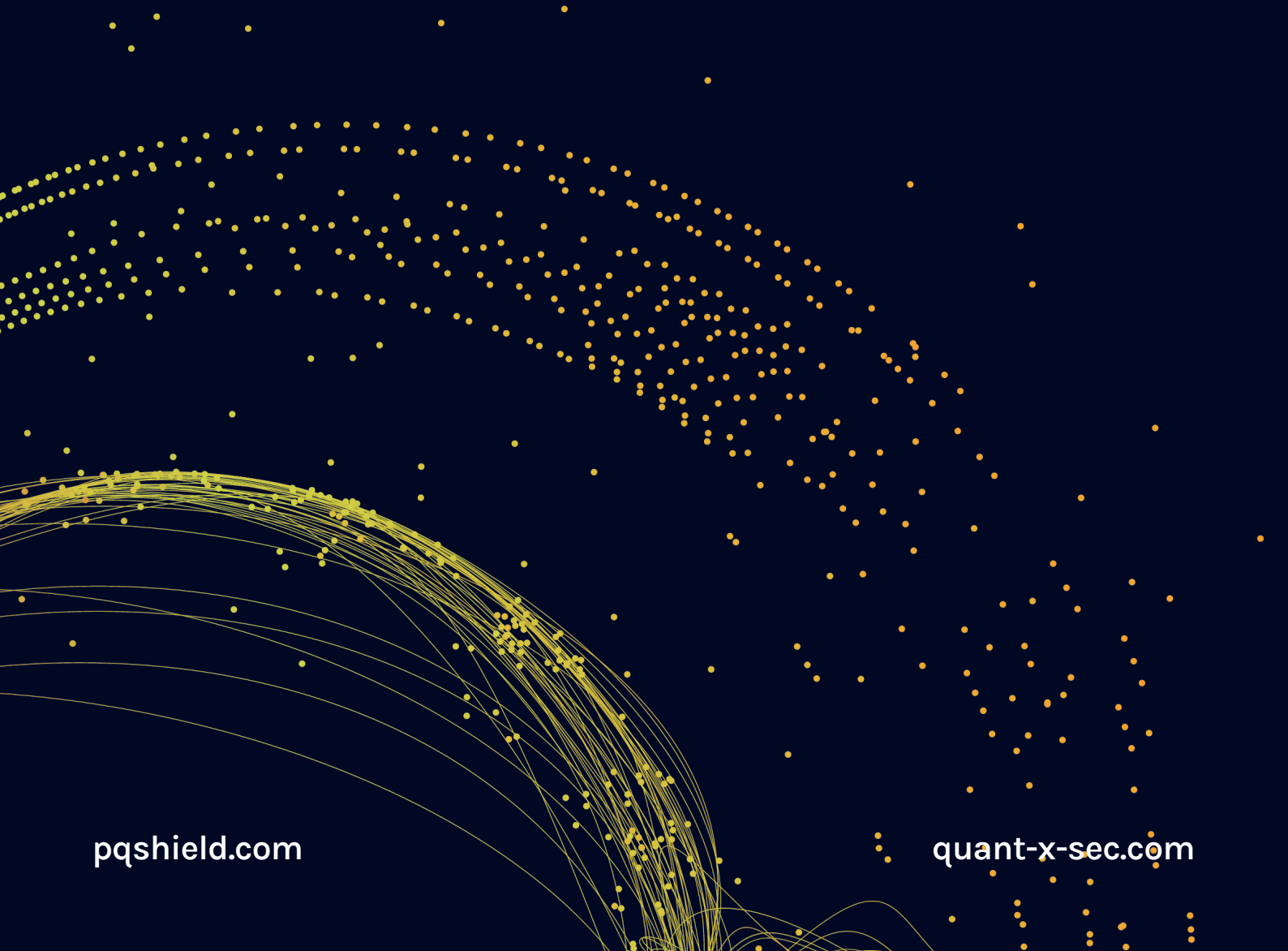
PQ SHIELD

QUANT-X SECURITY & CODING

The Financial Market's Transition to Post-Quantum Cryptography



pqshield.com

quant-x-sec.com

Executive Summary

Almost every organization relies heavily on the financial market's highly secure and high-performing digital infrastructures - a combination which is often a challenge in itself. Cryptography plays an essential role for both aspects. The development of new technology always initiates 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]

Quantum computers already exist[2] and malicious actors are already collecting confidential, classically encrypted data. While today's quantum computers are not yet capable of breaking classic encryption, this is forecasted to change in the coming decade, not only enabling attacks on non-quantum-safe financial infrastructure, but also allowing 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. State-motivated actors can already act under the long-term strategies of their respective governments. The development of quantum computers in a geopolitical context is therefore also often referred to as a "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: PQC includes cryptographic algorithms (usually public-key algorithms) that have been specifically designed to defend against attacks by quantum computers. For the last few years, a concerted effort has been made to develop and standardize these algorithms, resulting in the recent ratification of new NIST Post-Quantum Cryptography Standards[3].

