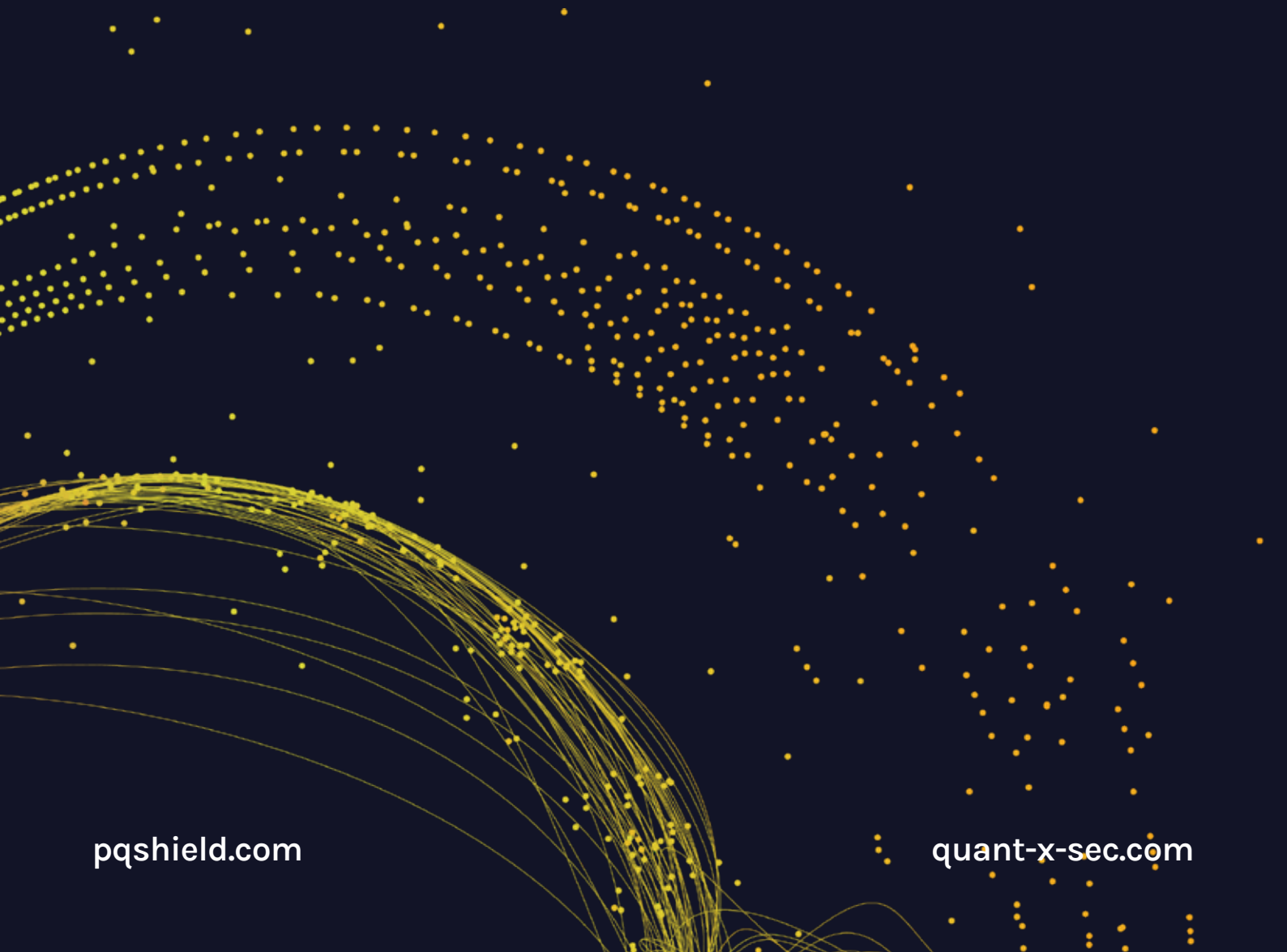
PQ SHIELD

QUANT-X SECURITY & CODING

# The Financial Market's Transition to Post-Quantum Cryptography



pqshield.com

quant-x-sec.com

# Executive Summary

Almost every individual and organization heavily rely on the financial market's highly secured and performing digital infrastructures, a combination which is a challenge in itself. Cryptography plays an essential role for both aspects. The development of new high performing technologies always initiated a shift in cryptography requirements. While some of those shifts can be realized by adjustments of existing cryptographic algorithms, the development of quantum computers demands a paradigm shift in cryptography. The Project Leap of the Bank for International Settlement states:

