In collaboration with
Financial Conduct Authority (FCA)

WORLD ECONOMIC FORUM

Quantum Security for the Financial Sector: Informing Global Regulatory Approaches

WHITE PAPER

JANUARY 2024

Images: Getty Images

Contents

Foreword

Jessica Rusu
Chief Data, Information
& Intelligence Officer,
Financial Conduct Authority

Jeremy Jurgens
Managing Director,
World Economic Forum

Quantum technology has the potential to revolutionize financial services, improving computation, modelling and fraud detection, but it also poses significant cybersecurity risks. To fully benefit from the sector's transition to the quantum economy era, it is key to address these challenges that could undermine the digital security and foundational elements of the financial sector. These potential systemic disruptions underscore the need for a unified, global and cross-industry approach to quantum security for the financial sector.

Shaping the development of the quantum economy, globally, has been one of the key priorities of the World Economic Forum's Quantum Economy Network since its inception. The network has been fostering public-private cooperation and driving action on key topics such as quantum governance and security.

Balancing innovation with consumer protection is paramount for the Financial Conduct Authority (FCA), as we seek to not only keep pace with technological advances but shape them for maximum benefit while mitigating risks. Initiatives such as the Emerging Technology Research Hub, digital and regulatory sandboxes and the Global Financial Innovation Network demonstrate the FCA's proactive approach to informed policy-making.

The World Economic Forum, in collaboration with the FCA, has been at the forefront of the international dialogue that has led to this paper, gleaning insights from industry, academia, financial authorities, regulators and central banks. This initiative lays the groundwork and provides guidance for more collaborative, harmonized and globally informed quantum security strategies. This initial discussion forms an invitation for ongoing collaboration with stakeholders to ensure that the financial sector is adequately equipped to tackle the security challenges posed by the quantum transition.

Together, we can ensure a cybersecure and resilient financial future for all.

Executive summary

This paper presents four guiding principles and a roadmap to inform global regulatory and industry approaches for a quantum-secure financial sector.

In an era marked by rapid digitalization, the financial sector stands on the brink of a transformation from a digital economy to a quantum economy. Quantum computing promises to revolutionize operations across the financial sector, with the potential to disrupt portfolio management and improve risk management. However, it also comes with challenges, as quantum computing could render most current encryption schemes obsolete, threatening consumer protections and the integrity of digital infrastructures and economies. The severity of these risks, combined with an uncertain timeline to transition to new security models, requires stakeholders to take proactive measures.

Addressing quantum-enabled cybersecurity risks in the financial sector is a complex task, given the sector's legacy infrastructure, the nature of quantum technology, and the interconnectedness of the industry. The global nature of the financial sector and the common threat posed by quantum technology require close collaboration between industry and regulators. Recognizing the need for a coordinated approach, the World Economic Forum, in collaboration with the Financial Conduct Authority (FCA), initiated a dialogue to help the financial sector transition to a quantum-secure future. This effort brought together regulators, central banks, industry players and academia for coordinated roundtables and curated discussions.

This collaborative approach produced four guiding principles along with a roadmap to serve as a blueprint to reduce complexity and align stakeholders' activities. These principles, to reuse and repurpose, establish non-negotiables, avoid fragmentation and increase transparency, are overarching and should inform actions throughout the transition to a quantum-secure economy.

The transition itself is a journey, and this paper provides a four-phase roadmap: prepare, clarify, guide, and transition and monitor. This roadmap will help the financial sector establish a more collaborative, harmonized and globally informed approach, ensuring that the financial sector is well-prepared for the security challenges that the quantum transition poses. This paper establishes the groundwork for future discussions between industry stakeholders and regulatory authorities towards a quantum-secure financial sector.

Introduction

The complexities and impact of quantum technologies on the financial sector require open dialogue between regulatory authorities and industry.

The financial sector is on the verge of a transformation as it begins to leverage emerging and frontier technologies. While the focus remains on technologies such as artificial intelligence (AI), quantum technologies are the next frontier. They offer disruptive opportunities to enhance the sector's capabilities, but also pose challenges for its operations.

> **The quantum economy era is fast approaching and we need a global public-private approach to address the complexities it will introduce. We welcome this opportunity to collaborate with the Financial Conduct Authority to chart the roadmap for a seamless and secure transition for the financial services sector to the quantum economy.**
>
> Sebastian Buckup, Head of Network and Partnerships; Member of the Executive Committee, World Economic Forum

Emerging quantum risks and opportunities in the financial sector

Quantum computers can handle and solve certain complex mathematical problems significantly faster than classical computers. This technology has the potential for disruption and provides financial organizations with the opportunity for competitive advantage. Investments by the financial sector confirm a growing commitment to harnessing quantum innovation, with a projected rise from $80 million in 2022 to $19 billion by 2032,[1] and to reach up to $850 billion over the next 30 years.[2]

This surge in investment is underpinned by the sector's pursuit of advancements in Monte Carlo simulations, portfolio optimization and complex derivative calculations, with the potential to add approximately $700 billion in value by 2035.[3]

While the sector's innovators focus on harnessing these opportunities, it is equally important to prepare for potential quantum-enabled cybersecurity threats.[4] At the core of this quantum dilemma lies the technology's potential to render some current encryption schemes obsolete, threatening the security of digital infrastructures, communications and data.[5] Such a scenario would not only undermine cybersecurity but also erode the foundation of trust and stability upon which financial services operate.

Taking a harmonized approach to quantum security

The severity of quantum cybersecurity risks for the financial sector, coupled with the limited time available to prepare, provide the motivation to act and the opportunity for all financial sector stakeholders to take appropriate, proactive measures.

Several major financial institutions expect quantum computing to significantly disrupt the sector in the next decade and beyond.[6] Furthermore, the emergence of "Harvest Now, Decrypt Later" attack vectors presents a significant current and long-term risk to the financial sector's data security.

