ALERT MEMORANDUM

Quantum Computing and the Financial Sector: World Economic Forum Lays Out Roadmap Towards Quantum Security

January 30, 2024

Quantum technology is seen as having the potential to revolutionize many aspects of technology, the economy and society, including the financial sector. At the same time, this technology represents a significant threat to cybersecurity, especially due to its potential to render most current encryption schemes obsolete.

With a view to meeting these challenges, the World Economic Forum, in collaboration with the UK Financial Conduct Authority (the "**FCA**"), has published a White Paper on "Quantum Security for the Financial Sector" (the "**White Paper**").[1] The White Paper aims to inform global regulatory approaches by laying down four guiding principles and setting out a roadmap for transitioning to a quantum-secure financial sector.

This alert memorandum sets out the key considerations of the White Paper and tangible actions financial sector businesses should consider taking, as well as broader regulatory developments across the US, the EU and the UK.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

LONDON

Ferdisha Snagg
+44 20 7614 2251
fsnagg@cgsh.com

Andreas Wildner
+44 20 7614 2248
awildner@cgsh.com

[1] The White Paper is accessible here.

I. Context

Quantum computers are a new type of computing device that leverages principles of quantum mechanics to perform calculations, or solve problems, that could not be solved by traditional computers.[2]

Quantum technology is regarded as having a wide range of possible applications with the potential to bring enormous benefits, including in the financial services sector. However, it also represents a significant threat, especially in terms of cybersecurity. In fact, the emergence of "Harvest Now, Decrypt Later" attacks (whereby data is being captured and stored now, to be decrypted latershows that the intention to abuse quantum technology already exists, when more advanced quantum algorithms are developed)[3] shows that the intention to abuse quantum technology already exists. The quantum transition also entails other complexities, such as skills and knowledge gaps, long-term cybersecurity priority management and the high resource intensity of migrating and upgrading the complex financial infrastructure.

The White Paper aims to foster a coordinated, global approach for managing the transition towards an economy that is quantum-secure while minimizing disruption and inefficiencies of such transition.

II. White Paper

1. *Guiding Principles*

The White Paper sets out four guiding principles to inform global regulatory and industry approaches:

i. **"Reuse and repurpose"**: the first guiding principle emphasizes the importance of making the best use of existing tools, techniques and frameworks to address quantum-enabled cybersecurity risks. For financial institutions, this may involve reusing processes and tools from areas such as vulnerability management. For regulators, this means clarifying, e.g., by way of context-specific guidance, how current frameworks apply to cryptographic management (this is similar to the UK's approach to regulating the use of Artificial Intelligence in the financial sector)[4] and develop new regulation primarily where gaps are identified in current frameworks.

ii. **"Establish non-negotiables"**: this principle calls for the laying down of overarching requirements which all industry players should meet in order to promote the integrity and safety of the financial sector. 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 and the evolving technological landscape.

iii. **"Increase transparency"**: this principle calls for industry players and regulators to exchange information on their strategies, best practices and approaches, as well as evidence-based, scientific communication, about security threats as well as preventive mechanisms.

iv. **"Avoid fragmentation"**: this principle calls for a globally coordinated approach to regulation and industry action, encompassing both mature and emerging markets, that ensures regulatory harmonization and interoperability.

2. *Roadmap*

i. **"Prepare"**: key considerations during this phase involve:

   a. **Raising awareness** regarding the benefits and associated risks of quantum technologies, and the potential impact on daily business operations. For businesses, this may involve tailored education programs for stakeholders at all levels of organizations and sharing perspectives externally to raise awareness

[2] As described in the September 2022 World Economic Forum report "Transitioning to a Quantum-Secure Economy" (accessible here), "*[i]n classical computing, all information is represented in bits (as 0s and 1s). Quantum computers use qubits that combine 0s and 1s at the same time (called "superposition"). Leveraging the principles of superposition and entanglement (the ability of remote qubits to be correlated to each other), quantum computing enables a new way of storing and processing information. These new building blocks are used to construct quantum algorithms that, in some cases, significantly accelerate the ability to solve computational problems.*" (section 1.1).

[3] See, e.g., the FCA's article "A Quantum Leap for Financial Services", July 4, 2021, accessible here.

[4] For an analysis of UK developments regarding the use and regulation of Artificial Intelligence in the financial services sector, please see our firm's memorandum on the Bank of England's and FCA's Feedback Statement relating to Artificial Intelligence and Machine Learning, accessible here.

across the sector. Regulators should consider knowledge sharing across jurisdictions.

b. **Understanding** the current state of infrastructure and its quantum readiness. Organizations should consider comprehensive reviews identifying 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), including a cryptographic inventory. Businesses should also engage with technology providers and other actors in the supply chain at this stage.

c. **Building internal capabilities** and upskilling workforces, e.g., by partnering with academic and quantum-focused research institutes, and considering collaborative initiatives such as secondment programs and workshops.

ii. **"Clarify"**: this phase aims at refining regulators' and industry's approaches to the quantum-secure transition. It again involves three key considerations:

a. **Formalizing engagement and collaboration**. This may involve promoting unified messaging emphasizing the collective responsibility of the sector, establishing formal working groups and industry organizations (possibly with regulators and other stakeholders as observers) to share insights and build partnerships. Regulators should also engage in discussions via international forums to ensure international alignment.

