

Post-Quantum Cybersecurity

Enhancing your Resilience for the Quantum Era



QuRISK offers you expert guidance through quantum challenges and opportunities, charting safe paths to success and unlocking new horizons.

We aim at **supporting you through two necessary and complex processes**, with our step-by-step offers, tailored to your specific needs:

the QUANTUM RESILIENCE journey

to mitigate the threat on data and communication security posed by the advent of quantum computers.

the QUANTUM ADOPTION journey

to strategically help you safely integrating quantum technology and gain a crucial competitive advantage in the coming decade.

Our experts continuously advance research and expertise in Quantum Risk and Cybersecurity , through our **Quantum Risk & Cybersecurity Lab (QuLab)** ensuring that our services are grounded in deep knowledge and practical innovation.

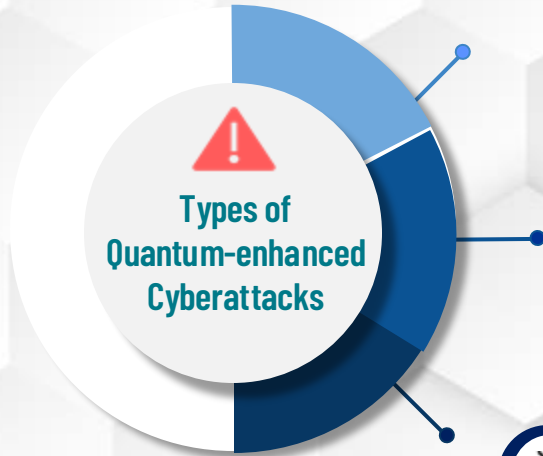
Will Quantum computers compromise current cryptography schemes?



It's not about *if*, it's about *when* !

> Understanding Quantum Cyber-Threat

Today, **a classical computer would take centuries to break strong encryption protocols** (like RSA-2048), whereas **a fully efficient Quantum computer is expected to do it in a more reasonable time.**



Quantum FACTORING ATTACKS

Shor's Quantum algorithm could potentially break public key cryptosystems (RSA, ECDSA, DSA, DH...) by solving the hard math problem of factoring large number in an extremely short time which will give the attacker the possibility to retrieve a private key from a public one.



Quantum BRUTE FORCE ATTACKS

Grover's Quantum algorithm could potentially perform brute force attacks much (quadratically) faster than classical computers, which could compromise the data encrypted with symmetric key algorithms (Twofish, Serpent, AES, Camellia, Salsa20, ChaCha20, Blowfish...).



Quantum RANSOMWARE ATTACKS

A Quantum ransomware would be a ransomware bolstered by a quantum random number generation (QRNG), which could enhance its ability to encrypt data and spread faster within targeted networks.

> Discover Emerging Quantum-Resistant Solutions

Quantum computers did not reach yet their optimal damaging capability. Nevertheless, **it is important to act now because:**

- **Experts are expecting important technological breakthroughs within the decade**
- **HNDL** (*Harvest Now, Decrypt Later*) cyberattacks are very common and very problematic for sensitive data

Fortunately, promising **Quantum-resistant solutions** are beginning to emerge, such as:

Post-Quantum Cryptography

*New encryption protocols
considered resistant to
Quantum Cyber attacks.*



Quantum Cybersecurity

*Secured communication
networks based on Quantum
properties.*



The US National Institute of Standards and Technology (NIST) has selected and standardized several Post-Quantum Cryptography (PQC) protocols, which are now recommended for adoption.

> "Securing Tomorrow, Today"

There's a growing consensus among global regulators: organizations are urged to start planning their PQC migration now, to proactively address future quantum cyber threats and safeguard critical infrastructures security.

In **Europe**, the European Commission released in June 2025 **"A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography"**, setting out a unified plan for Member States and critical sectors to embrace quantum-resilient solutions and ensure a secure transition over the coming decade.