While the timeline is still uncertain, leading experts in the field forecast the quantum threat to materialize within the next decade. Governments are advocating for action now to ensure that the industry is ready for the quantum threat by 2035,[7] as highlighted in the United States' (US) National Security Memorandum of May 2022.[8]

This requires action from diverse stakeholders, including industry, regulators, policy-makers and vendors. A recent survey conducted by the FCA highlighted this urgency, as 60% of the respondents from regulatory authorities said they anticipated quantum computing to significantly impact the financial sector within the next seven years. Given the existence of both present and future threats and the extensive time required to transition to quantum-secure systems,[9] industry and regulators must begin taking proactive steps now.

This aligns with recent Forum reports which have emphasized that global regulatory approaches are key drivers to improve cybersecurity towards a quantum-secure transition,[10] and are important guardrails to enable the responsible development of quantum technologies.[11] Regulatory authorities have also highlighted the importance of ensuring global and harmonized regulatory approaches, with 93% of the mentioned survey respondents agreeing that quantum technologies will have significant implications for their regulatory frameworks.[12]

> **Quantum computing presents considerable opportunities but also threats. The financial sector relies heavily on encryption to protect sensitive information, the exposure of which could cause significant harm to consumers and markets. Addressing this requires a truly collaborative effort to transition to a quantum-secure future.**
>
> Suman Ziaullah, Head of Technology, Resilience and Cyber, Financial Conduct Authority

Bringing together industry and regulatory authorities

Ensuring global and interoperable regulatory approaches is a complex task, given the diverse landscape, state of development, and investment and resources available in each jurisdiction. Ongoing collaboration between industry and regulatory authorities is essential to establish clarity and reduce complexity. Such collaboration fosters alignment to mitigate quantum cybersecurity risks, capture benefits and inform regulatory approaches to ensure security and harness the potential value of quantum technologies.

The World Economic Forum, in collaboration with the FCA, initiated an international dialogue, convening regulators, central banks, industry players and academia. This collaborative effort, comprising of coordinated roundtables and curated discussions, brought together industry and regulatory leaders to gather insights and navigate the challenges of transitioning to quantum-secure financial services.

Synthesizing the insights from these discussions, this report provides guiding principles to inform regulatory and industry action while charting a roadmap of actions for a transition towards a quantum-secure economy. The journey towards a quantum-secure financial sector is complex and challenging, yet through collaborative efforts and proactive engagement, it is a journey that the financial sector should embark upon with urgency and resolve.

1 Current landscape

Emerging misalignment in the regulatory landscape, and challenges in the industry, are limiting actions to embark on a quantum-secure transition.

Both public and private sectors are taking initiatives in specific regions, with the US setting a quantum-secure transition milestone for 2035[13] and its National Institute of Standards and Technology (NIST) leading international efforts to establish standards and guidance on post-quantum cryptography solutions by 2024.[14] While governments, regulators and industry are increasingly cognizant of the quantum threat, a tangible action plan to establish global and harmonized regulatory approaches remains elusive.[15] Furthermore, the complexity of quantum technologies poses challenges in several other areas, such as skills and knowledge, policy and guidance, long-term cybersecurity priority management, and the high resource-intensity of migrating and upgrading the complex financial infrastructure.[16]

Regulatory perspective

The regulatory authorities that have taken part in this dialogue have described the landscape as uncertain, with limited international coordination. In various jurisdictions, a lack of regulatory guidance has led to uncertainties for industry regarding how to prepare and manage the emerging quantum cyber risks. These uncertainties are further compounded by divergent governmental approaches and early misalignment across regulatory jurisdictions. Different regions are at varied stages of preparedness, and their approaches to quantum security differ due to size, investment and priorities.

This lack of harmonization poses significant challenges for global entities operating in multiple jurisdictions, adding layers of complexity and compliance burdens. On the other hand, it provides the opportunity to prioritize this issue on the international agenda and to set international guidelines that can be tailored to different jurisdictions to ensure consistency in how different jurisdictions deal with the transition.

Furthermore, the interconnected and global nature of the financial sector means that its security often depends on its most vulnerable points. As such, increased emphasis should be placed on supporting emerging markets and smaller organizations in their transition, ensuring that these financial hubs are also adequately prepared to deal with the quantum-enabled risks.

The novel and complex nature of quantum technologies requires further development in knowledge and capabilities across regulators to create the needed understanding to manage this risk.

Industry perspective

Industry stakeholders highlight challenges stemming from fragmentation and geographical variations in applying global standards. The lack of regulatory clarity hinders vendors' preparedness and reduces investor confidence in the emerging vendor market. The financial sector also faces technological challenges in understanding and implementing various quantum solutions, including post-quantum cryptography and quantum key distribution.

Moreover, financial sector organizations often rely on large, complex digital infrastructure with legacy environments, as well as third parties, for a wide range of services, exposing them to supply chain vulnerabilities and increasing the complexity of integrating quantum-secure solutions. The cost and time needed for a full transition to a quantum-secure environment is vast, and leaders struggle to balance between the increased cyber risk in a complex threat landscape and the long-term quantum-security risks that are yet to materialize.[17]

Discussions throughout this work programme have highlighted regulations as a catalyst for prioritizing and advancing the transition to quantum-secure systems. Balancing short-, medium- and long-term implications of quantum threats requires an approach that avoids excessive regulation while providing clear guidance. Collaboration on an international scale can facilitate the sharing of knowledge, best practices and expertise in implementing different quantum solutions to foster a cohesive approach across jurisdictions.

The current conditions in both the industry and regulatory landscapes highlight the urgent need for increased international collaboration to share knowledge, expertise and experience. This collaboration should involve industry players, regulators, central banks, standards organizations, third-party suppliers and other stakeholders to ensure a seamless transition to a quantum-secure economy.

