In collaboration with Deloitte

WORLD ECONOMIC FORUM

Quantum Readiness Toolkit: Building a Quantum-Secure Economy

WHITE PAPER

JUNE 2023

Images: Getty Images

Contents

Foreword

Leaders need to understand and take account of the quantum threat when strategizing about enterprise security.

Jeremy Jurgens
Managing Director,
World Economic Forum

Isaac Kohn
Partner, Deloitte, Switzerland

Colin Soutar
Managing Director,
Deloitte, USA

Accelerating developments in the field of quantum computing will bring new challenges to the cybersecurity landscape. Organizations will need to adapt to the risk posed by quantum computers, which will have the potential to break many of the cryptographic systems that we rely on today for secure communications and data protection.

Last year, the World Economic Forum, in collaboration with Deloitte, published the white paper *Transitioning to a Quantum-Secure Economy*, outlining the risks of quantum computers and providing initial guidance for organizations to transform their governance and security practices for the quantum era. Even if the quantum threat has not materialized yet, it is crucial for organizations to start planning a secure and timely quantum transition to avoid a more significant impact in future.

To help organizations prepare for this new reality, this white paper presents a set of principles that organizations can use to help ensure they are ready to enter the quantum computing era securely. These principles cover a range of areas, from strategizing about future-proof technology, embedding quantum risk in governance structures and existing risk management processes, to finding the right talent to head this new challenge.

At the heart of these principles is a focus on risk management and the need to take a proactive approach to security using technical and soft skills. Organizations must better understand the risk they are exposed to, so they can take the right steps to mitigate them. This requires a willingness to invest today in the necessary tools and experience to become quantum cyber-ready.

As we look to the future, quantum computing will undoubtedly bring new challenges and opportunities. With the right approach, however, organizations can prepare so they are ready to navigate this new landscape and protect their critical assets and information. We hope that the principles presented in this white paper will serve as a valuable resource for organizations as they seek to enhance their quantum security readiness.

Although the timescale for a fully mature commerically-viable quantum computer being available is still under much debate, there is consensus that there is a real probability that one will exist in the future. The real question is: how long will it take you to upgrade your infrastructure, and what is the expected lifetime of your data? If you do not yet know the answers to these questions, the time to act is now!

Executive summary

Five guiding principles can help organizations embrace the quantum-secure economy.

Quantum computers promise transformative powers for businesses and organizations across the globe and through a diverse range of industries. However, they also introduce significant risks to the current digital economy. In the near future, sufficiently powerful and commercially available quantum computers will undermine current cryptographic standards protecting most digital communications and vast amounts of sensitive data. Mitigating this security risk requires organizations to implement quantum-security technologies that quantum computers cannot break. Organizations need to embark on a large and complex transition to become resilient to quantum computer attacks.

There is a need for a cohesive, global, cross-border approach to cybersecurity and governing quantum risk. This *Quantum Readiness Toolkit* provides a framework of five principles to guide organizations to prepare for the quantum-secure economy by providing steps for assessing their quantum readiness and identifying and prioritizing future actions. The input arises from in-depth conversations during the World Economic Forum's quantum security working group, a global multistakeholder effort, which brings together a community of senior cyber and quantum executives and experts from business, government, regulators and academic institutions.

Organizations need to prioritize quantum risk alongside existing risks, through the definition of a clear roadmap, and clear roles and responsibilities. To face quantum risks, organizations need to raise awareness, invest in education and in technology adoption, as well as collaborate with the ecosystem. This toolkit and the accompanying knowledge base aim to provide leaders with guidance necessary to achieve organization-wide understanding of quantum risk and its governance – in order to thrive in a quantum-secure economy.

Since organizations vary in size, industry and maturity, the toolkit does not serve as a one-size-fits-all solution. The guidance laid out in the toolkit is suggestive and not exhaustive since all organizations will have to complete their own quantum security transition. The toolkit serves as a starting point to explore what an organization's unique strategy for quantum readiness can look like.

1 Guiding principles to become quantum cyber-ready

Five principles designed to guide and enable a quantum-secure transition.

The five guiding principles provide practical guidance to help organizations understand how to start their quantum-secure transition. It can help organizations understand where they are, identify gaps in their preparations to become quantum secure and improve their initial steps to quantum security.

FIGURE 1 **Guiding principles to understand the quantum-secure transition**

Ensure the organizational governance structure institutionalizes quantum risk

The quantum threat requires organizations to align their governance structure to their quantum cyber readiness transition by defining clear goals, roles and responsibilities and creating leadership buy-in to enforce change effectively.

Raise quantum risk awareness throughout the organization

Demystifying the quantum threat is key. This requires that not only quantum cyber readiness experts but also senior leaders and risk managers understand the risk and impact of the threat to the organization.