b. **Mapping current regulations**, i.e., conducting comprehensive reviews of existing frameworks to understand how they capture quantum risks and identify potential gaps. Again, this should involve a cross-jurisdictional perspective, to understand similarities and differences in approaches across different countries.

c. **Understanding the transition**, including costs and time frames of transition, underlying complexities and financial implications of inaction. This may involve modelling exercises, industry-wide impact assessments and discussions with cybersecurity supply chain partners and critical third parties. Regulators could conduct cost-benefit analyses of different approaches, and could also consider bringing together vendors and industry stakeholders to identify common priorities and action plans, e.g., through workshops, sandboxes or hackathon-style events.

iii. **"Guide"**: this phase focuses on steering the financial sector towards a successful transition. Key considerations involve:

a. **Addressing regulatory gaps.** This may involve security guidance from national and international cybersecurity agencies. Regulators should engage with industry and understand practical experiences and perspectives. New regulation should only be introduced where essential, and approaches across jurisdictions should be coordinated to avoid regulatory misalignment.

b. **Translating technical standards into practical, actionable implementation plans.** Global technical standards and open-source projects should be translated into practical applications and implemented across new and existing systems. Industry should work with vendors to understand and implement standardized approaches so as to limit disruptions and minimize operational inefficiencies, and should publicize their transition and integration plans to stimulate progress towards industry best practices. Regulators should work with international standard-setting bodies. The White Paper also recommends developing a map of industry dependency on standards and open-source software to ascertain where action is required, and to consider testing and benchmarking of different approaches and solutions.

iv. **"Transition and monitor":** this phase focuses on the implementation of strategies and continuous learning and adapting. Key considerations include:

a. **Modernizing cryptographic management**, such as through deployment of post-quantum cryptography. Businesses should consider how to repurpose and reuse existing practices, tools and processes (e.g., contemporary DevOps) and how to adopt a cryptographic-agile approach that takes into account future cybersecurity threats that may materialize quicker than quantum threats (e.g., by incorporating an inventory of systems, solutions and security protocols firms could easily switch between).

b. **Iterative regulatory development**, reflecting regulators' continuous monitoring and engagement with industry to pick up early innovative signals. Regulators should adopt forward-looking approaches which are outcomes-focused and flexible enough to adapt to technological advancements. Regulators may also consider merits of incentivizing the transition (being mindful of resources and capabilities of smaller firms).

III. Wider developments

While the White Paper represents an important step in fostering international regulatory developments relating to quantum-related cybersecurity, it is not the first such step.

In the US, for example, the White House, in May 2022, published a National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (the "**US Memorandum**").[5] The US Memorandum emphasizes the need for "*a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum-resistant cryptography . . . with the goal of mitigating as much of the quantum risk as is feasible by 2035*". The US Memorandum notes that the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA) are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions, and that the first sets of these standards are expected to be released publicly by 2024.

In October 2023, the US Financial Industry Regulatory Authority ("**FINRA**") published a report on 'Quantum Computing and the Implications for the Securities Industry' (the "**FINRA Report**"). The report provides an overview of quantum computing technology, potential applications in the security industry (e.g., optimization systems such as for trade-execution optimization, trade-settlement optimization or investment-portfolio optimization; simulation systems such as Monte Carlo simulations; or synergies with artificial intelligence) and potential threats to cybersecurity. It also sets out regulatory considerations for quantum computing, relating to aspects such as cybersecurity, outsourcing and third-party vendor management, data governance; and supervision and controls.

The EU similarly recognizes the potentially enormous significance of quantum technologies. In October 2023, the European Commission published a recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States,[6] which noted that "*[q]uantum technologies have a vast potential to transform multiple sectors, civil and military, by enabling new technologies and systems that make use of the properties of the quantum mechanics*" and listed quantum technologies (including quantum computing, quantum cryptography and quantum communications) as critical technology areas for the EU's economic security.

Building on this recommendation, the Commission's recent proposal for a new regulation on the screening of foreign investments (the "**FDI Proposal**")[7] includes quantum technologies in the list of technologies, etc. of particular importance for the security or public order interests of the EU, where a foreign investment may affect security or public order in more than one Member State or in the EU as a whole through an EU target. Under the FDI Proposal, where an EU undertaking is active in quantum

[5] The US Memorandum is accessible here.

[6] Commission Recommendation (EU) 2023/2113, accessible here.

[7] The Commission Proposal, dated January 24, 2024, 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 is accessible here.

technologies (or other specified sensitive technologies etc.), foreign investments in such undertakings may be subject to authorization requirements.[8]

Lastly, in the UK, the government, in March 2023, published its "National Quantum Strategy",[9] which recognizes the potential benefits of quantum technology for the financial sector, but equally puts emphasis on mitigating risks associated with quantum. Moreover, the FCA, aside from contributing to the White Paper, has been considering quantum technologies as one of its priority topics. Already in 2021, the FCA published an article exploring potential opportunities and challenges that quantum technologies could pose to policymakers,[10] and has since then been monitoring industry research and adoption of these technologies through collaboration with the National Quantum Computing Centre and the Quantum Computing & Simulation Hub. As part of the Digital Regulation Cooperation Forum horizon scanning program, UK member regulators held a symposium in March 2023 on Quantum Information Technologies to understand their potential impact across shared regulatory remits.

…

CLEARY GOTTLIEB

[8] FDI Proposal, Article 4(4)(b).

[9] The UK's National Quantum Strategy is accessible here.

[10] "A Quantum Leap for Financial Services", July 4, 2021, accessible here.