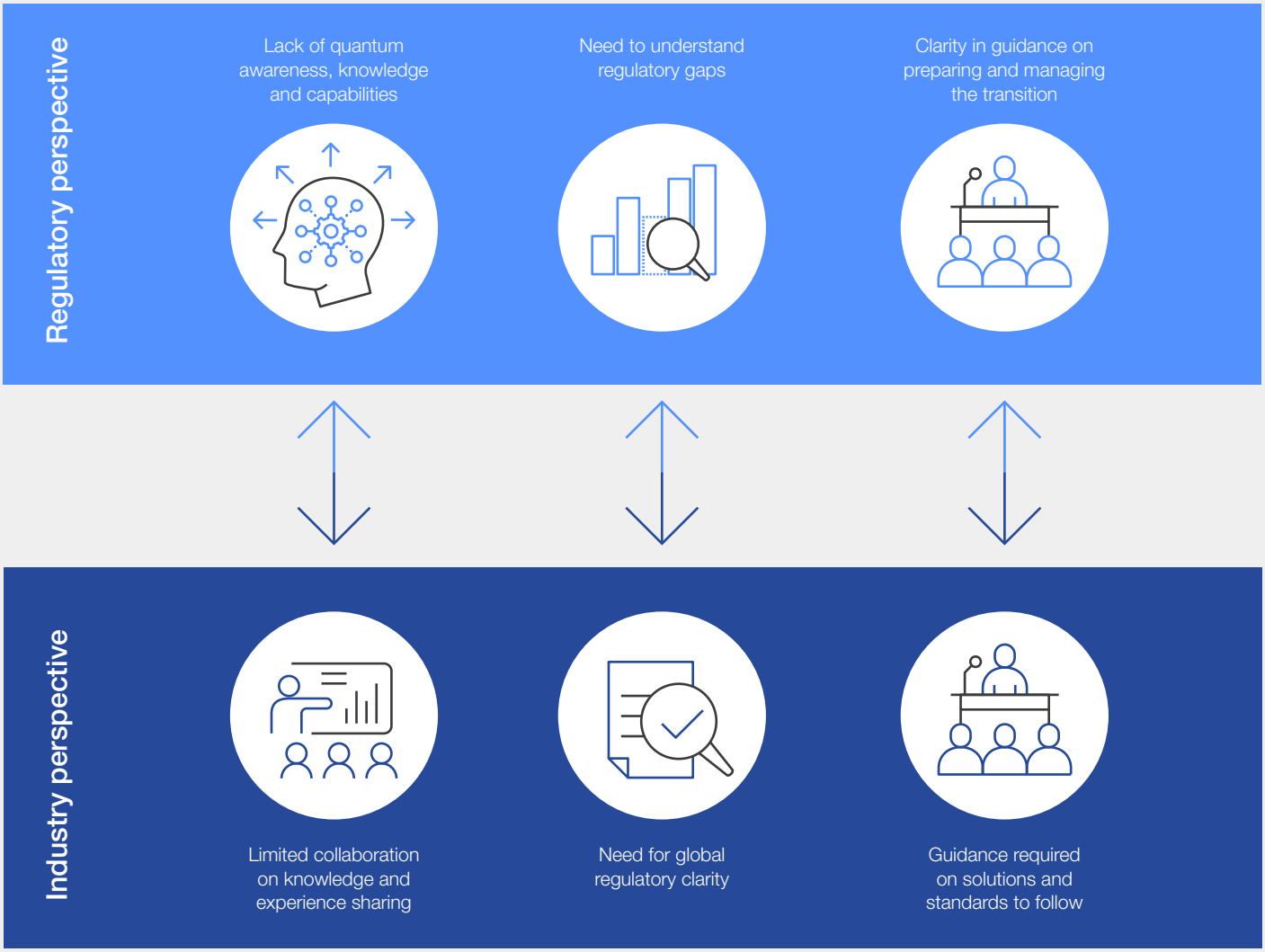
Joint regulator-industry perspective

The intricacies of quantum technology and the complexity of the financial sector present challenges for regulators and industry stakeholders.

Despite their distinct perspectives, many challenges are shared and require global collaboration to inform early and future regulatory approaches.

> **Industry and regulators must work together to navigate the uncharted territories of quantum computing and quantum-resistant cybersecurity. This pivotal period demands a shared understanding of the challenges and opportunities ahead.**
>
> Philip Intallura, Global Head, Quantum Technologies, HSBC, United Kingdom