Treat and prioritize quantum risk alongside existing cyber risks

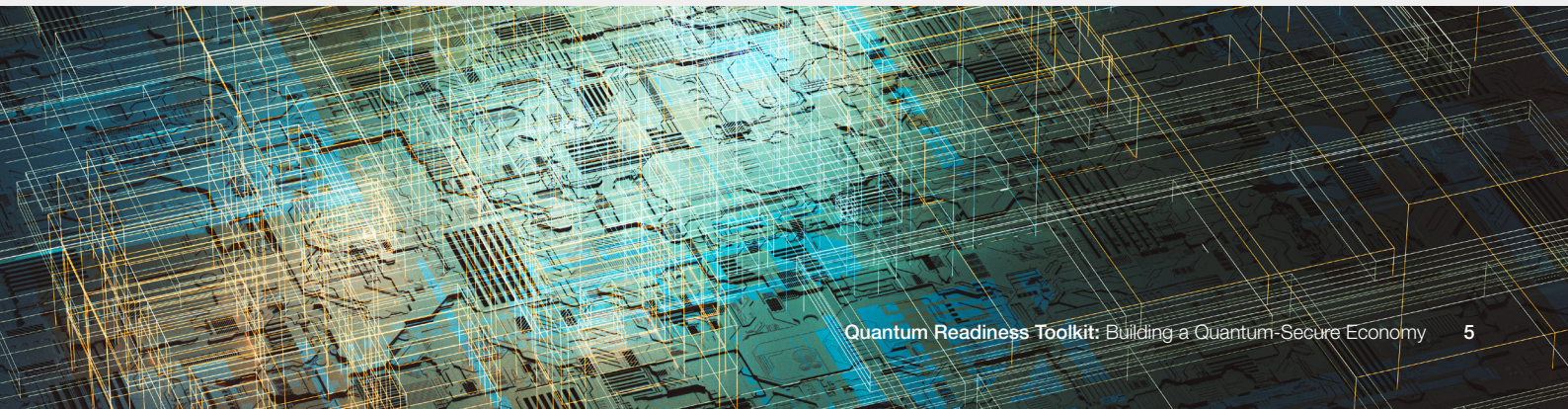
A quantum cyber-ready organization follows a structured approach to evaluate and manage quantum risk and integrates mitigating this risk into existing cyber risk management procedures.

Make strategic decisions for future technology adoption

Managing quantum risk provides organizations with opportunities to reassess their technology landscape, specifically the use of cryptography. To make the most out of technology solutions that help mitigate quantum risk, organizations should make strategic technology decisions that support “crypto-agility” to achieve their security objectives.

Encourage collaboration across ecosystems

Quantum risk is a systemic risk. An effective quantum security strategy includes collaborating and sharing information with other organizations to identify risks throughout the ecosystem and suppliers to jointly mitigate such risks.



2 The principles to become quantum cyber-ready: in-depth analysis

Each principle is defined with additional considerations and brief guidance to demonstrate effective adoption and implementation.

> **In navigating the complexities of the quantum era, the quantum readiness toolkit ensures our ability to not just withstand quantum-secure transitions, but to excel within them.**
>
> Daniel Cuthbert, Global Head, Cybersecurity Research, Banco Santander

