Young Talents Cybersecurity 2025

Survey Findings Report

How are organisations preparing for the **Post-Quantum Cryptography** era?

Robin THE
Tjitske KOSTER
Matteo GRELLA
Iman ABSHIR ALI
Teodora CURELARIU
Benjamin LEVERRIER

INSTITUT FRANÇAIS NL

December 2025

Executive Summary

Quantum computers are expected to become capable of breaking today's public-key cryptography around 2035, threatening the confidentiality and authenticity of digital systems. This risk already matters today due to **harvest-now, decrypt-later** attacks and the long timelines required to replace cryptographic infrastructure. Transitioning to post-quantum cryptography (PQC) is therefore a strategic necessity.

"How are organisations preparing for the PQC era?"

To answer the research question, we conducted a survey. We performed this study from July to December 2025, and cybersecurity professionals from 62 organisations participated. Most respondents represent government organisations and the IT sector, primarily based in the Netherlands, limiting generalisability.

What we assessed:

- Awareness of quantum and post-quantum risks
- Engagement with PQC developments and standards
- Cryptographic inventory and migration planning
- Expectations from the EU and national governments
- Coordination within multinational organisations

Key Findings:

This survey shows that PQC readiness is marked by strong awareness but limited follow-through. Respondents are familiar with quantum computing and well aware of the risk that a quantum computer might pose to classical cryptography. On the other hand, we find that respondents are not familiar with PQC solutions. Additionally, of the organisations:

- Only **36%** have conducted a cryptographic inventory
- Only **23%** have a PQC roadmap
- Only **20%** have started phasing out legacy algorithms (e.g., RSA, ECC)

Many organisations acknowledge long-term impact but prioritise short-term risks. Respondents repeatedly reported that top management is only marginally involved.

Expectations and takeaway

- Respondents expect the **EU** to provide frameworks and practical resources.
- They expect **national governments** to provide regulatory clarity and guidance.

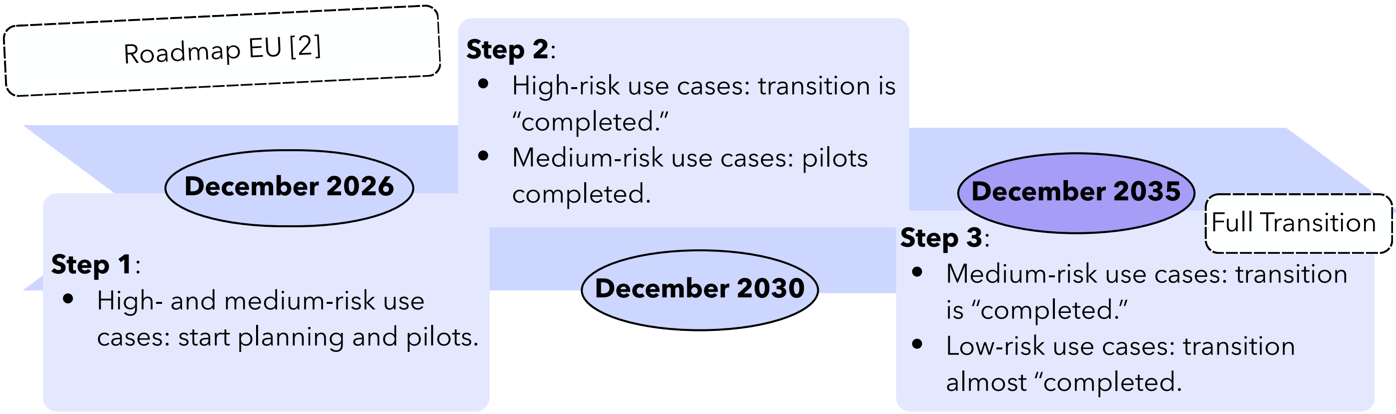
The practical takeaway from our work is simple:

Organisations do not need to "solve PQC" today, but they do need to start turning awareness into actions, beginning with visibility into cryptographic dependencies.