Worldwide, governments and regulatory bodies recognize these standards, 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 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 data involved. 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 that apply to the financial market in general. The protection goal of protecting confidentiality, integrity and availability applies to data with high and critical rating, 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 (for example), 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 an inherent but critical financial risk for any bank. Timely but adequate post-quantum security implementation can clearly 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 have a catastrophic effect on financial infrastructures. For example, an attacker could impersonate any account and initiate illegitimate transactions with a leaked SAML or OAuth signature key. Threats that could cause the compromise of a private key include:

- Admin account misusage
- Leaked admin or non-personal account credentials
- Any malware designed to extract private cryptographic keys, such as Emote or mimikatz[4]

We recommend including APT scenarios into the quantum threat model, and considering scenarios that apply to crypto agility and related changes.

The NIST PQC standards

Since 2016, the NIST Post-Quantum Cryptography Project[5] has been working towards the standardization of multiple PQC algorithms, resulting in ratified FIPS PQC 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. Additionally, SLH-DSA (FIPS 205, aka SPHINCS+ has also been standardized as a hash-based digital signature algorithm.

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

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 rarely simple peer-to-peer data transfers. Usually, there are several instances involved, in addition to the banks of the sender and receiver.

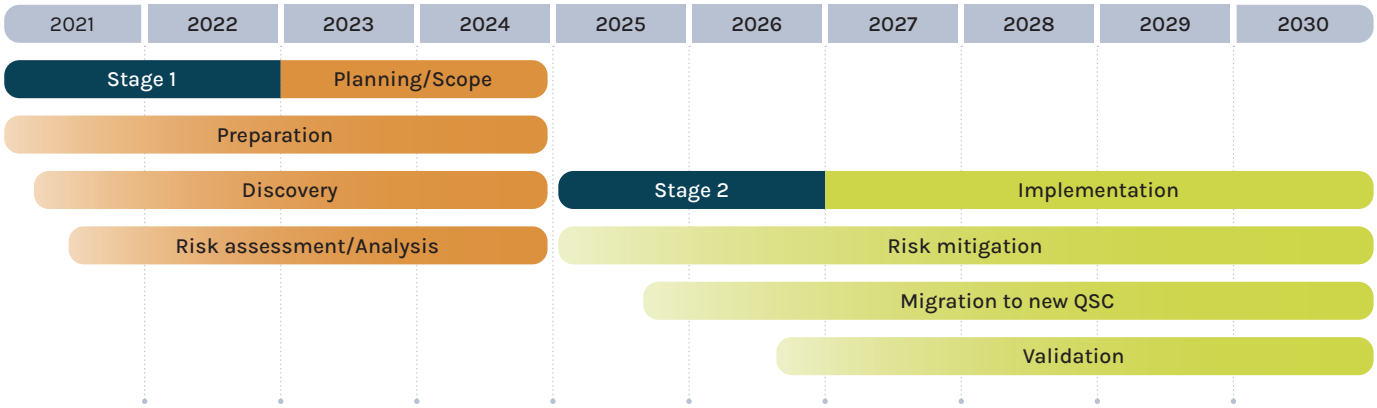
Considering that transactions are often protected by multi-layer hybrid and public key cryptography, it is crucial to implement efficient algorithms and ensure smooth digital processes in the transaction chain.

[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/
[7] https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

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]. In fact, McKinsey's 2024 Quantum Technology Report[9] suggests that Q-Day will be somewhere between 2027 and 2035.

Clearly, 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 a two stage plan for preparation, discovery, risk assessment, followed by implementation from 2025 onwards.



Other bodies around the world are suggesting similar roadmaps for transition. 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.

In March 2025, the UK's National Centre for Cyber Security (NCSC) also released updated guidance on PQC migration in its publication, Timelines for migration to post-quantum cryptography - specifying three key milestones for 2028, 2031, and 2035.