2.1 Ensure the organizational governance structure institutionalizes quantum risk

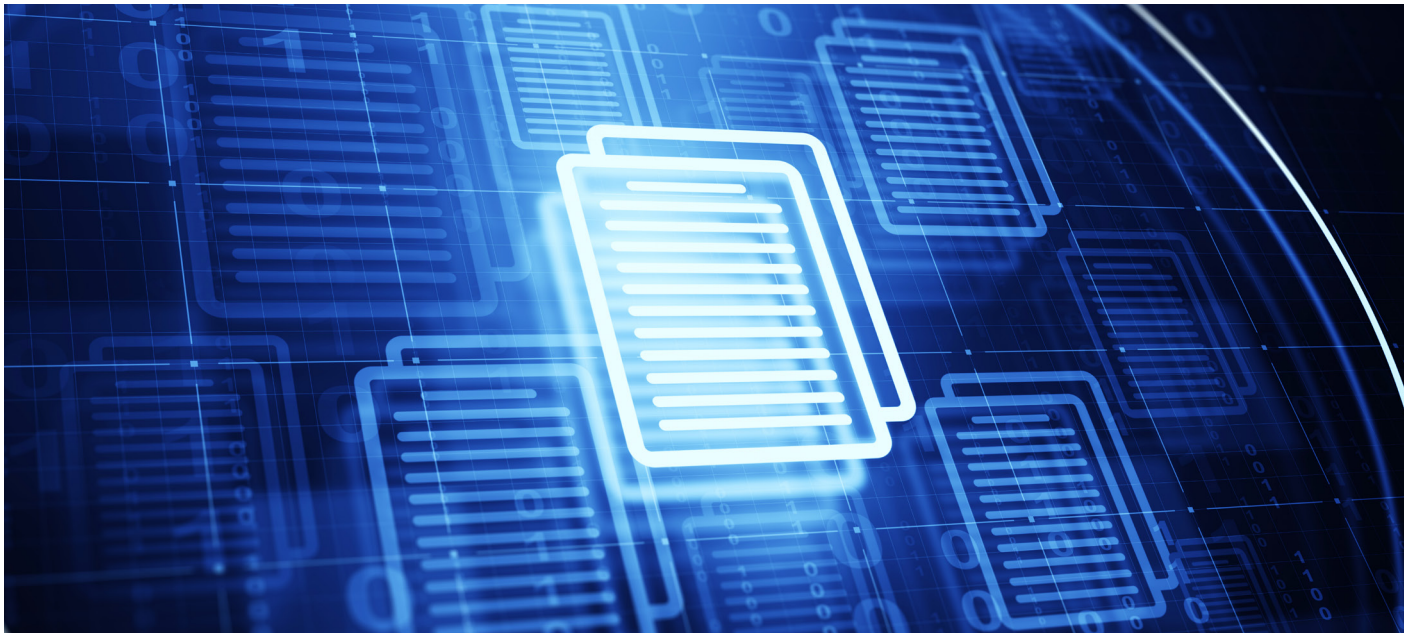
Clear and structured governance is essential to building an organization that is resilient to current and future quantum risks, such as quantum security transition programmes, allocated responsibilities and updated policies and operating procedures. To enhance readiness, the organizational governance structure should institutionalize quantum risk, allowing for change to be enforced effectively. Organizations need to formulate their quantum security goals and roles clearly.

Key considerations

- **Balance prescriptive versus open-ended guidance:** No “one-size-fits-all” approach exists for mitigating quantum risk. Developing (international) standards and creating consensus across geographies can help large organizations prevent conflicting requirements.
- **Start small:** Start with a small team and tasks by following an interactive step-by-step approach in tandem with socialization activities to get all stakeholders on board. Splitting the transition into several small segments (e.g. limited to a specific section of the organization or product suite) provides time for adoption and socialization, lowering the entry barrier and maximizing integration lessons learned in future phases.
- **Establish that mitigating quantum risk becomes part of business as usual:** Make quantum a recognized risk that is part of regular cybersecurity activities. Embed quantum risk and future cryptographic risks in the existing cybersecurity operating model.

TABLE 1 | **Practices and activities to ensure the organizational governance structure institutionalizes quantum risk**

Practices	Activities
Establish effective governance and mandates for quantum security projects.	– Assign appropriate responsibilities across the organization and include functions with respective ownership of mitigating the quantum threat. These functions include but are not limited to legal counsel, data officers and operational managers. – Provide staff working on the quantum security transition with sufficient executive support and mandates to drive change. – Report progress and programme risks to an accountable and responsible function lead within security, risk or related functions.
Appoint cryptographic champions to socialize the impact of quantum risk and to drive quantum security plans within the organization.	– Appoint or hire cryptographic champions that can drive and accelerate quantum cyber readiness as well as be the point of contact to provide broader awareness of quantum risk and insights. – Organize forums for cross-functional collaboration to encourage discussions and collaboration between cryptographic champions and stakeholder groups (e.g. security officers, engineers, IT project managers) to help address concerns and questions related to quantum. – Enable relevant stakeholders, such as cryptographic champions or quantum transition project teams, to challenge and provide feedback for quantum security transition plans. Then, incorporate feedback and lessons learned into the quantum security roadmap.
Develop a roadmap to become quantum secure and align the roadmap with quantum risk assessments and organizational risk appetite.	– Create a quantum security roadmap with clearly-established objectives, timelines, milestones and the ability to measure progress over time. – Develop an estimate of potential costs and timelines early in the quantum security transition to guide expectations and create awareness of transition costs. – Align the quantum security roadmap to broader roadmaps (e.g. the overarching cybersecurity roadmap) along with those for any relevant adjacent security or technology capabilities (e.g. a large cloud transition). – Implement feedback mechanisms to incorporate input from relevant affected stakeholder groups into the quantum security roadmap. – Document lessons learned from the quantum security transition and actively disseminate/include them in the development of new strategies and large-scale transformations. – Align quantum risk to relevant long-term strategic initiatives within the organization, such as corporate responsibility programmes, which will serve to gain more support and create more strategic cohesion.
Periodically update policies and procedures in line with organizational changes and relevant developments.	– Embed or develop quantum security requirements in cryptographic policies and standards within the organization. – Periodically update cryptographic policies to incorporate novel insights, organizational changes and industry good practices. – Organize training sessions to help teams understand organizational changes and new ways of working. – Integrate requirements on the use of quantum-secure technology in third-party contracts.