EU First Milestone: 31/12/2026

- ✓ Identify and involve stakeholders
- ✓ Support mature cryptographic asset management
- ✓ Create dependency maps
- ✓ Perform quantum risk analysis
- ✓ Include the supply chain
- ✓ Create an awareness and communication program
- ✓ Develop a timeline and an implementation plan

EU Second Milestone: 31/12/2030

- ✓ Complete PQC transition for high-risk use cases
- ✓ Plan PQC transition for medium-risk use cases
- ✓ Enable Quantum-safe upgrades by default



Your Quantum Resilience Journey

must be a gradual, well-planned, and aligned with your Business strategy

Quantum
Vulnerable

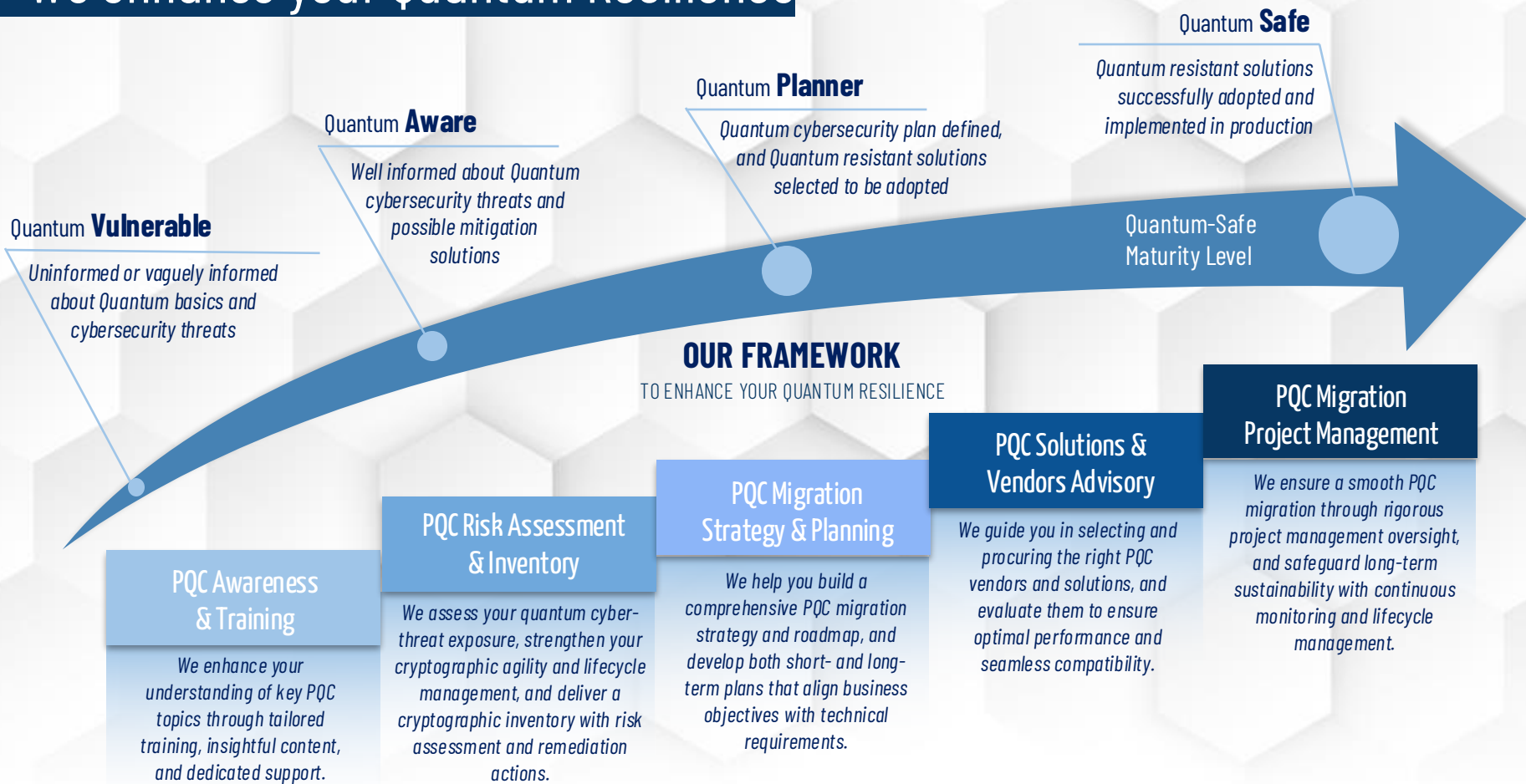
Quantum
Aware

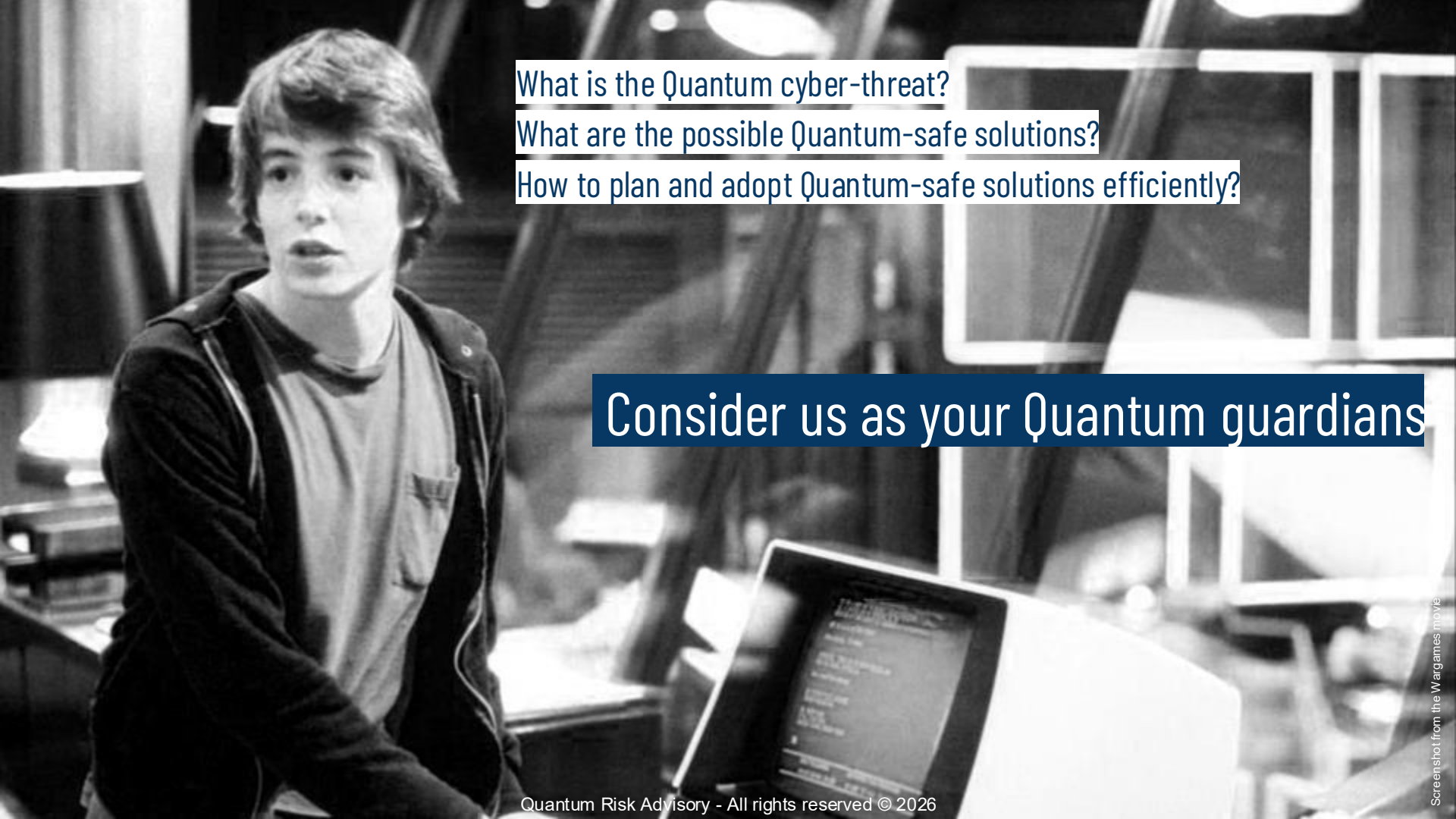
Quantum
Planner

Quantum
Safe

We advise you along the way

> We enhance your Quantum Resilience





What is the Quantum cyber-threat?

