



How can you prepare your organisation for post-quantum security? A practical roadmap

02 July 2026, 09:00

Farhad Aghili

Ludwig De Locht

From inventory to roadmap: 5 steps towards quantum-ready security

In a [previous article](#), we explained why you should already think about post-quantum security today. The arrival of cryptographically relevant quantum computers remains uncertain. Yet preparing for this transition can take years. A full migration is not needed today. But you can already take key steps to reduce future risks. By understanding where cryptography is used, and how systems can adapt, you make the move towards post-quantum security much more manageable.

Step 1: Map your cryptography

A successful migration starts with visibility. Many organisations do not know exactly where cryptography is used. They also lack insight into systems that depend on vulnerable algorithms.

Start by mapping where cryptography appears, for example in:

- Products
- Systems
- Communication protocols
- Software dependencies
- Certificates and PKI infrastructures
- Embedded components

This inventory forms the basis for every next step.



Step 2: Identify critical long-life systems

Not every system needs the same priority. Focus first on systems that will remain operational for many years. Also look at systems that are difficult to adapt. Think of systems that:

- Will remain in use for many years
- Are difficult to update remotely
- Have high replacement costs
- Are essential for business operations

The longer a system remains in use, the more important preparation becomes. Future cryptographic migrations need attention today.

Step 3: Assess the crypto-agility of your systems

Crypto-agility is a key feature of future-ready systems. It means you can replace cryptographic algorithms without redesigning the entire system. Check:

- Which cryptographic mechanisms can be replaced easily
- Which components depend strongly on specific algorithms
- How modular the current architecture is

The more flexible the architecture, the easier future migrations become.

Step 4: Map your dependencies

Cryptography is often not limited to your own software. It can also be hidden in external components and services. That is why you need a clear view of all dependencies. Look at:

- Suppliers
- Third-party software
- Cloud platforms
- Industrial ecosystems

These dependencies will help determine how complex a future migration becomes.

Step 5: Build a migration roadmap

The transition to the post-quantum era is not a one-off project. It is a long-term process that requires prioritisation, governance and phased decisions. A roadmap helps you set priorities, manage risks and spread investments. This allows you to prepare the migration step by step, without disrupting operations.



Build practical skills together

Post-quantum cryptography remains an active research field. At the same time, many organisations need practical guidance that fits real industrial environments. Their questions often focus on:

- Migration strategies
- Integration impact
- Crypto-agility
- Embedded system and OT constraints
- Lifecycle management
- Operational feasibility

Organisations also need practical ways to map cryptographic dependencies. They need to assess migration options and test their impact in real operational environments. To support this transition, Sirris explores how practical methodologies, validation activities and applied expertise can help Belgian companies prepare for post-quantum migration in realistic industrial contexts.

The goal is not to impose specific technologies or suppliers. It is to help you understand the impact, assess your readiness and identify practical next steps. As quantum-resistant systems become reality, collective learning and hands-on experimentation will play a key role. They will help industry move through this transition with more confidence.

Start preparing today

Do you want to understand what the post-quantum transition could mean for your products, systems or digital infrastructure? Sirris helps companies assess risks, explore migration paths and build practical expertise for long-term cyber resilience.

[Contact us](#)

This article is part of a two-part series on post-quantum security.

Part 1: [Post-quantum security starts with migration, not quantum computers](#)

Part 2: How can you prepare your organisation for post-quantum security? A practical

roadmap ?

Authors



Farhad Aghili



Ludwig De Locht