"Quantum computers represent a serious threat for the financial system […]. While functional quantum computers are not yet available, the security threat needs to be urgently addressed. Already, malicious actors can intercept and store confidential, classically encrypted data with the intention of decrypting it later when quantum machines become powerful enough to do so. This means that data stored or transmitted today are, in fact, exposed to "harvest now, decrypt later" attacks by a future quantum computer. The long term sensitivity of financial data means that the potential future existence of a quantum computer effectively renders today's systems insecure."[1]

We would like to add that quantum computers already exist[2], and that malicious actors and secret services are already collecting confidential, classically encrypted data. Whilst today's quantum computers are not yet capable of breaking classic encryption, this is forecasted to change in the coming decade. Which will not only allow attacks on non-quantum safe financial infrastructure, but also enable attackers to then decrypt and misuse all the data that they are already collecting today.

The current geopolitical situation increases the severity of the quantum threat as cyberwars are used to sabotage or even take over critical infrastructures. The involved state motivated attackers act under long-term strategies of their governments. The development of quantum computers in a geopolitical context is therefore also referred to as "war race".

A mitigation of the inherent risk is offered by post-quantum cryptography (PQC), sometimes known as quantum-proof, quantum-safe or quantum-resistant cryptography: cryptographic algorithms (usually public-key algorithms) that have been specifically designed to defend against attacks by quantum computers. For the last eight years, a concerted effort has been made to develop and standardize these algorithms, resulting in the recent ratification of the NIST Post-Quantum Cryptography Standard[3]. Worldwide, governments and regulatory bodies recognize this standard, and are working on regulations that mandate the transition to post-quantum cryptography.

This whitepaper summarizes the current state of the PQC standards and the governmental regulations, outlines generic financial market specific threats that can be mitigated by post-quantum cryptography and proposes mitigation measures.

[1] Bank for International Settlement (BIS) report: Quantum-proofing the financial system, https://www.bis.org/publ/othp67.pdf
[2] IBM Quantum Roadmap, https://www.ibm.com/roadmaps/quantum/
[3] https://pqshield.com/the-new-nist-pqc-standards-are-here/

# Quantum Threats to the Financial Market

Identification of organization-specific threats by quantum computers and their inherent risks follows the principles of any IT risk management process, including the long term confidentiality aspect of the involved data. Designing a roadmap for the implementation of post-quantum security in heterogeneous infrastructures is an individual process for each organization. However, there are some risks which apply to the financial market in general. The protection goals confidentiality, integrity and availability apply to data with high and critical ratings, such as financial transactions, personal and technical sensitive data. The long term confidentiality of financial transactions might not be critical for an individual's grocery purchases, but it is critical for many other use cases such as the purchase of medical products or financial business transactions. Furthermore, the threat of zero day vulnerabilities or exploits in the context of static public key cryptography for financial transactions comes with a critical inherent financial risk for any bank. The timeliness of adequate post-quantum security implementation can have an existential impact on a financial organization.

Advanced persistent threats (APT) and internal threats apply to post-quantum cryptography just as they do to classical cryptography. A compromised private key can cause catastrophic events in financial infrastructures. For example, an attacker can impersonate any account and initiate illegitimate transactions with a leaked SAML or OAuth signature key. Here are some threats that could cause the compromise of a private key:

- admin account misusage
- leaked admin or non-personal account credentials
- any malware which is designed to extract private cryptographic keys, such as Emote or mimikatz[4]

We recommend including APT scenarios into the quantum threat modeling, and also think about scenarios that apply to crypto agility and related changes.

