to a quantum-secure financial sector. This roadmap envisages four key stages in the quantum transition.

The first stage is one of preparation. As a starting point, this stage will involve raising awareness regarding the benefits, risks and potential impact on business operations of quantum technologies.

Moreover, business should focus on understanding the current state of infrastructure and its quantum readiness and on building internal capabilities and upskilling workforces.

This is followed by a clarify stage, aimed at refining regulators' and the industry's approaches to the quantum-secure transition.

This will involve formalizing engagement and collaboration, e.g., in the form of formal working groups, industry organizations or international regulatory fora.

It should also involve a mapping of current regulations to understand how they capture quantum risks and identify potential gaps. Moreover, organizations should aim to understand the transition, including costs and time frames of transitioning, underlying complexities and financial implications of inaction.

The guide stage — the third stage — largely aimed at regulators and lawmakers, focuses on steering the financial sector toward a successful transition. It will involve addressing regulatory gaps, e.g., through clarificatory guidance or, where necessary, new regulation.

Moreover, technical standards should be translated into practical, actionable implementation plans.

The last stage, transition and monitor, focuses on the implementation of strategies and continuous learning and adapting.

It will require firms to modernize cryptographic management, e.g., through deployment of post-quantum cryptography.

From a regulatory perspective, it might involve iterative regulatory development, reflecting regulators' continuous monitoring and engagement with industry to pick up early innovative signals.

**Key Takeaways**

The quantum transition seems to entail at least two key challenges for firms: That some aspects, such as workforce upskilling and capacity building, may take significant amounts of time, and that the entire transition process can be conducted much more efficiently with the end goal — and intermediary steps — in mind.

In light of that, reflecting on the white paper's roadmap and its implications for firms'

quantum strategy early on may have significant benefits for them.

The goal of the transition is to develop a cybersecurity architecture that is agile while also allowing for quantum security. Agility in this context means catering for the possibility of future cybersecurity threats that may materialize quicker than quantum threats.

This may be done, for example, by incorporating an inventory of systems, solutions and security protocols firms could easily switch between.

Essentially, firms should be doing two things now.

***Quantum Transition***

Firms should think about the quantum transition early, before the technology is widely available and before their transition process will need to be driven by regulatory obligations.

Firms will want to think about how their quantum transition can be implemented in the most efficient and least disruptive way.

To achieve this, they will need to consider how to repurpose and reuse existing practices, tools and processes, and they may wish to work with third-party providers to understand and implement standardized approaches.

Bearing in mind that not all present cryptographic methods are equally vulnerable to quantum-enabled attacks, firms may also wish to explore switching to cryptographic methods that are more quantum secure than, for example, asymmetric key cryptography.

This also involves ongoing monitoring of encryption updates designed to provide enhanced protection through quantum-resistant encryption.

***Prioritize Their Infrastructure***

Firms may also wish to consider prioritizing certain aspects of their infrastructure, especially in light of the threat of harvest now, decrypt later attacks.

To allow effective prioritization, firms should identify the most sensitive aspects of their infrastructure, e.g., where data is handled that is sensitive or integral to operational stability, vulnerable parts of the infrastructure, or infrastructure that is indispensable for the provision of critical business services. This may include compiling a cryptographic inventory.

Firms should be building capacities and upskilling their workforce. This may involve tailored education programs for stakeholders at all levels of organizations, e.g., by partnering with academic and research institutes, and considering collaborative initiatives such as secondment programs and workshops.

Practitioners will be expected to play an important role in this process, including by creating awareness of possible risks and ways to address these.

Advisers will undoubtedly be called upon to advise on key regulatory implications of quantum-related developments, including cybersecurity, data governance, outsourcing and supervisory processes.

*James Burns is a partner, Ferdisha Snagg is counsel and Andreas Wildner is an associate at Cleary Gottlieb Steen & Hamilton LLP.*



[1] The White Paper: https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf.

[2] The White House's National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems.

[3] Commission Recommendation (EU) 2023/2113 on critical technology areas for the EU's economic security: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302113.

[4] Proposal for a regulation on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024PC0023.

[5] UK National Quantum Strategy: https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national_quantum_strategy.pdf.

[6] FINRA, Quantum Computing and the Implications for the Securities Industry: https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing; the Commission's 2024 work programme for European Standardisation;"A Quantum Leap for Financial Services", July 4, 2021: https://www.fca.org.uk/insight/quantum-leap-financial-services.

[7] For an analysis of UK developments regarding the use and regulation of Artificial Intelligence in the financial services sector: https://www.clearygottlieb.com/news-and-insights/publication-listing/artificial-intelligence-in-the-financial-services-sector-uk-regulators-publish-feedback-statement.

[8] See FINRA Report, p. 12.