FIGURE 1 **Aligned challenges from regulator and industry perspectives**



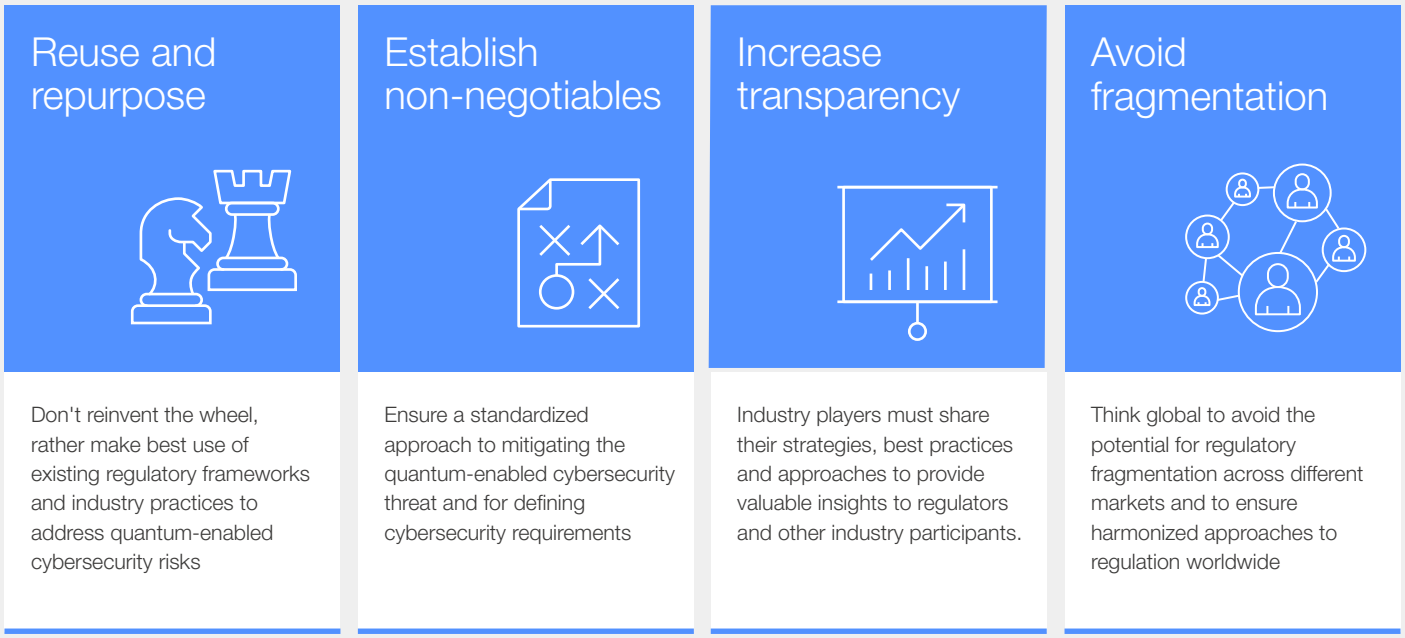
Source: World Economic Forum and Financial Conduct Authority.

2 Guiding principles

This section presents four principles to guide and inform global regulatory approaches for a quantum-secure transition.

To inform regulatory and industry approaches, this report identifies four guiding principles to create the conditions for collaboration. These principles provide initial guidance for organizations and regulators, by serving as a foundation to inform global regulatory and industry approaches towards a quantum-secure financial sector.

FIGURE 2 **Four principles for global regulation**



Source: World Economic Forum and Financial Conduct Authority.

Reuse and repurpose

This principle encourages the exploration and maximization of existing tools, techniques and frameworks to address quantum-enabled cybersecurity risks. It advocates for identifying successful strategies elsewhere and applying them to cryptographic governance.

For industry, this means following best practices while reusing processes and tools from areas such as DevOps and vulnerability management.[18]

For regulators, this means clarifying how current regulatory frameworks apply to the quantum threat and cryptographic management more broadly. Soft regulatory mechanisms should be the initial point of departure. Regulators should establish clarity by providing guidance on the application and scope of current regulatory frameworks to cryptographic management across the financial sector. Where there is concrete evidence of gaps in existing frameworks, new regulation should be developed.

Establish non-negotiables

This principle calls for the definition of overarching requirements, shared by industry and regulatory authorities, to address quantum security issues. These non-negotiable, baseline requirements should ensure that business action and regulation is customer-focused, technologically neutral and outcome-based. The requirements should follow best practices encompassing emerging international standards, an agile approach to cryptography and risk awareness in an evolving landscape.

Regardless of technological advancements and their own size or location, all industry players should strive to meet these requirements to guarantee the integrity and safety of the financial sector while ensuring consistency and interoperability.

Increase transparency

This principle urges industry players and regulators to exchange information on their strategies, best practices and approaches as much as possible. They should also be encouraged to share evidence-based, scientific communication about security threats on the one hand, and information about preventive mechanisms on the other.

Such open communication is crucial for developing effective regulatory approaches and best practices to enable a quantum-secure transition. Transparency establishes a level playing field where security is recognized as a non-profit-generating activity and a systemic, strategic objective that ultimately contributes to financial stability.

With the global financial sector being only as strong as its weakest link, collective learning and insight-sharing are essential for cybersecurity. Rather than being a competitive arena, cybersecurity is an essential foundation on which the financial sector rests.

Avoid fragmentation

This principle calls for a global approach centred on collaboration to avoid regulatory fragmentation across different markets. Fragmentation creates challenges for global entities operating in multiple jurisdictions, adding layers of complexity and compliance burdens.

Quantum-enabled cybersecurity risks require a globally coordinated, agile approach to regulation and industry action that encompasses both mature and emerging markets, and is adaptive to the evolving risk landscape. This approach requires collaboration and engagement between stakeholders across jurisdictions to understand the emerging differences in approaches and potential actions to ensure regulatory harmonization and interoperability. Given the global nature of the financial sector, international alignment and cross-border collaboration will boost innovation and bolster security, reducing vulnerabilities between firms in any end-to-end transaction.

3 Industry-regulator journey to a quantum-secure economy

This roadmap guides both regulators and industry in their joint transition to a quantum-secure economy.

> **The migration to quantum-safe systems is an unprecedented task for all, so it is important for the community to take a holistic approach and consider multiple quantum-safe solutions to achieve defense-in-depth.**
>
> Charles Lim, Global Head, Quantum Communications and Cryptography, JPMorgan Chase & Co.