Introduction

Cyberattacks increasingly influence our everyday lives. Attacks target public institutions, private companies, and critical infrastructure, resulting in serious financial, economic, and safety consequences. We must thus prepare for the next cyber challenge: the quantum computer. It is expected that a quantum computer in 2035 will be sufficiently advanced to break current cryptography. To protect against this, cryptography needs to be replaced with post-quantum cryptography (PQC).

The first main risk is “harvest now, decrypt later”; attackers can store encrypted data now and decrypt it once they possess a powerful enough quantum computer. The second risk is that quantum computers could break digital signatures and certificates, allowing attackers to impersonate websites and organisations. Migration of these signatures will be time-consuming [1]. Thus, we need to act now.



Roadmap EU [2]

December 2026

Step 1:
- High- and medium-risk use cases: start planning and pilots.

Step 2:
- High-risk use cases: transition is “completed.”
- Medium-risk use cases: pilots completed.

December 2030

December 2035

Full Transition

Step 3:
- Medium-risk use cases: transition is “completed.”
- Low-risk use cases: transition almost “completed.

Understanding the risks, we see that migrating to PQC is no longer optional. We need to assess the scale of the migration and make timelines. To this end, the EU has published a roadmap (see above) [2]. This roadmap and the most important “No regret move” highlight its importance, but we wonder:

“How are organisations preparing for the PQC era?”

As a team of the Young Talents Cybersecurity (Institute Français-NL), we engaged with 62 organisations and conducted a survey. After 6 months of research, we we are pleased to share the findings and provide hands-on tips to get started with the PQC migration.

First, the current state of Quantum Computers

Most likely, a quantum computer will not be able to break our cryptography tomorrow. We cite Byrd and Ding [3]: “scaling to the thousands or millions of qubits needed for game-changing applications is still a work in progress”. However, recently, Google Quantum AI [4] achieved a 13,000× speedup over the world’s fastest supercomputer in a physics simulation.

Second, how do we enforce the use of PQC?

Several key institutions documented the PQC transition, e.g., ENISA [5], BSI [6], ANSSI [7], TNO [8], and the NIS Cooperation Group [2]. Additionally, the EU roadmap [2] provides guidance on when and how to start. However, if migration is not enforced by law, organisations may not be willing to take the necessary steps. In this section, we focus on how existing legal and regulatory frameworks, de facto, encourage the PQC transition.

Most existing legal texts establish a state-of-the-art obligation: a requirement to apply security measures that reflect current technological standards, as mandated by existing legal frameworks. We focus on four primary EU legal instruments even if this list is not exhaustive. Nevertheless, each contains provisions that could implicitly require organisations to anticipate future evolving cryptographic risks.

NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS 2)

By requiring "state-of-the-art encryption" (Recital 51) and periodic updates of cryptographic policies (§9.3; Articles 21–23), NIS2 establishes a moving security baseline. Once PQC becomes the recognised state of the art, NIS2 could implicitly require its adoption. The directive also promotes stronger cybersecurity through robust encryption and anticipates certification as a future compliance benchmark, even though PQC-certified products remain rare today.

CYBER RESILIENCE ACT (CRA)

The CRA introduces security-by-design and vulnerability-management duties for all connected products. Articles 10–15 and Annex VIII require products to remain "in conformity with the state of the art," which obliges manufacturers to anticipate future cryptographic risks even though PQC is not explicitly mentioned. Once PQC becomes the recognised state of the art, integrating PQC algorithms could become necessary to maintain CRA compliance.

GENERAL DATA PROTECTION REGULATION (GDPR)

Article 32 links encryption to "appropriate technical measures." If a cryptographic protocol is broken by a QC, their legal sufficiency is compromised, especially under harvest-now–decrypt-later attacks. Organisations may need to adopt PQC to maintain GDPR-compliant levels of confidentiality, integrity, and availability of data.

