



## **G7 CYBER EXPERT GROUP STATEMENT ON Advancing a Coordinated Roadmap for the Transition to Post-Quantum- Cryptography in the Financial Sector**

**November 2025**

### **Purpose**

The G7 Cyber Expert Group (CEG) advises G7 Finance Ministers and Central Bank Governors on cybersecurity matters of importance for the security and resilience of the financial system. Recognizing the cryptographic risks that quantum computers may introduce to financial systems, the CEG has developed this roadmap to encourage a coordinated approach for migration to quantum-resistant cryptography and transition to cryptographic agility.<sup>1</sup> This statement does not set guidance or regulatory expectations. Rather, it is intended to inform and provide context to support migration activities, outline key considerations, and suggest approaches to consider for enabling a timely, secure, and harmonized transition to post-quantum cryptography across the financial sector.

### **Opportunities and Risks with Quantum Computers**

In September 2024, the G7 CEG released a [statement](#) highlighting the benefits and risks associated with quantum computing. The statement noted that while quantum computing promises significant new capabilities for financial services, sufficiently advanced quantum computers will be capable of breaking widely used cryptographic protocols that protect systems and data.<sup>2</sup> A primary way of addressing these risks is for entities to transition to what is known as post-quantum cryptography and quantum-resistant cryptographic algorithms.<sup>3</sup> Over the past year, many national authorities have issued guidance and some participants in the financial ecosystem have begun developing migration plans and implementing quantum-resistant algorithms.

### **Support for Navigating the Risks of Quantum Computing in the Financial System**

Building on the 2024 statement, the G7 CEG developed this high-level roadmap to inform senior leaders on the types of activities that may help organizations transition to post-quantum cryptography in a coordinated, timely, and objective-driven way in advance of future risks. The roadmap and associated timelines are not intended to be prescriptive, rather to inform about the various activities that could be considered before risks materialize, supporting operational continuity.

---

<sup>1</sup> This roadmap offers key considerations for financial authorities, financial entities, providers of critical services, cryptographic and security technology vendors, infrastructure operators, national cyber agencies, standard-setting bodies, and other stakeholders that support security and resilience in the financial sector.

<sup>2</sup> This risk does not impact all currently used cryptographic algorithms equally but is especially significant for the most widely used algorithms that support public key cryptography.

<sup>3</sup> While quantum-resistant algorithms exist today that can be used on current information systems, cryptographic transition is often a complex and time-consuming process that must be undertaken with care to be done safely.

## TLP: CLEAR



This roadmap was developed by a dedicated CEG task force of experts from financial authorities and industry across G7 jurisdictions and reflects extensive stakeholder consultation in relevant forums.<sup>4</sup> It presents considerations to promote harmonization and cooperation across jurisdictions while preserving flexibility and may serve as a resource to guide the planning and governance of the transition.

Additionally, financial institutions of all sizes are often highly dependent upon and interconnected with information technology products, vendors and other third-party providers. This roadmap may help these entities better understand the importance of quantum-resistant cryptography to the financial sector and the potential time constraints for migration.

### Considerations for Transition to Post-Quantum Cryptography

This roadmap is based on several considerations that the G7 believes are important for promoting successful transition.

*Flexibility* – The roadmap is intended to promote flexibility based on the unique circumstances of individual entities. It features mechanisms for ongoing monitoring and recalibration so that plans may be adapted in consideration of evolving risks.

*Risk-Based Approach* – Not all entities, systems, or functions face the same level of exposure or systemic importance.<sup>5</sup> Entities may decide to apply more aggressive timelines to the most critical areas while applying extended timelines to lower-risk areas. In some situations, non-critical use cases can serve as early pilots to build experience before the migration of more critical systems.

*Standards-Based Approach* – Organizations may consider use of existing roadmaps and IT security delivery standards (e.g., ISO 27001, ITIL) and establish quantifiable metrics to track progress, demonstrate accountability, and enable recalibration. These metrics may help assess readiness at both institutional and system-wide levels—enabling coordinated monitoring across the financial ecosystem.

*Collaboration and Cooperation* – Collaboration across jurisdictions and all sizes and types of financial entities may enable entities to learn from one another and mitigate the risk of fragmented approaches, thereby enhancing interoperability. Additionally, collaboration with third-parties may enable active management of third-party dependencies and address the availability of third-party solutions in advance of proposed timelines, especially for smaller institutions with higher levels of vendor dependency.<sup>6</sup>

### Transition Activities and Associated Outcomes

---

<sup>4</sup> Including domestic and international organizations such as the National Institute of Standards and Technology (NIST), the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Canadian Forum on Digital Infrastructure Resilience (CFDIR), the UK National Cyber Security Centre (NCSC), and the European Quantum-Safe Financial Forum (EU-QSFF).

<sup>5</sup> These frameworks are anchored in the concept of critical functions developed by the Financial Stability Board (FSB) and informed by Business Impact Analyses (BIA) conducted within organizations. The determination of “critical systems” within private-sector entities remains primarily the responsibility of the entities themselves. Public authorities may identify specific systems where they operate sectoral infrastructures (e.g. clearing or settlement platforms).