2.2 Raise quantum risk awareness throughout the organization

> **The importance of acting on post-quantum security cannot be overemphasized. Organizations often wonder when to start and how to start, who should be the stakeholders, etc. The quantum readiness toolkit is the attempt to answer these questions and move forward.**
>
> Reena Dayal, Chairperson, Quantum Ecosystems and Technology, Council of India

Quantum risk is a novel concept to many stakeholders and is often misunderstood or viewed as a highly complex technical topic for business leaders. This perceived complexity tempts many stakeholders to postpone any meaningful action or to disregard the topic completely. To raise awareness of quantum risk, organizations should actively understand and discern quantum risk and spread focused knowledge on quantum risk to relevant internal and external stakeholders.

Key considerations

- **Avoid spreading fear, uncertainty or doubt:** Many conversations around managing quantum risk are fear-focused. Treating the quantum threat like other (emerging) cyberthreats aids in clarity, and with adequate preparation, reduces the overall panic that surrounds the topic.
- **Develop a creative talent strategy:** There is a scarcity of talent, and not everybody needs to be an expert in quantum physics, mathematics or computer science. The lack of available talent means organizations should be creative with hiring and reskilling existing talent to help ensure sufficient expertise is available.
- **Tailor awareness and education activities:** Various functions, including C-suite and broader security community, should be kept up to date with advances in the quantum threat. However, without sufficient context, news relating to the quantum threat might trigger organization leaders to approach the topic with fear and panic rather than a level-headed and well-thought-out strategy. Therefore, updates should put innovations and developments into the proper context.

TABLE 2 **Practices and activities to ensure the organizational governance structure institutionalizes quantum risk**

Practices	Activities
Assess what knowledge is required across stakeholder groups to make the organization quantum ready.	– Map all relevant roles within the organization (e.g. cryptography talent, human resources, risk managers) that might be impacted by the quantum threat.[1] – Develop a skills matrix that describes each role's knowledge requirements and needs to help prioritize and tailor awareness activities. Use existing guides and examples, such as Quantum-Safe Canada's curriculum guide[2] or the EU's *Competence framework for quantum technologies: methodology and version history*[3]).
Enhance the organization's access to talent specialized in the quantum threat.	– Assess what quantum security talent is needed and develop a strategy that includes hiring, training and/or upskilling of talent. – Establish partnerships and collaboration networks to augment quantum security talent. – Provide tailored training and development opportunities for talent in functions that are critical to managing quantum risk (e.g. cryptographers, product developers and network engineers).
Build awareness and knowledge among relevant leaders in the organization.	– Develop and implement an actionable socialization plan that aims to create awareness for senior stakeholders in the organization of the importance of becoming quantum ready. – Appoint function leads within security, risk management and related functions to serve as ambassadors responsible for addressing quantum risk within their domains. – Support senior leadership in understanding that mitigating quantum risk is a shared responsibility and actively promotes this view amongst relevant stakeholders (i.e. by making quantum risk a part of senior leadership meetings). – Support C-level employees in understanding quantum risk, for instance by organizing table-top exercises, setting up a "hype free hotline" for ad-hoc support, or by developing a "quantum monitor", which provides input on recent quantum (risk) developments and how the C-level employees should react to these events. – Communicate to leadership in a way that resonates with them (i.e. by explaining quantum risk in business terms, providing actionable next steps and using accessible language).

2.3 Treat and prioritize quantum risk alongside existing cyber risks

> **The quantum readiness toolkit is a valuable resource for cybersecurity leaders and practitioners alike as they prepare strategies to transition cybersecurity infrastructure to a quantum-resilient posture. The toolkit offers clear guidance on governance, raising awareness and pathways for technology adoption. I believe it to be an important asset for professionals tasked with managing the quantum risk to cybersecurity.**
>
> Vikram Sharma, Chief Executive Officer, QuintessenceLabs

Many organizations realize that in order to thrive digitally, they must effectively manage risks while allowing and enabling the business to prosper. The risks of quantum computers to current cryptographic methods fit under the cyber risk management umbrella. To treat and prioritize quantum risk, organizations should follow a structured approach to evaluate and manage quantum risk as cyber risk and as part of an organization's existing cyber risk management programme.

Key considerations

- **Acknowledge organizations have divergent priorities:** They will also vary in what actions should be undertaken to make their organizations quantum ready. This means that specific objectives and approaches to managing quantum risk can differ from one organization to the next.
- **Learn from previous (cybersecurity) transitions:** Success factors and lessons learned from earlier transitions can and should be reused. Similarly, lessons learned from the quantum security transition should be applied to mitigating future emerging threats.
- **Mitigate quantum risk through a combination of risk management, effective and up-to-date documentation, and technical tools**. Documenting an organization's technology and the requirements for them to work correctly could be combined with creating a cryptographic "bill of materials" (CBOM) that includes all the cryptographic components used in applications and services across the organization. Ideally, organizations will adopt a modular approach and separate cryptography from the applications, which is a starting point for cryptographic agility. Technology-focused practices and activities will be discussed within the fourth principle on sustainable technology decisions.