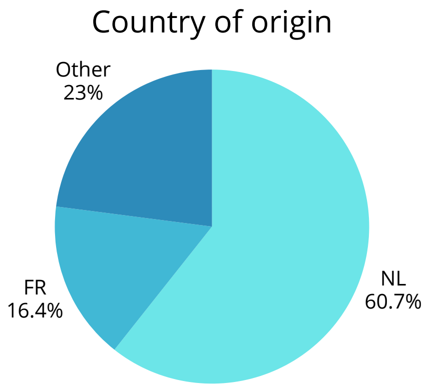
DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

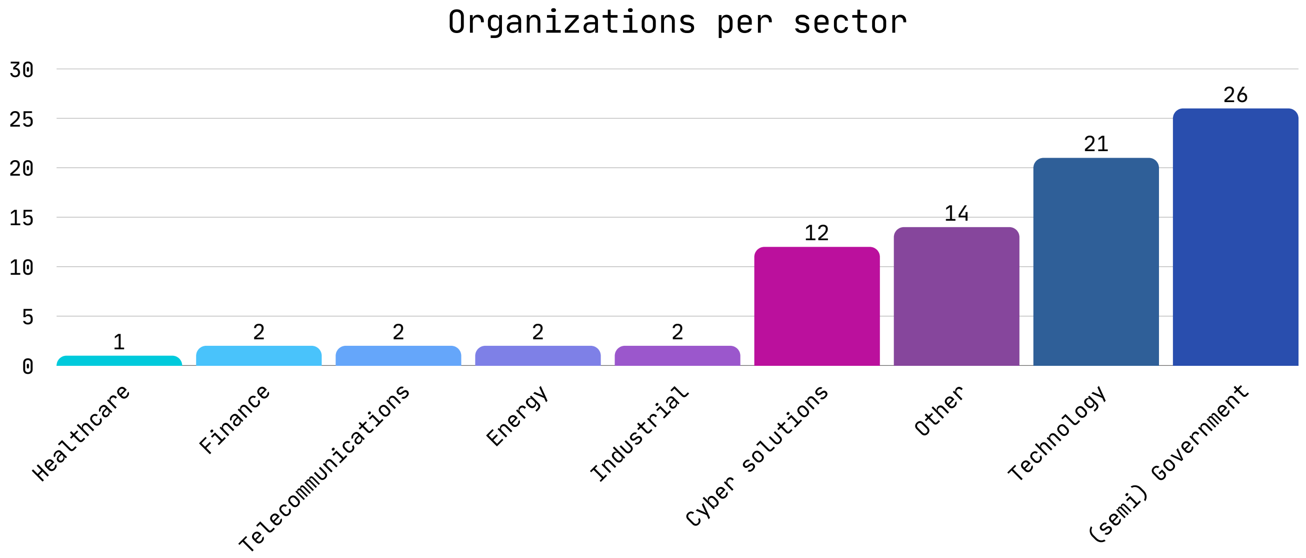
DORA imposes strict ICT risk management and supply chain oversight for the financial sector. Because it requires entities to stay aligned with evolving cryptographic risks, its governance and mandatory testing frameworks are likely to prompt the financial sector to adopt PQC earlier than other EU regimes.

Some organisations highlight that there is no explicit obligation to migrate yet. Nevertheless, we argue that compliance with the state of the art already requires addressing the emerging quantum risks.

The survey

To gain a deeper understanding of how organisations are preparing for the post-quantum era, we conducted a survey. For our study, we engaged with 62 cybersecurity professionals from various organisations. However, we stress that there is limited diversity. First, we note that most respondents are from government organisations, reflecting the authors' network. The second-largest group of respondents comes from the IT sector; they may have a deeper understanding of the issue and also provide cybersecurity services to other organisations. Additionally, most organisations are Dutch, and the response rates might have been affected by the study's timing (summer).





Key areas explored in this survey

AWARENESS AND UNDERSTANDING

To assess how familiar respondents and their organisations are with quantum computing.

INVENTORY AND ROADMAP

To identify which steps organisations have already taken toward post-quantum (PQ) readiness.