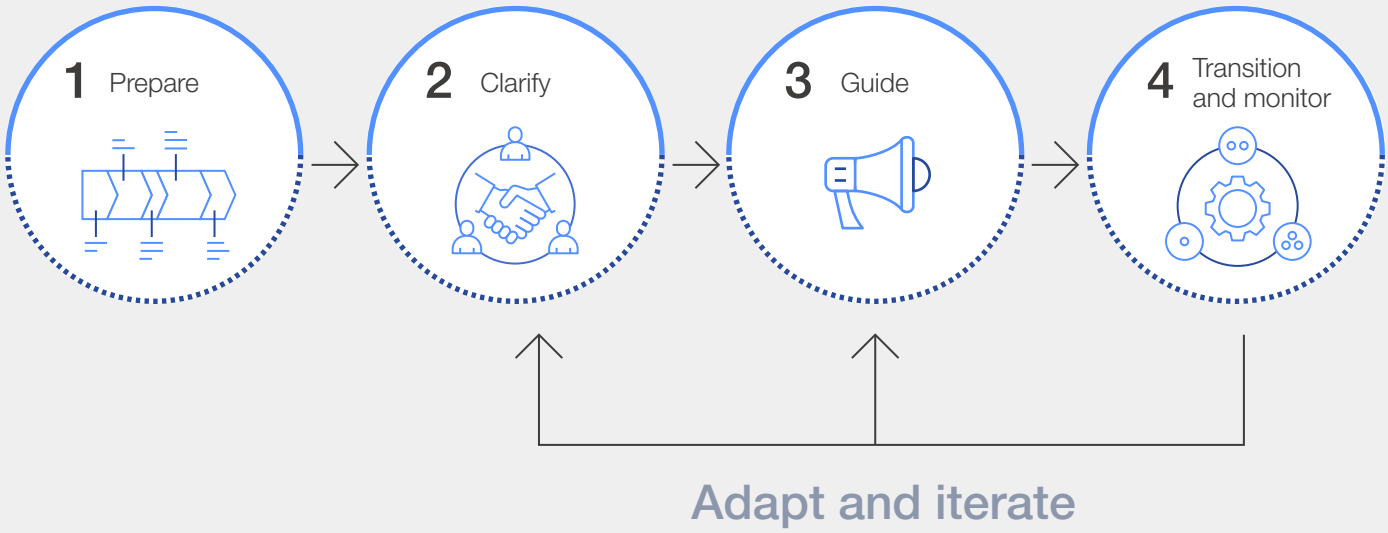
The transition to a quantum-secure economy is not just a technological shift but a comprehensive transformation of the financial sector's approach to stakeholder collaboration, cryptographic management and cybersecurity.

Towards this goal, the roadmap should not be a race, but a strategic journey, with sustained collaboration and focused action among stakeholders across international boundaries. It comprises four distinct phases: prepare, clarify, guide, and transition and monitor. Each phase builds on the previous, addressing the complexity of the transition in a sequential yet interconnected manner, and many actions span multiple phases. In this sense, the roadmap is sequential, iterative and adaptable for a diverse range of stakeholders.

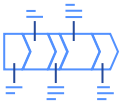
The roadmap serves as a foundational blueprint, fostering a coherent approach to simplifying and managing the intricacies associated with a quantum-secure transition. It aims to catalyse internal and external dialogues within organizations and across the financial sector and to generate momentum on actions to drive the sector towards a quantum-secure future. The roadmap is a tool to guide the transition required to maintain security, integrity and consumer trust in the global financial sector.

> **Quantum computing development is set to accelerate over the next decade and will trigger significant change in the cyberthreat landscape. Acting in anticipation can improve policy effectiveness, and is of utmost relevance to provide an inclusive transition path accounting for the different economic burden on different countries.**
>
> Giuseppe Bruno, Director at Economics, Statistics and Research, Central Bank of Italy, Italy

FIGURE 3 **Overview of the roadmap**



Source: World Economic Forum and Financial Conduct Authority.



Phase 1. Prepare

The prepare phase marks the first step for the financial sector's journey towards quantum security and modernizing approaches to cryptography. It focuses on raising awareness about quantum risks, understanding the current state of cryptographic infrastructure, and building internal capabilities.

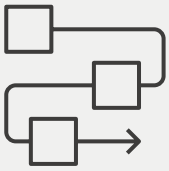
This phase is crucial for financial sector organizations, many of which may already be at or past this stage, as it lays the groundwork for the transition. By establishing a clear baseline, organizations can align their strategies with the emerging quantum landscape, ensuring they are prepared for action.

> **It is important to raise awareness among firms by providing an overview of how developments in quantum computing may impact business models and processes, including implications for related regulatory considerations.**
>
> Haimera Workie, Vice-President and Head, Financial Innovation, Financial Industry Regulatory Authority (FINRA)

Key considerations

Raise awareness

Raising awareness is essential to clarify the benefits and associated risks of quantum technologies while building and maintaining momentum. Organizations across the financial sector should consider tailored education programmes to raise awareness among stakeholders at all levels of their organization, to demystify quantum computing and demonstrate how it could impact daily business operations. Both regulators and industry should consider how to share their perspectives externally to raise awareness across the sector. Regulators should also focus on sharing knowledge between jurisdictions at this early stage to ensure a level of global awareness of quantum-enabled cyber risks.



Understand the point of departure

Transitioning to quantum-secure systems is a long-term and strategic operation. Both industry and regulatory authorities must critically examine their current states of quantum readiness to inform their approach to transitioning. Financial sector organizations should consider conducting comprehensive reviews of their cryptographic infrastructure to generate a clear understanding of their current states. This can include creating a cryptographic inventory, identifying the most vulnerable aspects of their digital and data infrastructure systems and prioritizing parts of their organization that handle sensitive data or are integral to operational stability and the provision of critical business services. It is also important to engage ecosystem partners at this stage, including technology providers and the supply chain that supports the industry. Setting achievable timelines for these assessments and publicizing these plans can enhance industry-wide awareness and foster a collective approach to quantum readiness.

Build internal capabilities

Financial sector organizations should build internal capabilities and upskill workforces to transition to quantum-secure systems and prepare for a quantum-enabled economy. Collaboration will be critical to ensure that the sector builds a holistic knowledge base and the necessary technical skills to transition. Regulators and industry should consider partnering with academic and quantum-focused research institutes to create new training programmes to build quantum-relevant skills and knowledge. Industry, regulators and academia could also collaborate on initiatives such as secondment programmes and workshops, focusing on bridging the quantum knowledge gap, and sharing domain expertise.