<sup>6</sup> Overcoming barriers related to limited transparency, including obtaining detailed vendor roadmaps for specific cloud and cryptographic services, can be essential to enable effective planning and prioritization.

## TLP: CLEAR



The table below outlines considerations for key migration activities and associated outcomes, organized within broad transition phases, for planning by both financial entities and authorities. Recognizing that some financial authorities also operate as financial entities, these activities and phases may overlap. While presented in a sequential format, the migration activities are not intended to follow a rigid or linear progression. Many activities may occur in parallel or be revisited iteratively. Each organization may tailor the timing and sequence of actions based on its risk profile, system complexity, and criticality. This phased approach provides a shared reference for planning and coordination—not a prescriptive path.

Key Migration Activities and Outcomes	Potential Activities for Financial Entities	Potential Activities for Public Authorities
<b>1. Awareness &amp; Preparation</b>	Executive-level risk awareness and initial post-quantum resilience strategy, and defined key roles.	Executive-level awareness of post-quantum cyber risks and implications.
	Mapped critical systems, functions, sensitive data, and communication protocols.	Clear communication of risks, expectations and/or guidance to their stakeholders.
<b>2. Discovery &amp; Inventory</b>	Comprehensive inventory of cryptographic assets, communication protocols, and relevant third-party dependencies.	Assessment of system-wide post-quantum maturity across financial institutions and public sector.
	Identified gaps in people, processes, organization, and technology capabilities.	Clear communication of risks, effective practices, and/or guidance for stakeholders.
<b>3. Risk Assessment &amp; Planning</b>	Tailored migration plans for critical and less critical functions, including tools, standards and interoperability.	Clear communication to guide migration across financial institutions.
	Adapted internal processes for capability building, governance and risk management.	Enhanced communication among domestic and international stakeholders to support consistent regulatory approaches.
<b>4. Migration Execution</b>	Quantum-resistant solutions progressively deployed, starting with priority functions.	Monitoring and/or oversight of migration progress.
	Transition pace adapted to evolving quantum threat landscape.	Identifying and removing potential barriers and/or providing capacity building support.
<b>5. Migration Testing</b>	Migrated functions are tested.	Embedding of quantum-resistant considerations in regulatory approaches, as appropriate.
	Ecosystem-oriented quantum-resilience exercises performed.	Potential incorporation of quantum resilience considerations in testing and crisis coordination exercises.
<b>6. Validation &amp; Monitoring</b>	Continuous validation and ongoing improvement.	Adaptive policy frameworks reflecting the evolving quantum threat landscape.
	Incorporation of new cryptographic standards.	Continued support for industry capability refinement and knowledge dissemination.

In practice, many organizations have already initiated pilot implementations or integrated quantum-resistant cryptography components — for example, through hybrid key exchange in web infrastructure. This roadmap is not intended to delay or discourage such proactive adoption. On the contrary, organizations may benefit from beginning migration as soon as relevant products and standards become available and are validated for their specific use cases. Organizations may also benefit from incorporating a goal of cryptographic agility in their transition plans to adapt new cryptographic solutions for emerging threats and vulnerabilities.

In parallel with the activities described above, the following continuous ongoing activities may be considered to support effective migration. These ongoing lines of effort may continue in parallel throughout the entire migration process.

(1) **Governance and Risk Management:** Embedding quantum-resistant cryptography into existing organizational governance and public oversight frameworks, including, where relevant, supervisory and sectoral mechanisms to support implementation;

## TLP: CLEAR



(2) **Management of External Dependencies:** Monitoring maturity of quantum technologies, standards, tools, and threats; and

(3) **Stakeholder Dialogue:** Facilitating structured engagement to identify issues, share insights, and promote shared solutions.

### Considerations for Potential Timelines for Transition to Quantum-Resistant Cryptography

While the trajectory of quantum computing development is uncertain, it may be helpful for organizations to establish comparable migration timelines to ensure their milestones can be achieved prior to the availability of cryptographically relevant quantum computers (CRQCs). When defining implementation milestones, authorities and institutions may consider emerging benchmarking efforts led by standard-setting bodies, national cybersecurity agencies, industry coalitions, and others.

The G7 CEG assessed a variety of inputs to identify a challenging but prudent target time range to consider for the overall transition of the financial sector to quantum-resistant cryptography. While such a time range is non-authoritative and will need to evolve with the risk landscape, it may be helpful as a general target to communicate planning among jurisdictions. Current guidance from several jurisdictions, standards-setting bodies, and multilateral bodies often points to 2035 as an overall target date for quantum-resistant cryptography migration for governmental systems, private sector systems, or both.<sup>7</sup> This is generally consistent with the CEG's review of expert opinion and the timeline provided by some developers of quantum technologies for when a CRQC might be developed and the consideration that under a "harvest now, decrypt later" scenario, data may be at risk even if it is intercepted well before the emergence of a CRQC.<sup>8</sup> This also recognizes the reality of the potentially long lead times needed for the safe and sound cryptographic transition of systems based on input received by the G7 CEG. In addition, prioritizing systems determined to be the most critical (for example, by addressing them in 2030-32) will limit the downside risk of the risks being realized early.<sup>9</sup>

Target dates are subject to change based on changes in the risk environment. These timelines may be adapted by each organization based on factors such as the evolving threat landscape, criticality of data and systems, and the complexity of migration. Other factors include the maturity of quantum-resistant cryptographic standards, and applicable regulatory expectations.