ROLE OF THE EU & NATIONAL GOVERNMENTS

To explore expectations from the European Union and national governments.

MULTINATIONAL ORGANISATIONS

To understand whether companies coordinate their PQ strategies with their subsidiaries.

ACTIVE PARTICIPATION

To determine whether organisations stay informed and engaged in the evolution of PQC standards.

Results of the survey

To start, we evaluated, on a scale from 0 to 10, the self-reported level of understanding and awareness of respondents and their organisations regarding quantum and post-quantum topics. The results show a solid familiarity with quantum computing and a strong awareness of the risks to classical cryptography. Meanwhile, knowledge of PQ solutions remains moderate.

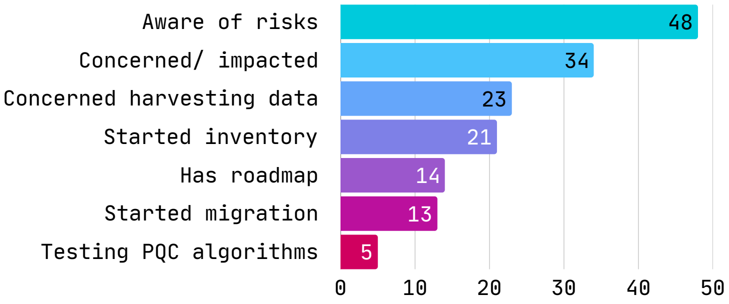
7.1/10
Familiar with quantum computing

8.0/10
Awareness of the risks to classical cryptography

5.8/10
Knowledge of post-quantum solutions

The histogram on the right shows that most respondents are well aware of the risks, but companies are less concerned about PQC and even less so about harvest now/decrypt later. Only about a third started doing the inventory, and as the migration steps proceed, we see fewer and fewer companies answering yes. Only 14 companies have a roadmap, and 20% started migrating.

Here, we follow the EU PQC migration model. Later, we return to this in more detail.



36% Of the organisations conducted an inventory

Of the organisations have a roadmap **23%**

These initial results suggest that most organisations can be described by a quote from one of the respondents: "concerned no, but impacted yes."

There is a clear tendency to prioritize short-term risks above the risk a quantum computer poses to the long term. This is despite the fact that many respondents acknowledged the potential long-term impact. Some respondents also mentioned a lack of involvement from top management, indicating that the topic has not yet become a strategic priority.

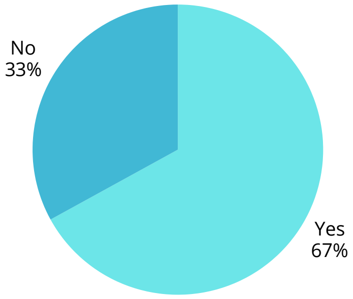
"Concerned, no, but impacted, yes."

Very few organisations have already phased out the use of legacy encryption algorithms such as RSA or ECC.

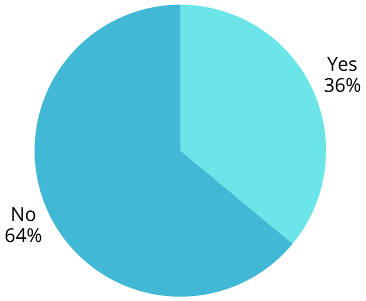
What are the main difficulties?

To understand the urgency of the PQ migration for organisations, we asked them if they think it is necessary to allocate a budget for the PQ migration. Two-thirds think it is, but only a third started with inventory. They provided several reasons not to start with this.

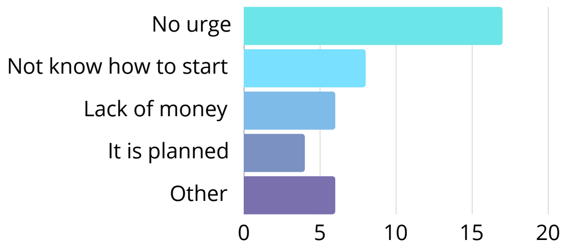
Necessary to invest in PQ migration?