- **By 2028 - Define migration goals and build an initial plan.** This phase includes assessing services and infrastructure to plan for upgrade to PQC, and could include assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded.
- **By 2031 - Early, high-priority migration activity.** The NCSC also suggest refining the plan to show a 'thorough roadmap' for completion of migration.
- **By 2035 - Complete migration of PQC to all systems, services and products.** While some rarely-used technologies might be harder to upgrade by this deadline, NCSC points out that all organizations should work towards this target.

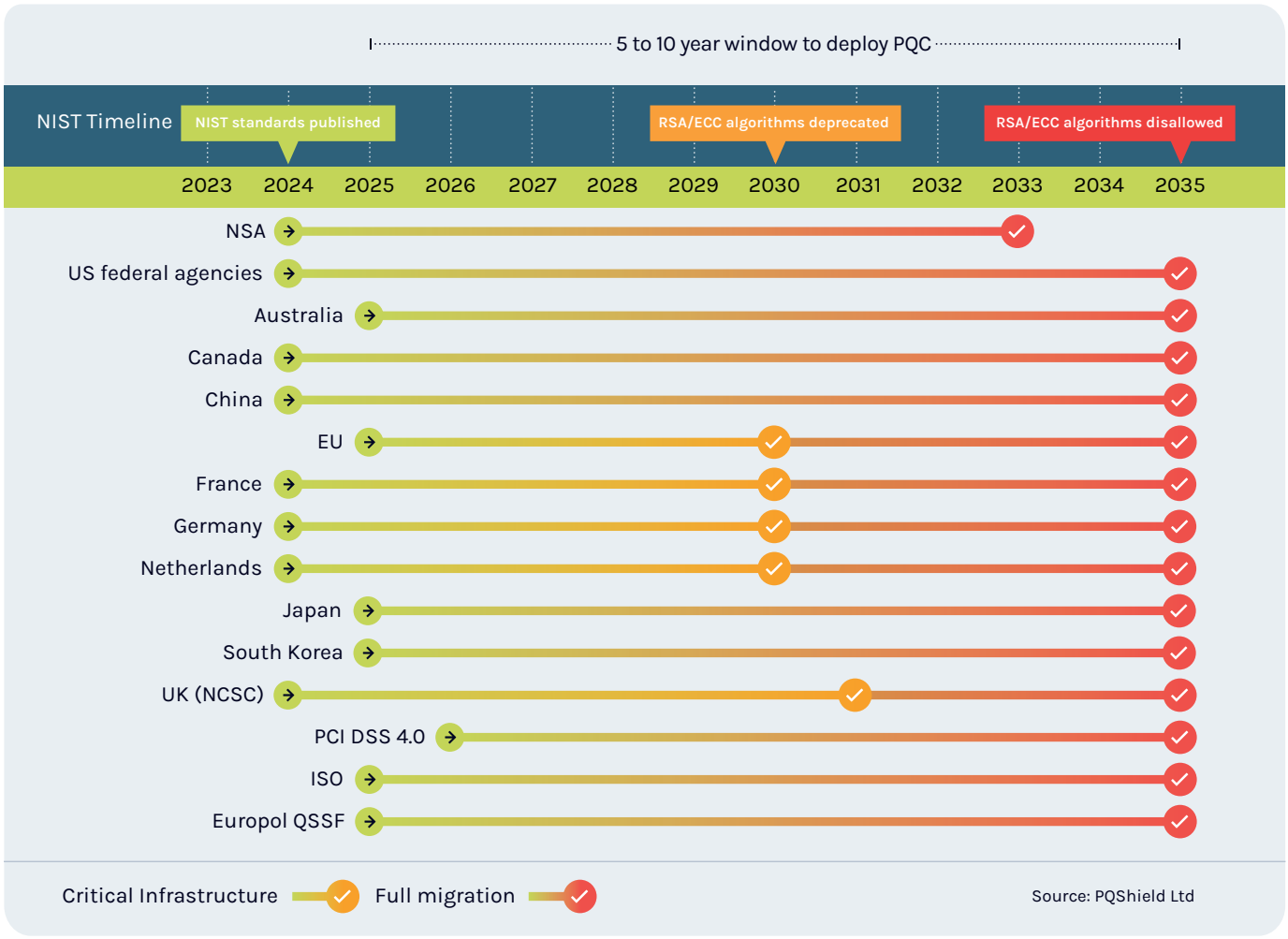
The only conclusion is that all data, whether historical or current, is already at risk today unless protected by quantum-safe security.[11]