Phase 2: Clarify

The clarify phase provides organizations in the financial sector the opportunity to refine their understanding and approach towards the quantum-secure transition. This phase is about fostering collaboration among global financial stakeholders to gather evidence, identify existing gaps and crystallize both regulatory and industry understanding of the transition. It is particularly important for organizations that have laid their foundational groundwork and are now ready to comprehensively understand the complexities of the transition.

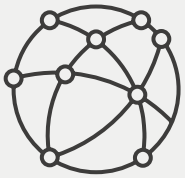
> **It is vital for financial regulators and institutions to monitor ongoing quantum computing developments that may pose cybersecurity risk to the financial sector, and work collaboratively to explore possible risk mitigation measures."**
>
> Monetary Authority of Singapore

Key considerations

Formalize engagement and collaboration

Formalizing engagement between regulators, industry and broader stakeholders is crucial for a coherent and aligned approach to quantum threats. This involves promoting unified messaging across industry stakeholders, governments, national security agencies and regulators. These stakeholders should seek to establish cybersecurity as the collective responsibility of the sector, focusing on its non-profit-making nature and its collective benefits for the stability and integrity of global financial markets. Industry may wish to take the lead in establishing formal working groups to share insights and build partnerships towards transitioning. Identifying an industry organization with wide support to lead these working groups is key.

These working groups could include regulators and other stakeholders as observers to ensure that insights are disseminated across the sector. Regulators and other government stakeholders should ensure that international forums discuss the transition to quantum security, and that countries align on a cohesive agenda for quantum security.



Map current regulations

It is not yet clear if and to what extent existing regulatory frameworks are adequate for regulating quantum computing. Both regulators and industry should engage in a comprehensive review of existing frameworks to understand how they capture quantum risks and identify potential gaps. Collaboration should be central to these efforts, ensuring that regulators and industry openly share insights and alternative perspectives. These mapping exercises should also apply a global lens that analyses the similarities and differences in approaches across jurisdictions. This international dynamic can help to reduce the risk of regulatory fragmentation, avoiding compliance complexities and vulnerabilities in the global financial sector.

Understand the transition

To successfully navigate the transition to quantum security, financial sector organizations need robust evidence of the cost of transitioning and a comprehensive overview of the underlying complexities. Industry stakeholders should begin modelling the costs and time frame of transitioning, while also analysing the financial implications of inaction. Supplementary, industry-wide impact assessment will also help to build consensus on the actions required. Industry stakeholders should simultaneously open discussions with their cybersecurity supply chain partners and critical third parties to gather insights on their approach, development timelines and adoption plans for quantum-secure systems.

Regulators could consider bringing together vendors and industry stakeholders in collaborative workshops, sandboxes or hackathon-style events to develop a common set of priorities and early action plans. Regulators could also conduct a cost-benefit analysis of different approaches to quantum risks to understand the financial impact on markets and the potential regulatory burden, so as to take decisions accordingly. This understanding will help in planning and executing a transition that is both efficient and financially viable for the entire sector.

Phase 3: Guide

The guide phase shifts the focus to key considerations that steer the financial sector towards a successful transition. It involves harnessing the power of regulatory and industry efforts and collaboration to effectively address any regulatory gaps and translate technical standards into practical, actionable implementation plans. For organizations, this phase is about moving beyond preparation and clarification to actively shaping and guiding their transition strategies. It focuses on actively developing global industry and regulatory best practices.

> **Global guidelines can help to shape the transition to a post-quantum world. Internationally aligned standards for quantum-safe protocols and encryption will ensure smooth and secure communication channels, which is crucial for the stability of the globally interconnected financial market.**
>
> Petra S. Haefliger, Senior Risk Manager, Swiss Financial Market Authority (FINMA)

Key considerations

Address regulatory gaps

Global collaborative efforts between industry and regulators will be essential to address where current regulations might not adequately capture quantum risks. National and international cybersecurity agencies should publish security guidance. Regulators should actively engage with industry to understand their practical experiences and perspectives to evaluate the diverse tools at their disposal and respond accordingly. Regulators should leverage both "soft-regulatory approaches" such as signalling through public speeches, and, where required, "hard-regulatory approaches" such as formal regulatory activities.

Given the time required to develop and implement regulatory changes, regulators should not seek to reinvent the wheel, but consider new regulation only where essential. Regulators should also seek to coordinate across jurisdictions to ensure that any action does not result in regulatory misalignment in approaches to quantum risks and the transition to quantum security in the financial sector.

Enact standards

Global technical standards and open-source projects are a trigger-point for the transition to quantum-security, but concerted effort from industry stakeholders is required to translate standards into practical applications. Technical standards, such as those being developed by NIST,[19] will provide the foundation for quantum security, but industry should seek to understand and plan for their implementation across new and existing systems.

In doing so, industry should work with vendors to understand and implement standardized approaches in a manner that limits disruptions and minimizes operational inefficiencies. Industry stakeholders should embrace transparency by publicizing their plans for transition and integration to stimulate progress towards industry best practices. Regulators could support these efforts by working more closely with international standard-setting bodies to align messaging around application of technical standards across the financial sector.

Developing a map of the industry dependency on standards and open-source software will demonstrate where action is required. Industry stakeholders and regulators could consider identifying a suitable independent body to support the testing and benchmarking of different approaches and solutions to help inform industry action.

Phase 4: Transition and monitor

This phase focuses on the implementation of strategies developed during the preceding stages, while learning and adapting from the entire transition journey. The emphasis shifts to modernizing cryptographic management and refining policy development processes to ensure long-term agility and resilience. This phase marks the transition from adaptation to innovative action, ensuring the sector's resilience and readiness for quantum computing challenges.