---

<sup>7</sup> The National Institute of Standards and Technology (NIST) is establishing strategic timelines for transitioning to quantum-resistant cryptography to inform the efforts and timelines of government agencies, industry, and standards organizations. NIST also released a cybersecurity white paper that provides a detailed review of current approaches for achieving cryptographic agility, highlighting the importance of timely transition and noting that "this transition will certainly not be the last one required." The International Organization for Standardization (ISO) and Internet Engineering Task Force (IETF) have developed cryptographic standards and specifications for cryptographic and security protocols covering cybersecurity and privacy protection. The Bank for International Settlements (BIS), World Economic Forum (WEF), Canadian Forum for Digital Infrastructure Resilience (CFDIR), UK's National Cyber Security Centre (NCSC) and Cross Market Operational Resilience Group (CMORG), European Commission, Europol Quantum Safe Financial Forum (QSFF), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and others have summarized approaches and timelines for post-quantum cryptographic migration.

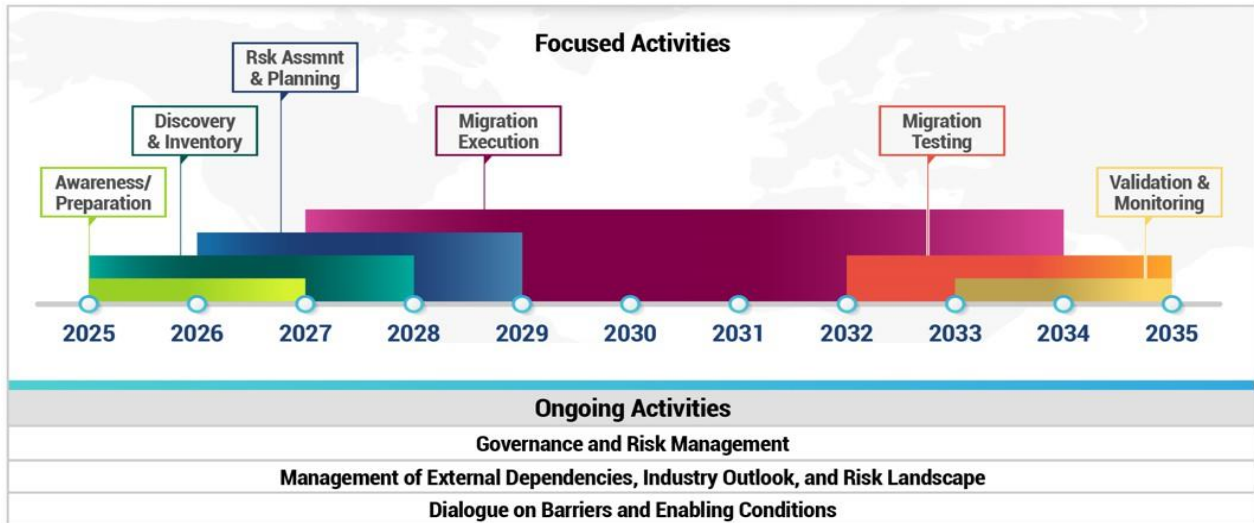
<sup>8</sup> For example, see Global Risk Institute and evolutionQ Inc. [Quantum Threat Timeline Report 2024](#).

<sup>9</sup> A dual-track approach encourages institutions to consider a risk-based prioritization of their systems and data assets rather than prescribe fixed timelines. The period 2030-32 is reflective of the variety of envisaged approaches taken across G7 jurisdictions on the migration of critical systems.

## TLP: CLEAR



The figure below presents a sample, illustrative visual summary of the quantum-resistant transition of a notional non-critical system at a financial entity. Financial entities may consider developing and applying other roadmaps similar to this one based on the criticality of the systems for which they are responsible and their unique circumstances.



The G7 CEG encourages financial authorities and financial entities to:

- Consider integrating these approaches into existing governance and risk management frameworks and technology strategies, with sustained executive engagement.
- Consider prioritizing migration planning based on exposure and systemic importance to contribute to collective resilience.
- Consider integrating the success factors outlined in this roadmap within organizational plans to guide implementation.

The G7 CEG reaffirms its commitment, in cooperation with financial authorities, to:

- Monitor progress with post-quantum cryptography migration and share information across jurisdictions, support transitional efforts, and encourage jurisdictional consistency. As the technology and our understanding of it develops, timelines may be revisited as needed.
- Coordinate with standard-setting bodies and other key stakeholders to promote international cooperation.
- Facilitate dialogue and knowledge sharing across critical infrastructure sectors and with technology providers to accelerate preparedness.
- Monitor evolving threats, technology, and migration lessons learned and consider updating resources to support organizations.