# The NIST Post-Quantum Cryptography Standard

Since 2016, the NIST Post-Quantum Cryptography Project[5] has been working towards the standardization of multiple PQC algorithms, which recently resulted in ratified FIPS standards.

ML-KEM[6] (FIPS 203, aka CRYSTALS-Kyber) is the standard for public-key encryption and key encapsulation mechanisms, while ML-DSA (FIPS 204, aka CRYSTALS-Dilithium) has been selected as the standard for digital signatures.

These algorithms have explicitly been selected with an eye on mass-market applicability, as they have very reasonable requirements regarding computing performance, key size and cybertext size.

[4] https://gitbook.seguranca-informatica.pt/credentials-exfiltration/extracting-certs-private-keys-from-windows-using-mimikatz-and-intercepting-calls-with-burpsuite
[5] https://csrc.nist.gov/projects/post-quantum-cryptography
[6] https://pqshield.com/new-whitepaper-the-new-nist-standards-are-here-what-does-it-mean-for-pqc-in-2024/

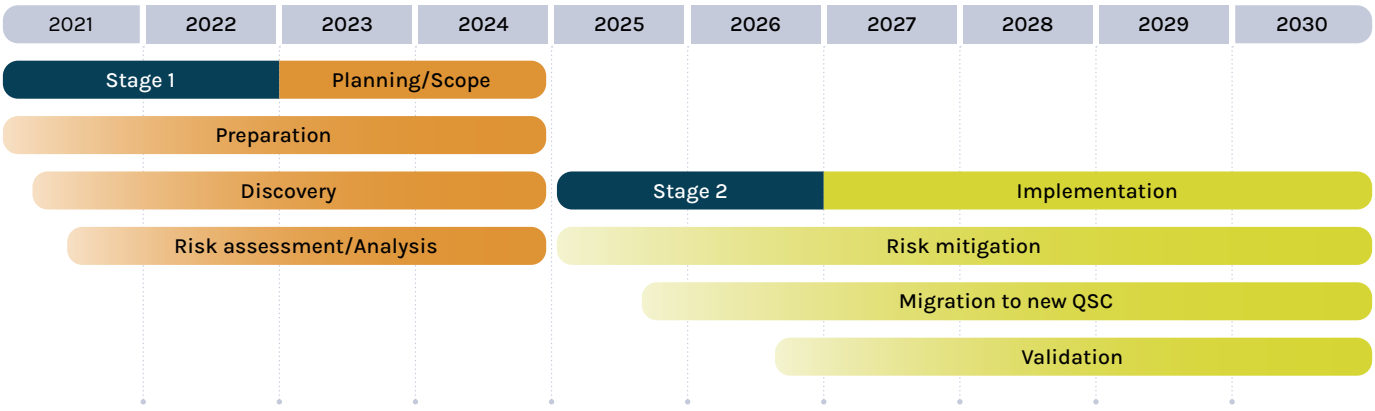
All three aspects are crucial for complying with the EU NIS 2 directive[7] which translates to requirements for fast transactions and high system availability. Financial transactions are hardly ever simple peer to peer data transfers. Usually, there are several instances involved besides the banks of the sender and receiver. Considering that the transactions are often protected by multi-layer hybrid and public key cryptography, it is crucial to implement efficient algorithms and ensure smooth digital processes in the whole transaction chain.

## The Quantum Timeline

It's thought that 'Q-Day', the date when quantum computers will be powerful enough to break today's cryptography, will happen within the next decade. For high security systems, the German Federal Office for Information Security (BSI) is predicting that cryptographically relevant quantum computers could be available in the early 2030s[8]. McKinsey's 2024 Quantum Technology Report[9] suggests that Q-Day will be between 2027 and 2035.

The time for action is now: Considering that the adoption and rollout of quantum-safe cryptography could take multiple years for planning, implementation and verification, it's best to think of Q-Day as the point of completion, and consider the timeline between now and then.