> **Organizations should enhance their cryptography practices now, as they did with vulnerability management before. Industry-regulator collaborations can help establish coordinated transition roadmaps.**
>
> Jaime Gómez García, Head of Quantum and Architecture at Crypto & Blockchain CoE, Banco Santander

Key considerations

Modernize approaches to cryptography

The quantum-enabled cybersecurity risk has highlighted the pressing need for the financial sector to modernize its overall approach to cryptography and cryptographic management. To remain resilient and secure against potential future risks, it is essential to modernize approaches to cryptographic management, such as the deployment of post-quantum cryptography. Organizations should also consider how to update their cryptographic management to align with contemporary DevOps, seeking to repurpose and reuse existing practices, tools and processes.

This means industry shifting its focus from a one-size-fits-all approach to a cryptographic agile approach. Such an approach would incorporate an inventory of systems, solutions and security protocols that firms could easily switch between to remain resilient in the long term. Future cybersecurity threats may materialize quicker than the present quantum threat. To mitigate this risk, industry could also consider adopting a resilient-by-design approach to current and future systems. These considerations are crucial in ensuring that the financial sector can respond effectively to the evolving threat landscape, maintain the trust and confidence of its customers, and uphold the integrity of the global financial sector.

Iterative regulatory development

The emergence of quantum computing demonstrates the increasingly dynamic nature of innovation across the financial sector; to remain effective, regulatory approaches should iterate to keep pace and continuously monitor developments. By engaging earlier with industry, regulators could adopt an inherently iterative approach by picking up early innovative signals and understanding the potential regulatory implications ahead of time.

This will help regulators maintain a forward-looking approach that focuses on outcomes and is flexible enough to adapt effectively to technological advancements across the sector. For transitioning to quantum security, regulators could also consider the potential merits of incentivizing the transition in the event of a market failure, taking an approach mindful of the resources and capabilities of smaller firms.

> **Quantum computing shines light on the systemic risk created by our profound dependency on digital platforms without resilience-by-design.**
>
> Michele Mosca, Chief Executive Officer, evolutionQ

Conclusion

All stakeholders must collaborate towards a cybersecure financial sector in the quantum economy.

In an era when the potential of quantum computing looms large, bringing with it immense opportunities and profound challenges, the financial sector must act with foresight and agility. By initiating early discussions between industry, technology providers and regulatory authorities across the globe, this work programme and final report have highlighted the intricate interplay between the industry and regulatory landscapes, highlighting the challenges that impede the sector's transition to post-quantum security.

To address these challenges, this report crystallizes insights from collaborative discussions between industry and regulators to provide guiding principles and a phased roadmap for the transition to a quantum-secure economy. The principles and the roadmap are strategic tools to catalyse dialogue, guide decision-making, generate momentum and inform global regulatory approaches towards the quantum-security transition.

As the financial sector embarks on this journey, it is imperative to remember that the transition to quantum security is not a destination but an ongoing process of adaptation and evolution. This requires a multistakeholder approach across public and private sectors, including governments, regulators, international technical standards, industry players and vendors. The financial sector must remain vigilant, adaptable and united in its approach to harnessing the transformative power of quantum computing while mitigating its risks.

This work programme and report outline a starting point for continued stakeholder collaboration to ensure that the financial sector transitions to a secure, stable and trusted financial ecosystem in the quantum era.

> **Post quantum security is a challenge we can't solve individually. Thanks to the World Economic Forum and FCA for bringing together a broad range of stakeholders and setting a bold ambition to drive a quantum secure economy.**
>
> Sabrina Feng, Chief Risk Officer for Technology, Cyber and Resilience, London Stock Exchange Group, UK

Appendix

Methodology

For this paper, the World Economic Forum in collaboration with the Financial Conduct Authority (FCA) gathered insights from five sources throughout 2023. These included:

- Regulator-only discussions: Two sessions gathered 24 global financial-sector regulatory authorities. The first was an education session with leading academics to ensure a base-level understanding among regulators on quantum security. The second was a roundtable discussion that convened regulators to collect perspectives and actions to forge a path towards international collaboration on quantum security.

- Regulatory survey: Conducted by FCA as part of pre-regulatory discussion, the survey was anonymous and non-attributable to the respondent and institution. It contained nine questions with key challenges on the topic to better understand the state of regulators. It collected a total of 15 responses from 20 regulatory authorities across different jurisdictions, including Asia, Australia, Europe, the Middle East and North America.

- Industry-only discussions: Two roundtable discussions convened close to 40 industry stakeholders active in the financial sector ecosystem, to gather insights on adoption trends, challenges regarding quantum security and expected actions towards international regulatory collaboration.

- Joint industry-regulator discussion: An in-person roundtable gathered 27 industry and global regulators from the financial sector ecosystem to discuss, align and collect insights to define the guiding principles to inform action in global regulatory collaboration.

- Bilateral interviews with regulatory authorities were also conducted to gain further insight into the current landscape.

Teams from the World Economic Forum and FCA consulted 24 financial regulators and nearly 40 industry stakeholders from across the world. All the discussions were held under Chatham House rules; consequently, no information in this report is attributed to a specific member.

Contributors

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Giulia Moschetta
Research and Analysis Specialist,
Centre for Cybersecurity

Financial Conduct Authority

Pavle Avramovic
Manager, Emerging Tech & Research,
Data Technology & Innovation

Charlie Markham
Senior Associate, Emerging Tech & Research,
Data Technology & Innovation

Acknowledgements

This paper was co-created by diverse stakeholders in the World Economic Forum's quantum security working group, part of the quantum computing network, and global financial regulatory authorities. The authors thank them for sharing their insights at workshops and consultation sessions, particularly the following individuals:

Bushra AlBlooshi
Dubai Electronic Security Center

Hoda Al Khzaimi
New York University Abu Dhabi

Ibrahim Almosallam
Saudi Federation for CyberSecurity and Programming

Mansour Alsaleh
Saudi Central Bank

Jaya Baloo
Rapid7, Inc.