TABLE 3 **Practices and activities to treat and prioritize quantum risk alongside existing cyber risks**

Practices	Activities
Perform quantum risk assessments to better understand and prioritize quantum risk.	– Assess the extent to which attackers using a quantum computer are a threat to the organization, e.g. by reviewing publicly available threat reports or performing a threat analysis. – Perform an initial quantum risk assessment to get an idea of how serious quantum risk may affect the organization's cybersecurity posture, including by looking at how long data will remain potentially valuable for attackers (based on "data shelf life" or "data half-life"). – If possible, prioritize the sequence of IT assets being made quantum secure using existing risk management processes such as a business impact analysis (BIA). This can also be used to identify and quantify systems vulnerable to "harvest-now, decrypt-later" (HNDL) attacks. – Monitor high-risk technology such as systems and applications regularly and prioritize these technologies in the broader quantum security roadmap. – Explore the potential of (partially) managing quantum risk through other means than implementing quantum-secure technology, for example with cybersecurity insurance or accepting any residual risk for low-risk technology.
Embed quantum risk mitigation plans into existing risk management procedures.	– Embed quantum risk into the organization's risk register or risk scorecard to track and prioritize within broader risk management efforts, considering the long materialization and mitigation timeline of quantum risk.[4] – Create quick wins by including quantum risk as part of annual data mapping exercises to identify systems that are processing sensitive data and may therefore have a higher risk.
Assess vendors and other third parties to understand how they might impact the organization's strategy to become quantum secure.	– Perform risk analyses on (potential) third parties to assess their quantum risk, such as based on the value of the data they will be able to access and their existing quantum cyber readiness plans and progress. – Prioritize mitigating quantum risk of existing third-parties based on their quantum risk and business value: engage with them to foster collaborative efforts across supply chains aiding quantum readiness.

2.4 Make strategic decisions for future technology adoption

> **The development and sharing of useful tools for preparing our digital platforms to be secure in the quantum era, alongside the increasing imperative to manage systemic cyber risks posed by code-breaking advances, will facilitate the evolution to a more secure and resilient cryptographic foundation for the global economy.**
>
> Michele Mosca, Professor and Co-Founder, Institute of Quantum Computing, University of Waterloo

Mitigating quantum risk requires organizations to re-assess their technical infrastructure, specifically regarding their use of cryptography, and make strategic decisions to maintain the confidentiality, availability and integrity of data. This includes considering novel concepts, such as crypto-agility, and investing in new, emerging technologies. To make strategic decisions for future technology adoptions, organizations need to think ahead, enable crypto-agility and ensure that cybersecurity capacities are adaptable to the ever-evolving threat environment.

Key considerations

- **Use tools and applications that are easy to use safely and secured by design:** Ensuring tools are designed with proactive security objectives in mind, developers can aid end users by making it hard for end users to trigger cybersecurity incidents.
- **Start experimenting and assessing now for adoption later:** Organizations may not fully understand what crypto-agility looks like or what the impact and effectiveness of standardized post-quantum cryptography might mean for them. Engaging with these concepts and standards will aid understanding and confidence in adoption later. Organizations could start experimenting with small proofs of concept or assessing what adopting these technologies might mean for them and their risk profile.
- **Harness the technological adoption to mitigate existing cybersecurity risks:** Organizations can make use of the implementation of quantum-secure technology as an opportunity to resolve long-known cybersecurity deficiencies (e.g. implementing auto-updating of certificates to decrease system downtime).

TABLE 4 **Practices and activities to make strategic decisions for future technology adoption**

Practices	Activities
Design a crypto-agile technology landscape that enables quick and effective implementation and configuration of post-quantum cryptography.	– Assess the impact of quantum-secure technologies on existing services, including stability and efficiency. – Create a CBOM that provides an overview of all cryptography in use in the organization. – Assess quantum risk for individual cryptographic components; for high-risk components that might be more vulnerable to cryptanalytic attacks, develop mitigation plans. – Enable hybrid solutions where post-quantum and classical algorithms are layered for broader protection. – Consider both quantum threats, but also potential new avenues of securing information using the positive application of quantum applications, e.g. quantum key distribution or quantum networks.
Create a product life cycle that supports products becoming more quantum secure.	– Create crypto-agility by designing strategies for systems affected by the quantum threat. – Identify legacy technologies within the organization that might not be able to run quantum-secure technologies and define tailored quantum risk mitigation plans. – Embed quantum-secure requirements throughout the system development life cycle (e.g. by mandating developers and engineers to use white-listed cryptographic algorithms). – Include quantum security requirements, such as the use of post-quantum cryptography, in the scope of technical security tests.
Implement appropriate security controls for developers and third-party products.	– Include quantum security requirements in new or renewed product contracts. – Prioritize penetration tests for high-risk third-party products, these should include quantum security requirements.