For example, the recommended timeline of the Canadian National Quantum-Readiness Working Group[10] suggests the following:




What's more, it's possible that even now, a potential adversary could steal and harvest sensitive data with a view to decrypting and misusing it later, when the technique becomes available. All data, whether historical or current, is already at risk today unless protected by quantum-safe security.[11]

[7] https://digital-strategy.ec.europa.eu/de/policies/nis2-directive
[8] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4
[9] Slide 88, available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/
[10] https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf
[11] https://www.ibm.com/quantum/quantum-safe

# PQC adoption initiatives around the world

As with all technological advances, the adoption of post-quantum cryptography is necessary not only for security, but also for compatibility. Worldwide, governments and standardization bodies have been working on schedules for the PQC adoption.[12]

In fact, for US government agencies, there is already a mandatory schedule[13] to move to PQC. Additionally, both the French national security agency (ANSSI) and the Canadian Forum for Digital Infrastructure Resilience (CFDIR) recommended the immediate introduction of post-quantum defenses throughout the private sector, and Germany's BSI has already endorsed the use of post-quantum cryptography.

| Country | PQC algorithms under consideration | Published guidance | Timeline (summary) |
|---|---|---|---|
| Australia | NIST | CTPCO (2023) | Start planning; early implementation 2025-2026 |
| Canada | NIST | Cyber Centre (2021) | Start planning; implementation from 2025 |
| China | China Specific | CACR (2020) | Start Planning |
| European Union | NIST | ENISA (2022), European Commission (2024) | Start planning and mitigation |
| France | NIST (but not restricted to) | ANSSI (2023) | Start planning; transition from 2024 |
| Germany | NIST (but not restricted to) | BSI (2022) | Start planning |
| Japan | Monitoring NIST | CRYPTREC (2022, 2024) | Start planning; initial timeline |
| Netherlands | AES, monitoring NIST, SHA-DSA-256 and XMSS | NCSC (2023) | Draft action plan with time frames |
| New Zealand | NIST | NZISM (2022) | Start planning |
| Singapore | Monitoring NIST | MCI (2022), Monetary Authority of Singapore (2024) | Start planning |
| South Korea | KpqC | MSIT (2024) | Second selection round 2024 |
| United Kingdom | NIST | NCSC (2023) | Start planning; implementation from 2024 |
| United States | NIST | CISA (2021, 2022, 2023), NIST (2023), NSA (2022, 2024), White House (2022, 2024), Congress (2022) | Implementation 2023-2033 |

[12] Management summary: https://www.gsma.com/newsroom/wp-content/uploads//PQC-Guidelines-for-Telco-Use-Cases-Executive-Summary.pdf Full document: https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf

[13] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_%20ALGORITHMS_.PDF

# Global Regulatory Approaches for the Financial Market

With the Financial Market both being a critical infrastructure and handling highly sensitive Personally Identifiable Information (PII), its security is of highest importance. The 2024 whitepaper "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches"[14] by the World Economic Forum summarizes the current state and advises on actions towards the transition to PQC.

Europe already has a number of laws, regulations and directives in force that require state-of-the-art cybersecurity for financial institutions, including

- **The EU Critical Entities Resilience Directive (CER, EU Directive 2022/2557)**[15] intends to enhance resilience to risks that could impact the provision of essential services for the society and economy, including energy, transport, banking, financial market, digital infrastructure, public administration, water, food, and space. It is in force since 2023, entity compliance is required by 2026 … 2027.

- **The EU General Data Protection Regulation (GDPR)**[16] is a data privacy and security law, protecting Personally Identifiable Information (PII). It is already in force and imposes very severe penalties up to 4% of yearly revenue for non-compliance and data leaks.

- **The Digital Operational Resilience Act (DORA, EU Regulation 2022/2554)**[17] demands information and communication technology (ICT) risk management requirements for financial institutions. The draft regulation has been released, the final regulation is expected to be in force early 2025.

- **The Revised Directive on Security of Network and Information Systems (NIS 2, EU Directive 2022/2555)**[18] requires cybersecurity measures for energy, transport, banking, financial market infrastructures, water, healthcare and digital infrastructure, imposing very severe penalties for non-compliance, including personal liability for managers. It is the successor of the current NIS Directive and expected to be in force in October 2024.