Did you start the inventory?



Why did you not start with an inventory?

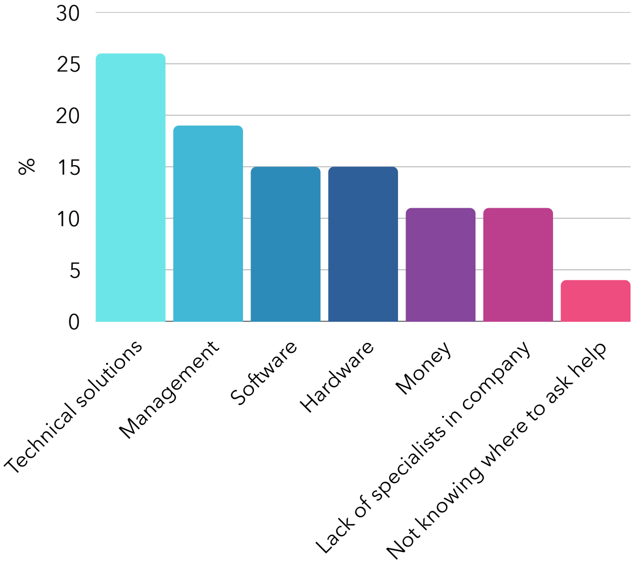


“Companies see that PQ will pose risks, but they don't know what to do about it, and are in a "freeze" state”

We can split the organisations into two groups: those that started the PQC migration (22%) and those that did not (78%). We asked the first group what the main difficulties were (left), and the second group what the main difficulties will be (right):

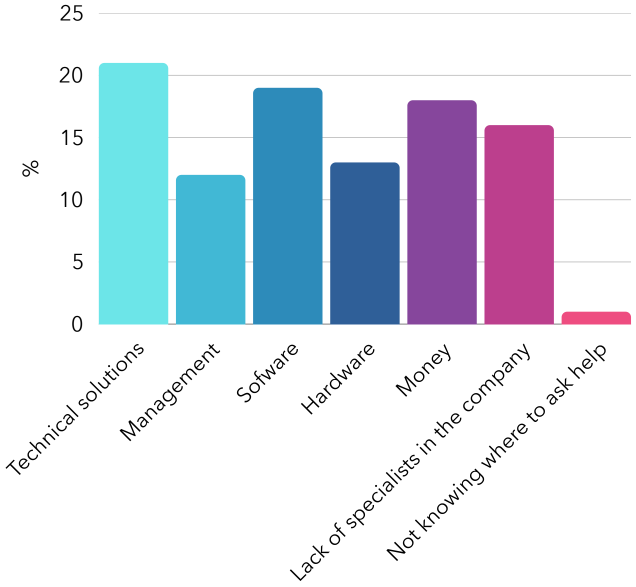
What were the main difficulties?

Asked to those who started the PQC migration



What will the main difficulties be?

Asked to those who did not start yet



Management teams often struggle to view PQC as a high-priority concern, despite its long-term strategic importance.

“organisations cannot migrate without PQC-ready tools from their vendors”

Main issues identified

Our survey shows that the four main issues that limit companies from migration are:

LACK OF PQC SOLUTIONS

- "Lack of standards for hybrid PQ encryption/signatures."
- “If Google/Microsoft will provide solutions, we will buy them.”
- “Software is incompatible.”

LACK OF LEGAL OBLIGATION

- “Management is only willing to migrate if this is enforced by NIST/ law, because this is a high-risk company.”
- “We have to follow the ISO standards and EU regulations” (ISO is mentioned 4 times)

MORE URGENT SECURITY ISSUES

- "We do not see an urge to start" (17 times).
- “PQ is not a threat for everyone, and even so, it's a future threat. I'd rather focus on current threats.”

MANAGEMENT

- "Main difficulty management" (11 times).
- "Management did not consider 'harvest now, decrypt later' as a current risk."
- "No hard constraints from management."

We observe that management does not want to invest in PQC because there are no explicit legal obligations to migrate. Instead, budgets and attention are primarily focused on short-term security issues.