2.5 Encourage collaboration across ecosystems

In the hyperconnected digital economy that today's organizations are a part of, data is shared and stored across ecosystems. Many cybersecurity risks are systemic and, therefore, cannot be mitigated by individual organizations. To aid quantum cyber readiness across ecosystems, organizations must connect and engage with peers, third parties, governments and academia to discern and demystify quantum risk and its systemic impact. Hence, encouraging collaboration across ecosystems allows organizations to work together and share relevant information and insights related to (mitigating) quantum risk.

Key considerations

- **Collaborate to understand systemic risks across your ecosystem:** An organization providing key parts to another organization without considering quantum security could lead to unknown vulnerabilities for the downstream organization using these key parts within their products or network.
- **Help cultivate a unified, broad view across the ecosystem**: This includes a wide array of stakeholders, including vendors, supply chain partners and academia. Ecosystems can share leading practices, create urgency within the industry and collaborate on reducing risk spread over multiple actors within supply chains. Collaboration with academia and students will aid innovation speed and getting insights on the latest research.

TABLE 5 **Practices and activities to encourage collaboration across ecosystems**

Practices	Activities
Connect with ecosystems on quantum-readiness strategy.	– Create a broad view of the ecosystem and map all actors that impact or can be impacted by quantum risk. – Identify, track and use existing platforms and initiatives that spread knowledge relevant to the quantum security transition. – Connect with industry groups, informal connections or Information Sharing and Analysis Centers (ISACs)[5] to collectively mitigate systemic quantum risks.
Contribute to initiatives building shared technical standards.	– Contribute to product certification regimes such as through common criteria. – Facilitate interoperability by using shared technical standards where possible, like the technical standard used for payments (e.g. Europay, Mastercard and Visa (EMV))[6]. – Remain cognizant of any geographic or regulatory restrictions or import/export controls.
Contribute to collaborations on developing quantum knowledge.	– Invest in ecosystem initiatives that increase the collective knowledge base and future talent pool, such as university initiatives (e.g. the Columbia Quantum Initiative[7]). – Encourage employees to get quantum-security-related certifications.

Conclusion

As organizations around the globe formulate their plans to mitigate the cyber risk aspects of quantum computing, these five principles will allow them to chart a course that is in line with the real threat posed by the technology, and consistent with their more general cyber risk management practices.

Colin Soutar, Managing Director, Deloitte, USA

Sufficiently powerful quantum computers pose a serious threat to today's digital economy and data protection, requiring organizations to embark on a quantum security transition. This *Quantum Readiness Toolkit* offers organizations guidelines which they can use to assess, prioritize and act now. To enhance the successful implementation of the principles, organizations should consider to:

- **Raise awareness of quantum risk and the need to mitigate it now**. Provide decision-makers with a clear and coherent message to build meaningful partnerships and drive action. Despite the deep technical aspects of quantum risk, mitigating it will be a people business and require a workforce that understands and prioritizes the risk.

- **Realize there is no silver bullet.** No individual quantum security solution, policy or hired expert will make an organization quantum secure overnight. It will require a variety of tools adapted to the environment and use cases focused on people, governance and technology to make an organization resilient to present and future cryptographic risks, of which quantum risk is only one.

- **Act now**. Nobody knows for sure when a sufficiently powerful quantum computer will arrive, but the timeline is shrinking. Everyone is aware that transitions take time, and nobody wants to be too late. Organizations should start now to give themselves sufficient time to start small, experiment and get acquainted with the challenges and success factors that will allow a quantum-secure transition. Regulators can play an important role in driving timely action across ecosystems, but they should contemplate guardrails that encourage adoption and support organizations in becoming quantum secure.