- **The Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (April 2024)**[19] encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition

As a non-european example, the Monetary Authority of Singapore released an "Advisory on Addressing the Cybersecurity Risks Associated with Quantum"[20] in February 2024.

[14] https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/
[15] https://www.deloitte.com/cbc/en/services/risk-advisory/perspectives/navigating-the-eu-critical-entities-resilience-directive.html
[16] https://gdpr.eu/what-is-gdpr/
[17] https://www.digital-operational-resilience-act.com/
[18] https://www.nis-2-directive.com/
[19] https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/
[20] https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf

# How To Act

The outcome of the initiative Project Leap provides guidance to other organizations in the financial sector. It enables faster transition by less trial and error scenarios within the migration to post-quantum security in financial digital infrastructures.

The first phase of “Project Leap: Quantum-proofing the financial system”[21] of BIS Innovation Hub, Deutsche Bundesbank, and Banque de France in June 2023 successfully established a quantum-safe environment in a financial systems context. A second phase of Project Leap is planned in order to investigate more network architectures, test different types of hardware, and incorporate additional communications layers to build a complete chain of trust, as well as to include additional central bank processes.

Further, the Europol Quantum Safe Financial Forum (QSFF)[22] has been founded in April 2024 to drive the transition to PQC in the financial sector.

Now it is the responsibility of each organization to implement post-quantum cryptography in their own infrastructures. A sensible approach is to integrate the imminent “harvest now, decrypt later” threat to the regular risk management processes according to the applicable global and local standards, such as the NIST risk management framework, the BSI risk management standard 200-3 and MaRisk for German banks. The inherent risks for the organization need to be evaluated in a joint effort of 1st and 2nd line of defense representatives from business, IT security and risk management departments.

The inherent risks can be of financial, regulatory, customer, staff or reputational nature, depending on the business case, processed data and users of an IT asset or service. For an efficient evaluation of the asset specific “harvest now, decrypt later“ risk and identification of adequate post-quantum security implementation, cryptographic information needs to be added to the configuration management database for the whole IT stack of the IT asset. This applies to all asset types, such as internal and external software, middleware, on premise and cloud IT infrastructure and OT/IoT infrastructure.

Integration of post-quantum security to crypto agility concepts is the base for all following post-quantum security implementations. Cryptography for data in transit must mostly be compatible with at least two systems and organizations. Therefore, it is also important to define process interfaces with business partners and service providers for cryptographic changes in the commonly used digital connection.

We also recommend re-evaluating existing APT mitigation measures in the scope of post-quantum security implementation. This concerns the cryptographic key and certificate management as well as regular related admin and non-personal account password rotation.

Last but not least, responsibilities need to be assigned to the remediation teams and emergency response teams. We also recommend implementing proof of concepts for various use cases that are not urgent in order to collect experience. It might be necessary to act quickly in case of unexpected events.

[21] https://www.bis.org/publ/othp67.pdf
[22] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff

# About the Authors


## Burkhard Jour, PQShield

Burkhard Jour is Sales Director Europe of PQShield (www.pqshield.com), the worldwide leader in high-quality hardware and software implementations of post-quantum cryptography. He combines a strong engineering background covering embedded software and hardware with 30+ years of experience in sales and project management in the areas of real-time control, telecommunications, and security solutions.

**Get in touch** contact@pqshield.com | www.pqshield.com


## Xenia Bogomolec, Quant-X Security & Coding

Xenia is the founder of Quant-X Security & Coding (www.quant-x-sec.com), an SME that specializes in post-quantum security integration to critical infrastructures. She consults critical infrastructure providers, mainly banks, in IT risk governance and IT security within software engineering and infrastructure migration projects since 2015. Quant-X Security & Coding also coordinates the consortium Quant-ID - Quantum Secure Digital Identities[23], which is funded by the German Government.

**Get in touch** xb@quant-x-sec.com | www.quant-x-sec.com

[23] https://quant-id.de/