John Beric
Mastercard

Arvinder Bharath
International Monetary Fund (IMF)

Guiseppe Bruno
Central Bank of Italy

Daniel Clemens
ShadowDragon

Daniel Cuthbert
Banco Santander

Michael Daniel
Cyber Threat Alliance

Reena Dayal Yadav
Institute of Electrical and Electronics Engineers

Jérôme Desbonnet
Capgemini

Stefan Deutscher
Boston Consulting Group

Ali El Kaafarani
PQShield

Sabrina Feng
London Stock Exchange Group

Benjamin W. Flatgard
JPMorgan Chase & Co.

Tommaso Gagliardoni
Kudelski Security - Kudelski Group

Jaime Gómez García
Banco Santander

Roger A. Grimes
KnowBe4

Petra S. Haefliger
Swiss Financial Market Authority

Philip Intallura
HSBC Holdings

Duncan Jones
Quantinuum

Isaac Kohn
Deloitte

Rebecca Krauthamer
Quantum Thought

Antia Lamas-linares
Amazon Web Services

Charles Lim
JPMorgan Chase & Co.

Michele Mosca
evolutionQ

Toni Pesonen
IQM Quantum Computers

Markus Pflitsch
Terra Quantum AG

Ana Predojevic
Stockholm University

Kelly Richdale
SandboxAQ

Arunima Sarkar
World Economic Forum

Roland Scharrer
AXA

Tamara Scott
US Department of State

Vikram Sharma
QuintessenceLabs

Jacob Sherson
University of Aarhus

Colin Soutar
Deloitte

Rick Switzer
US Department of State

Salvador E. Venegas-Andraca
Tecnológico de Monterrey

Mira Wolf-Bauwens
IBM Corporation

Haimera Workie
Financial Industry Regulatory Authority (FIRA)

Suman Ziaullah
Financial Conduct Authority

The Forum also wishes to acknowledge contributions from Mark Barwinski, as well as participation of all the following financial regulatory authorities:

Authority for the Financial Markets of the Netherlands

Australian Securities and Investments Commission (ASIC)

Bank of England

Bank of Israel

Bank for International Settlements (BIS)

Central Bank of France

Central Bank of Italy

Danish Financial Supervisory Authority

Deutsche Bundesbank (Central Bank of Germany)

European Securities and Markets Authority

Federal Reserve Board of Governors

Financial Industry Regulatory Authority (FINRA)

Italian Companies and Exchange Commission (CONSOB)

Monetary Authority of Singapore, Singapore

Office of the Superintendent of Financial Institutions (OSFI)

Saudi Central Bank

Securities and Exchange Board of India (SEBI)

South African Reserve Bank (SARB)

Swiss Financial Market Authority (FINMA)

Swiss National Bank

US Securities and Exchange Commission (SEC)

World Bank

Production

Michela Liberale Dorbolò
Designer, World Economic Forum

Madhur Singh
Editor, World Economic Forum

Endnotes

1. Deloitte, “Industry spending on quantum computing will rise dramatically. Will it pay off?”, 2023: https://www2.deloitte.com/xe/en/insights/industry/financial-services/financial-services-industry-predictions/2023/quantum-computing-in-finance.html
2. Jean-Francois Bobier et al., “What Happens When ‘If’ Turns to ‘When’ in Quantum Computing?”, BCG, 2021: https://web-assets.bcg.com/89/00/d2d074424a6ca820b1238e24ccc0/bcg-what-happens-when-if-turns-to-when-in-quantum-computing-jul-2021-r.pdf
3. McKinsey & Company, “Quantum Technology Monitor”, 2023: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf
4. UK Finance, “Minimising the risks: Quantum technology and financial services”, 2023: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial
5. World Economic Forum, “Transitioning to a Quantum-Secure Economy”, 2022: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
6. Bank for International Settlements, “Project Leap: quantum-proofing the financial sector”, 2023: https://www.bis.org/publ/othp67.htm
7. The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”, 4 May 2022: 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/
8. Michele Mosca and Marco Piani, “2021 Quantum-Threat Timeline Report”, Global Risk Institute, January 2022: https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/
9. World Economic Forum, “Transitioning to a Quantum-Secure Economy”, 2022: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
10. World Economic Forum, “Global Cybersecurity Outlook”, 2023: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf; World Economic Forum, “Quantum Readiness Toolkit: Building a Quantum-Secure Economy”, 2023: https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf
11. World Economic Forum, “Quantum Computing Governance Principles”, 2022: https://www.weforum.org/publications/quantum-computing-governance-principles/
12. The survey was conducted by FCA as part of this paper. For detailed information, see Methodology
13. Tandem, “Financial Institutions & Quantum Computing: A Cybersecurity Compliance Timeline”: https://tandem.app/blog/financial-institutions-quantum-computing-a-cybersecurity-compliance
14. NIST, “Post-Quantum Cryptography”: https://csrc.nist.gov/projects/post-quantum-cryptography
15. Digital Regulation Cooperation Forum (DRCF), “Quantum Technologies Insights Paper”, 2023: https://www.drcf.org.uk/__data/assets/pdf_file/0027/262674/DRCF-Quantum-Technologies-Insights-Paper.pdf; Bank for International Settlements, “Project Leap: quantum-proofing the financial sector”, 2023: https://www.bis.org/publ/othp67.htm
16. FINRA, Quantum Computing and the Implications for the Securities Industry, 2023: https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing
17. Jean-François Bobier, Cassia Naudet-Baulieu, Matt Langione, Brett Thorson, Jaroslav Šnajdr and Stefan A. Deutscher, “Are You Ready for Quantum Communications?”, BCG, 2022: https://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications; World Economic Forum, “Transitioning to a Quantum-Secure Economy”, 2022: https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf
18. World Economic Forum, “Quantum Readiness Toolkit: Building a Quantum-Secure Economy, 2023”: https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf
19. NIST, “Post-Quantum Cryptography”: https://csrc.nist.gov/projects/post-quantum-cryptography

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org