What are the possible Quantum-safe solutions?

How to plan and adopt Quantum-safe solutions efficiently?

Consider us as your Quantum guardians

> PQC Awareness & Training

We provide tailored **Post-Quantum Cybersecurity training and awareness sessions** designed **for a wide range of audiences**, including Cybersecurity, IT, Risk, Business, and Management, covering the following **topics**:

Overview to Quantum Computing

- > Introduction to Quantum computing
- > Quantum computing applications and use cases
- > Quantum computing evolution and forecasts

Quantum Cybersecurity Threats

- > Overview of current cryptography protocols
- > Explaining Shor's Quantum factoring algorithm
- > Understanding Quantum cyber threats toward current cryptography

Post-Quantum Cybersecurity

- > Quantum Cyber threats mitigation options (PQC & QKD)
- > Understanding Post-Quantum Cybersecurity (PQC)
- > Overview of NIST and other Post-Quantum Cryptography initiative

PQC Planning & Migration

- > Overview of PQC migration standards & regulations
- > PQC migration framework, methodology and project risk management
- > Technological and regulatory updates regarding PQC migration



Q-DAY* DISASTER RECOVERY PLAYBOOK

The training sessions conclude with an interactive workshop built around a **Q-Day*** **emergency scenario**. During this exercise, the animators engage participants from various corporate functions and asks: ***If Q-Day were happening today, what would you do?*** The insights collected during the workshops are then consolidated to formalize a dedicated Q-Day Disaster Recovery Playbook.

***Q-Day** is the day when quantum computers will be powerful enough to break today's public-key cryptography.

> PQC Risk Assessment & Inventory

We perform focused assessments and cryptographic mappings to provide a clear view of your cryptographic landscape, uncover gaps, prioritize risks, and lay the foundation for a secure and successful PQC migration.

QUANTUM CYBER THREAT EXPOSURE

We evaluate your level of exposure to quantum cyber threats and identify your organisation's vulnerability areas and attack surface, focusing on critical business data and cryptographic usage to prioritise PQC migration efforts.



CRYPTOGRAPHY LIFECYCLE ASSESSMENT

We evaluate your cryptographic assets and key lifecycle management, and assess your **crypto-agility**, your capacity to seamlessly transition to new cryptographic protocols when needed.



PQC MIGRATION READINESS ASSESSMENT

We evaluate your PQC migration maturity and identify key challenges, risks, and dependencies, delivering a report that consolidates findings and strategic recommendations to provide a clear view of your post-quantum readiness.

CRYPTOGRAPHY LANDSCAPE INVENTORY & ASSESSMENT

We map your cryptographic landscape to identify algorithms, keys, libraries, systems, secured data, and vendor dependencies, and assess them against quantum threats, hybrid options, and quantum-resistant equivalents.



> PQC Migration Strategy & Planning

To strengthen your immediate readiness, we help you develop short-term disaster recovery planning, and to secure your long-term post-quantum resilience, we design a comprehensive PQC migration strategy tailored to your organization's needs.



QUANTUM-SAFE & PQC MIGRATION STRATEGY PLANNING

We design a comprehensive strategy, consolidating all prior assessments to prioritize actions, allocate resources, and provide a clear roadmap for a secure and efficient transition to quantum-safe solutions (including Post-Quantum Cryptography).



Q-DAY* CONTINUITY & CRISIS MANAGEMENT PLANNING

We conduct a crisis management exercise simulating a Q-Day scenario, enabling your stakeholders to rehearse the disaster recovery playbook, strengthen coordination, and improve preparedness for a sudden quantum threat.