What are respondents’ expectations towards the EU and their national governments?

When the organisations do have to migrate, they cannot do this alone. We wonder what they expect from the European Union and from their own government.
The results indicate that the European Union should play a crucial role in developing guidelines, frameworks, and toolkits/open-source libraries. From the national government, they also expect regulatory clarity, not as much the toolkits, but a lot of guidance is expected.

EUROPEAN UNION

- Regulatory clarity & updated guidelines (40x).
- Certification frameworks (36x).
- Practical toolkits & open-source libraries (22x).

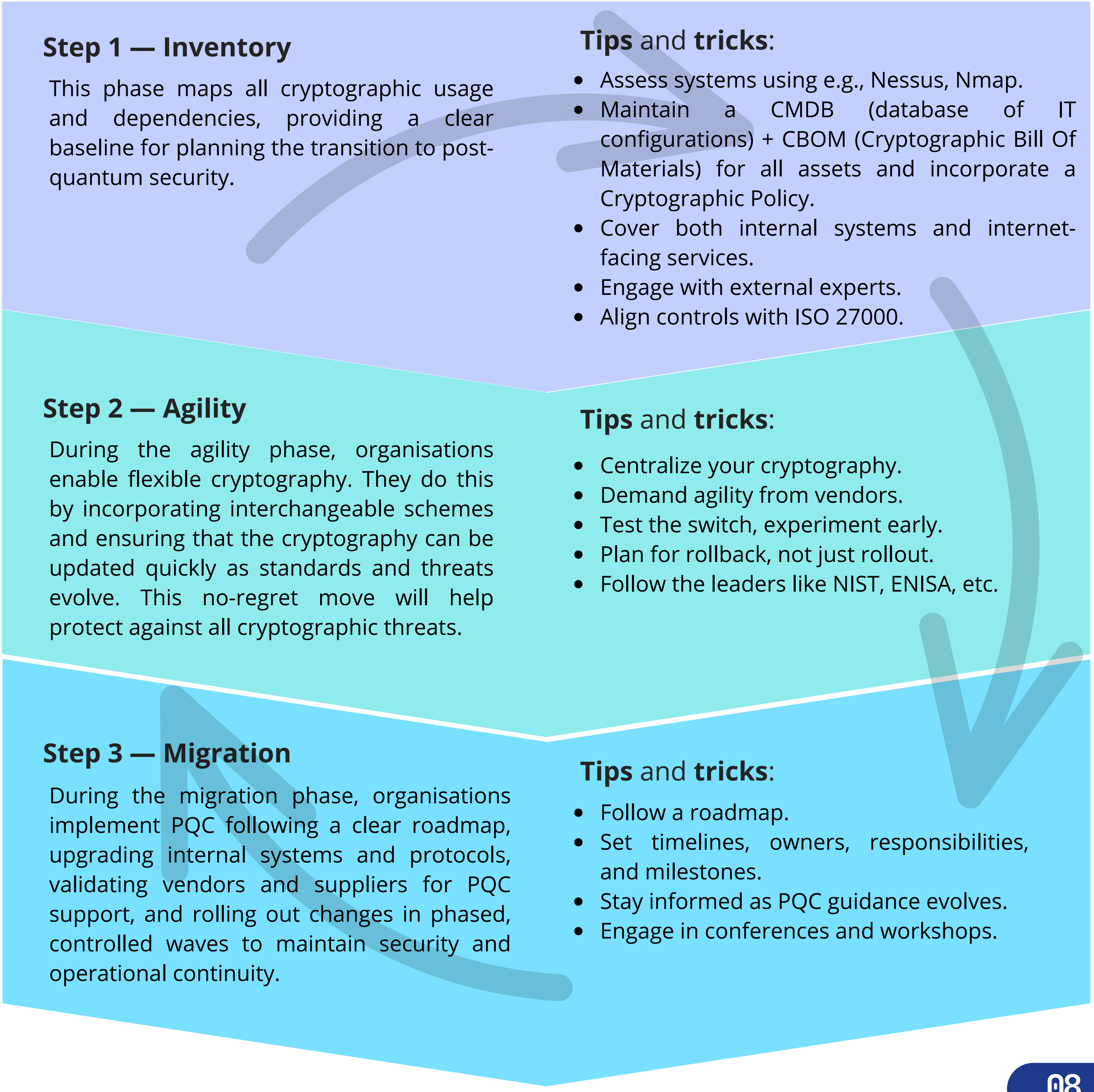
GOVERNMENTS

- Regulatory clarity & updated guidelines (35x).
- More guidance (25x).
- Certification frameworks (22x).

We asked the few organisations that started the PQC migration how they began. We combine their answers with information from the ANSSI, NCSC, the EU Roadmap, and our expertise to give some hands-on tips we present in the coming sections.

Inventory, Agility & Migration

To ensure the long-term protection of sensitive data, organisations should begin preparing now. The European PQC roadmap [9] encourages a structured transition built around understanding current cryptographic usage, ensuring systems can evolve, and then migrating to post-quantum secure solutions. This is not a sudden switch, but a phased, pragmatic journey. We provide our own practical interpretation of the three steps: **inventory**, **agility**, and **migration**, with tips and tricks we learned from the survey. We depict them below in 3 steps, but in practice, the migration will require continuous looping through them.



Step 1 — Inventory

This phase maps all cryptographic usage and dependencies, providing a clear baseline for planning the transition to post-quantum security.

Tips and **tricks**:

- Assess systems using e.g., Nessus, Nmap.
- Maintain a CMDB (database of IT configurations) + CBOM (Cryptographic Bill Of Materials) for all assets and incorporate a Cryptographic Policy.
- Cover both internal systems and internet-facing services.
- Engage with external experts.
- Align controls with ISO 27000.

Step 2 — Agility

During the agility phase, organisations enable flexible cryptography. They do this by incorporating interchangeable schemes and ensuring that the cryptography can be updated quickly as standards and threats evolve. This no-regret move will help protect against all cryptographic threats.