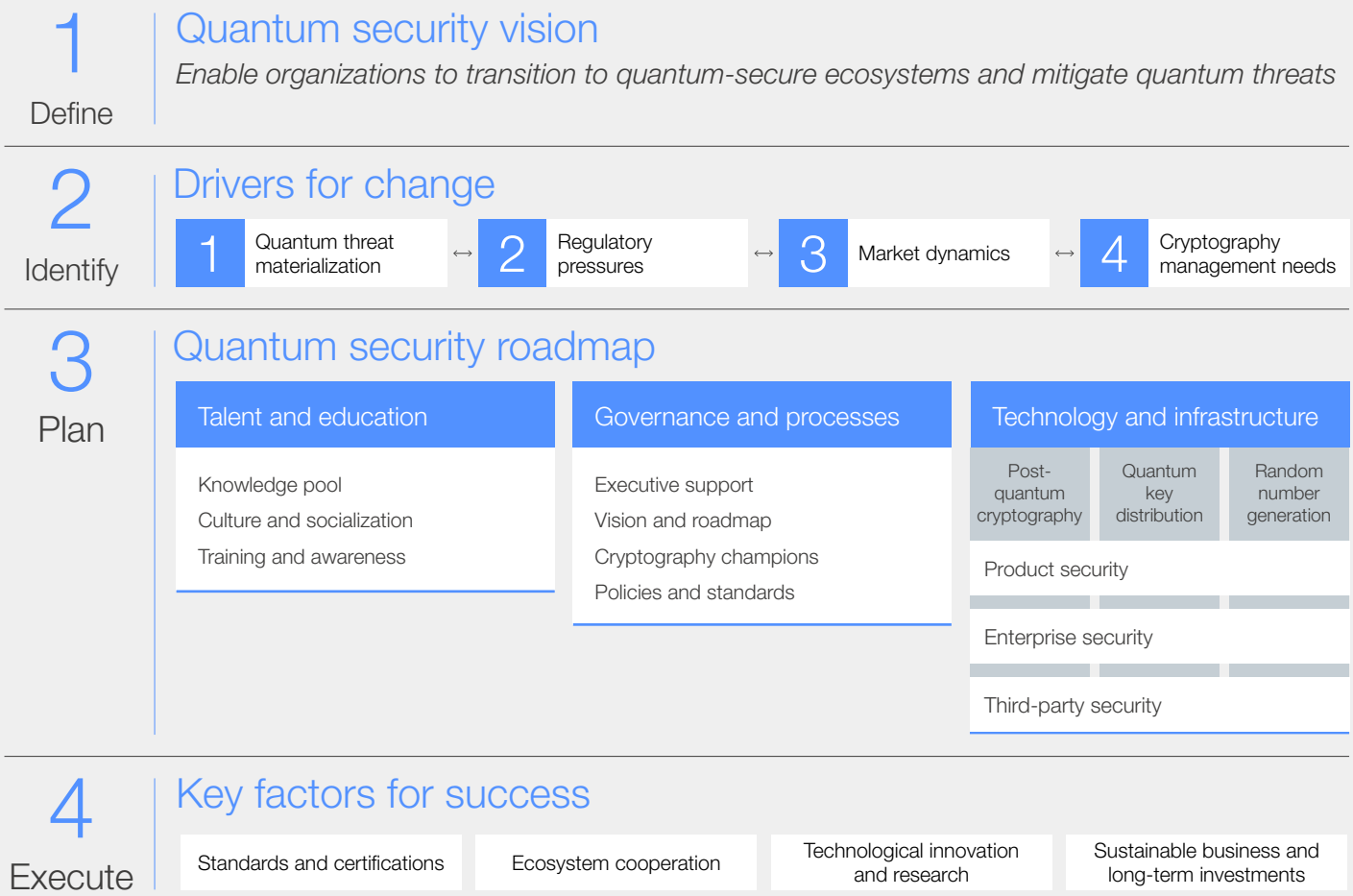
This *Quantum Readiness Toolkit* is a meaningful step in providing organizations guidelines on becoming quantum secure, based on input from a global and diverse community of experts. As more organizations become aware of the need to act now, this can also lead to more interest in assessing to what extent peer organizations are becoming quantum secure. Driving and coordinating systemic change requires collective action and support from governments and organizations by providing additional guidance, showcasing examples and quantitative metrics.

Appendix

A1 Methodology

During the first year of the Quantum Security Initiative, the community developed a consensus-based quantum security transition framework (see Figure 2) as part of the *Transitioning to a Quantum-Secure Economy* white paper.[8] This framework provided high-level guidance for organizations in defining milestones in their quantum security transition. The framework consists of four layers (define, identify, plan and execute) that help organizations structure their goals and objectives for a secure quantum transition.

FIGURE 2 **Quantum-Secure Transition Framework**



Source: World Economic Forum, *Transitioning to a Quantum-Secure Economy*, 2022.

In the second year of the initiative, the community convened in working sessions to further drive the adoption of this framework by helping organizations with actionable guidance. For each of the three pillars (talent and education, governance and processes and technology and infrastructure), the community defined good practices and detailed activities. The output of the working session led to the adoption of a set of high-level principles that have been used to structure the *Quantum Readiness Toolkit*.

For each high-level principle, the toolkit contains good practices and detailed activities based on the input provided in working sessions by Forum quantum security experts representing businesses, academia and government. Organizations are encouraged to adopt the principles described, Organizations are encouraged to adopt the principles described, develop a strategy and kickstart their journey to become quantum cyber-ready.