****Q-Day** is the moment when quantum computers will be powerful enough to break today's public-key cryptography.*

> PQC Solutions & Vendors Advisory

To ensure the success of your PQC migration, we help you select the right solutions and vendors, support you throughout the procurement process, and conduct comprehensive risk evaluations using our holistic 360-degree Risk Framework.

We will help you build:

- Suitable vendors selection process
- Resilient supply chain
- Comprehensive risk evaluation
- Internal expertise



> PQC Migration Project Management

Our Quantum Risk & Project Managers expertly guide you through the complexities of PQC migration, leveraging a comprehensive methodology to deliver a seamless, efficient, and tailored process aligned with your unique needs and timelines.

Our PQC Migration Advisory Methodology consists of three phases:

1. PQC MIGRATION PROJECT PLANNING:

PQC Roadmap: We develop a comprehensive migration plan outlining key milestones, timelines, and resource allocation to ensure a smooth transition.

PQC Governance: We establish clear policies and procedures to define roles, responsibilities, and decision-making frameworks for the migration process.

PQC Resource Allocation: We help you allocate the required resources, including budget, skilled personnel, and advanced technology, to support every stage of the migration.

PQC Stakeholder Engagement: We collaborate with stakeholders to define project objectives, scope, and deliverables, ensuring alignment and securing support from the outset.

2. PQC MIGRATION PROJECT MANAGEMENT:

Progress Tracking: We monitor the project's progress to ensure adherence to established timelines, milestones, and deliverables.

Risk Management: We identify, evaluate, and address risks and issues proactively throughout the migration lifecycle.

Quality Assurance: We perform extensive testing and validation of PQC implementations to meet industry standards and client-specific requirements.

Project Communication: We provide regular, detailed project updates, including status reports, key risks, and resolutions, to keep stakeholders informed and aligned.

3. PQC POST-MIGRATION ASSISTANCE:

Performance Monitoring: We continuously evaluate the performance and security of deployed PQC protocols to ensure they meet operational expectations.

Quantum Threat Monitoring: We track and provide updates about advancements in quantum computing to assess the ongoing resilience of PQC solutions.

Lifecycle Management: We monitor the lifecycle of PQC solutions to anticipate updates, maintenance needs, or potential replacements.

Post-Migration Support: We deliver ongoing support to address any operational issues, optimize solutions, and ensure long-term quantum resilience.



Be proactive

Don't let incidents dictate your Resilience Strategies

> Trusted by the Ecosystem



Funded by
the European Union

The PQ-REACT initiative is funded by the EU's "Horizon Europe" research and innovation programme. Its main objective is to validate a framework for EU transition to Post-Quantum Cryptography.

QuRISK was selected by the PQ-REACT initiative to participate in the evaluation of PQC vendors and solutions, competing within their programme.

Leveraging their expertise, QuRISK's experts successfully completed the evaluations and presented their findings to the PQ-REACT board.

These insights played a crucial role in identifying and selecting the most promising finalists for further development and testing within the framework.



The Forum des Compétences is a leading French community that brings together cybersecurity and resilience experts from the financial sector to share knowledge, and strengthen collective cyber resilience.

QuRISK was selected by the Forum des Compétences to lead the 2025 working group on Quantum & Cybersecurity, engaging with CISOs and resilience professionals in monthly sessions.

Leveraging its expertise, QuRISK is steering discussions on the quantum cyber threat, PQC migration, and the opportunities and risks of quantum computing.

This collaborative effort will culminate in the publication of a collective white paper* and a dedicated event, reinforcing the Forum's commitment to preparing the financial sector for the quantum era.

* <https://www.forum-des-competences.org/livre-blanc-quantique-cybersecurite/>

We wish you a pleasant
Quantum Resilience Journey.

Travel *safe* with QuRISK.

> They trust us



> Our Labels





Quantum Risk Advisory
25, quai du Président Paul Doumer
92400 Courbevoie
France

contact@qurisk.fr

www.qurisk.fr