Tips and **tricks**:

- Centralize your cryptography.
- Demand agility from vendors.
- Test the switch, experiment early.
- Plan for rollback, not just rollout.
- Follow the leaders like NIST, ENISA, etc.

Step 3 — Migration

During the migration phase, organisations implement PQC following a clear roadmap, upgrading internal systems and protocols, validating vendors and suppliers for PQC support, and rolling out changes in phased, controlled waves to maintain security and operational continuity.

Tips and **tricks**:

- Follow a roadmap.
- Set timelines, owners, responsibilities, and milestones.
- Stay informed as PQC guidance evolves.
- Engage in conferences and workshops.

NCSC (National Cyber Security Centre - NL)

The NCSC (National Cyber Security Center) is the Dutch National CSIRT and the central expertise center for cybersecurity. We asked them to give some hands-on tips to start with the PQC migration, and they said the following:

The urgency and speed of migration depend on your organisation's risk profile. The NCSC recommends taking the first steps toward building a quantum-safe organisation as soon as possible by:

- Identifying the risks a quantum computer poses to the digital resilience of your organisation;
- Inventorying how and where your organisation uses cryptography;
- Assessing the risks for your organisation; and
- Developing a migration plan.

For detailed information on the PQC migration, consult the PQC migration handbook [8], written by the AIVD, CWI, and TNO.

You can learn more about how cryptography works, what the risks are of a powerful quantum computer, and how experts are preparing for this technological revolution in the ENTER podcast on quantum computers [9].

For practical guidance to get started with the first steps in your migration to quantum-safe cryptography, consult the publication “Make Your organisation Quantum-Safe” by the NCSC and AIVD [10].

ANSSI (French Cybersecurity Agency)

As ANSSI's Director General warned [11]:

> **“When it happens, there won't be a quick fix; everything will collapse.”**

As France's national cybersecurity and certification authority, ANSSI plays a central role in the PQC transition: conducting market studies and pilots with vendors and operators, helping organisations define their transition plans, and evaluating products that integrate PQC.