[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 and compliance. Worldwide, governments and standardization bodies have been working on schedules for 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) have recommended the immediate introduction of post-quantum defenses throughout the private sector, and Germany's BSI has endorsed the use of post-quantum cryptography. Around the world, the story is a similar one, with governments and regulatory bodies planning for transition along a timeline:



[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

As well as being part of critical infrastructure, the financial market handles highly sensitive PII (Personally Identifiable Information). 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 in particular, 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]
  This directive intends to enhance resilience to risks that could impact the provision of essential services for society and the economy, including energy, transport, banking, financial market, digital infrastructure, public administration, water, food, and space. It has been in force since 2023, and entity compliance is required by 2026/2027.

- **The EU General Data Protection Regulation (GDPR)**[16]
  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 noncompliance and data leaks.

- **The Digital Operational Resilience Act (DORA, EU Regulation 2022/2554)**[17]
  The Act mandates information and communication technology (ICT) risk management requirements for financial institutions - including identifying, assessing and planning appropriate mitigation strategies against threats. The legislation entered into force in January 2025.

- **The Revised Directive on Security of Network and Information Systems (NIS 2, EU Directive 2022/2555)**[18]
  This directive 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 previous NIS Directive and came into force in October 2024.

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

As a non-European example, the Monetary Authority of Singapore released guidance entitled: "Advisory on Addressing the Cybersecurity Risks Associated with Quantum"[20] in February 2024. There are many more examples around the world from organizations pushing for resilience in updated regulations.

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

The first phase of “Project Leap: Quantum-proofing the financial system”[21] of BIS Innovation Hub, Deutsche Bundesbank, and Banque de France (June 2023) successfully established a quantum-safe environment in a financial systems context. A second phase of Project Leap is planned 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. Furthermore, the Europol Quantum Safe Financial Forum (QSFF)[22] (April 2024) is also driving the transition to PQC in the financial sector.

It is the responsibility of each organization to implement post-quantum cryptography in their infrastructures. Regulators are likely to signpost existing policy, so it’s important not to wait for specific new regulations, but to identify your at-risk data early.

A sensible approach is to integrate the “harvest now, decrypt later” threat to the regular risk management processes according to the applicable standards, such as the NIST risk management framework, the BSI risk management standard 200-3, MaRisk for German banks.

Organizational risks should be evaluated in a joint effort of first and second line-of-defense representatives from business, IT security and risk management departments. It’s likely that your highest-risk data will be the most vulnerable and will need identifying early. It’s also important to assess your infrastructure by vendor - in reality, 80% of the issues will be components provided by the supply chain.

The inherent risks can be of financial, regulatory, customer, staff or reputational nature, depending on context. For an efficient evaluation of the asset-specific “harvest now, decrypt later“ risk, and identification of adequate PQC 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 or OT/IoT infrastructure.

With crypto agility in mind, cryptography for data in transit must be mostly compatible with at least two systems and organizations. Therefore, it's also important to define process interfaces with business partners and service providers.

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

Finally, responsibilities need to be assigned to the remediation teams and emergency response teams. It’s likely that you will need dedicated and expert help, both internally and externally - migration is a project that needs support all the way up to the board room.

We also recommend implementing proof of concepts for various use cases that are not urgent in order to collect experience. Prioritize and plan. If you act now, it will be far easier to make this transition over multiple years, managing costs and avoiding crisis-driven deployments.

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

About the Authors

PQSHIELD

PQShield is a post-quantum cryptography (PQC) company that builds quantum-safe solutions designed to safeguard sensitive data against the threat of quantum computing. With quantum computers potentially capable of breaking current encryption algorithms, industry leaders are increasingly collaborating with organizations such as PQShield to ensure the transition to the quantum era. PQShield's focus is on the delivery of fast, secure, real-world implementations of quantum-safe cryptography.

Headquartered in the UK, we're a team of world-leading implementation engineers, cryptographers, mathematicians and specialists. We build solutions for hardware, software, applications and devices, and our products are flexibly designed to optimize speed and performance. We believe in staying ahead of the attackers, preserving confidentiality, accessibility, and integrity in every transaction.

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

QUANT-X SECURITY & CODING

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