Contributors

World Economic Forum

Anne Ardon
Project Fellow, Quantum Security, World Economic Forum; Junior Manager, Deloitte, Netherlands

Itan Barmes
Project Fellow, Quantum Security, World Economic Forum; Specialist Leader, Deloitte, Netherlands

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Deloitte

Chris Knackstedt
Senior Manager, Deloitte, USA

Casper Stap
Senior Consultant, Deloitte, USA

Steering committee

Jaya Baloo
Chief Security Officer, Rapid7

Daniel Cuthbert
Global Head, Cybersecurity Research

Reena Dayal
Chairperson, Quantum Ecosystems and Technology Council of India

Isaac Kohn
Partner, Deloitte, Switzerland

Michele Mosca
Professor and Co-Founder, Institute of Quantum Computing, University of Waterloo

Vikram Sharma
Chief Executive Officer, QuintessenceLabs

Colin Soutar
Managing Director, Deloitte, USA

Acknowledgements

This *Quantum Readiness Toolkit* was co-created by many practitioners and diverse stakeholders in the World Economic Forum's project community on quantum security as part of the quantum computing network that shared insights and lessons learned through interviews, design workshops and consultation sessions. The World Economic Forum would like to thank the following individuals for their insightful reviews and feedback.

Ibrahim Almosallam
Saudi Federation for CyberSecurity and Programming (SAFCSP)

Pavle Avramović
Financial Conduct Authority (FCA)

John Beric
Mastercard

Arvinder Bharath
International Monetary Fund (IMF)

Kirk Bresniker
Hewlett Packard Enterprise

Marijus Briedis
Nord Security

Maya Bundt
Bâloise-Holding

Mark Carney
Banco Santander

Daniel Cuthbert
Banco Santander

Michael Daniel
Cyber Threat Alliance

Jérôme Desbonnet
Capgemini

Stefan Deutscher
Boston Consulting Group (BCG)

Gabrijela Dreo Rodosek
University of the German Federal Armed Forces (Bundeswehr München)

Ken Durazzo
Dell Technologies

Dimitri van Esch
ABN Amro

Roland Fejfar
Morgan Stanley

Jacques Francoeur
International Telecommunication Union (ITU)

Tommaso Gagliardoni
Kudelski Security

Roger A. Grimes
KnowBe4

Jack Hidary
SandboxAQ

Ali El Kaafarani
PQShield

Hoda Al Khzaimi
New York University Abu Dhabi

Antia Lamas-Linares
Amazon Web Services (AWS)

Soon Chia Lim
Cyber Security Agency of Singapore

Paul Mee
Oliver Wyman (MMC)

Julian Meyrick
International Business Machines (IBM)

Giulia Moschetta
World Economic Forum

Toni Pesonen
IQM Quantum Computers

Ana Predojevic
Stockholm University

Kelly Richdale
SandboxAQ

Arunima Sarkar
World Economic Forum

Jacob Sherson
University of Aarhus

Rodney Tan
Cyber Security Agency of Singapore

Salvador Venegas-Andraca
Tecnologico de Monterrey

Marc Verdonk
Deloitte, Netherlands

Desmond Wan
Cyber Security Agency of Singapore

Mike Wilkes
New York University Tandon School of Engineering

Carl J. Williams
National Institute of Standards and Technology (NIST)

The Forum also wishes to acknowledge expert contributions from Taher Elgamal and Brian LaMacchia for their thorough leadership, insights and guidance throughout the development of this report.

Production

Laurence Denmark
Creative Director, Studio Miko

Sophie Ebbage
Designer, Studio Miko

Martha Howlett
Editor, Studio Miko

Endnotes

1. World Economic Forum, *Quantum Personas: a multi-stakeholder approach to cyber risk management*, 2021, https://www3.weforum.org/docs/WEF_Quantum_Personas_GFC_on_Cybersecurity_2021.pdf.
2. Quantum-Safe Canada, *Quantum-Safe Skills Development – An Analysis of International Models*, 2022, https://quantum-safe.ca/wp-content/uploads/2022/12/2022-10-16-QSCurriculumGuide_v1.0_Final.pdf.
3. European Union, *Competence framework for quantum technologies: methodology and version history*, 2021, https://op.europa.eu/en/publication-detail/-/publication/93ecfd3c-2005-11ec-bd8e-01aa75ed71a1/language-en.
4. Global Risk Institute, *Quantum Threat Timeline Report*, 2022, https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/.
5. "Information Sharing and Analysis Centers (ISACs)", *European Union Agency for Cybersecurity (ENISA)*, n.d., https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.
6. "Why EMV?", *EMVCo.,* n.d., https://www.emvco.com/why-emv/.
7. "Columbia Quantum Initiative", Columbia University in the City of New York, n.d., https://quantum.columbia.edu/.
8. World Economic Forum, *Transitioning to a Quantum-Secure Economy*, 2022, https://www.weforum.org/whitepapers/transitioning-to-a-quantum-secure-economy/.

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