The three milestones for this transition from the ANSSI are [12]:

- In **2026**, ANSSI plans to update several reference frameworks, such as the IPsec-DR guide and the RGS (General Security Framework) [13].
- From **2027**, ANSSI will no longer certify security products that do not integrate quantum-resistant cryptography.
- By **2030**, it will become mandatory not to procure solutions that fail to offer long-term quantum resistance.

Hands-on tips to start

Keep yourself informed

Follow organisations (e.g., newsletters) such as NIST, AIVD, NCSC, ENISA, OBVIA Quantum cybersecurity watch.

Make a roadmap

A structured approach prevents inconsistency and downtime, ensuring crypto-agility against future quantum threats.

Active participation

Attending conferences (e.g., PKI conference), participating in Quantum working groups (ISO, finance-specific, PCSI, ANSSI), and convincing management to allocate funds for crypto agility.

Conclusion

The transition to post-quantum cryptography is not a single event, but a strategic journey. The previous migrations already showed how long, complex, and challenging such updates can be for organisations. By first understanding where cryptography is used (Inventory), then ensuring systems can adapt (Agility), and finally executing a guided transition (Migration), organisations can move confidently toward long-term security.

The most important message is clear: the no-regret move is to start preparing now. Building cryptographic agility today ensures that tomorrow’s migration will be manageable, cost-effective, and aligned with European PQC guidance.

Today, national agencies are still working on documents to help public and private organisations begin the transition. In 2026, many updates are expected, including new reference frameworks in France, such as ref IPsec DR or RGS. Documentation is one thing, but the market for PQC solutions also plays a key role in accelerating the transition. As always, the availability of PQC solutions can drive demand, and demand can, in turn, drive the availability of solutions.

Join our PQC Conversation

LET’S TAKE THE FIRST STEPS TOGETHER

Want to stay in the loop on PQC and potentially attend hands-on sessions? Leave your email via the contact form so we can gauge interest and share future updates:

Form: Join our PQC Conversation

Bibliography

[1] Bas Westerbaan, https://blog.cloudflare.com/pq-2025/, Second migration: signatures / certificates, 28 October 2025
[2] NIS Cooperation Group, Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography in the European Union, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography, 23 June 2025
[3] G. T. Byrd and Y. Ding, "Quantum Computing: Progress and Innovation," in Computer, vol. 56, no. 1, pp. 20-29, Jan. 2023, doi: 10.1109/MC.2022.3217021.
[4] Google Quantum AI and Collaborators. Observation of constructive interference at the edge of quantum ergodicity. Nature 646, 825–830 (2025). https://doi.org/10.1038/s41586-025-09526-6
[5] ENISA, Post-Quantum Cryptography: Current State and Quantum Mitigation, https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, 3 May 2021.
[6] BSI, Migration to Post-Quantum Cryptography, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2, 31 May 2021.
[7] ANSSI, Avis de l'ANSSI sur la migration vers la cryptographie post-quantique, https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique-0, 21 December 2023.
[8] AIVD, CWI, TNO, The PQC Migration Handbook, https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf, December, 2024.
[9] NCSC, Enter Podcast, https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/enter-de-podcast
[10] NCSC, make your organisation quantum secure, 18 September 2023, https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig
[11] Director General of ANSSI, L'Anssi lance le chantier de la sécurité post-quantique, 08 October 2025, https://www.lemondeinformatique.fr/actualites/lire-l-anssi-lance-le-chantier-de-la-securite-post-quantique-98115.html
[12] ANSSI, Cryptographie post-quantique (PQC), https://cyber.gouv.fr/cryptographie-post-quantique-pqc, 13 October 2025
[13] Talk ”Introduction and Guidelines from ANSSI for the Transition to Post-Quantum Cryptography (PQC)” by Samih Souissi (ANSSI) at the European Cyber Week 2025.