A PQC-Roadmap for the EU: acting upon the quantum threat now!

Presented by:

Dr. Stephan Ehlen, BSI
David Racapé, ANSSI
Anita Wehmann, QvC Rijk

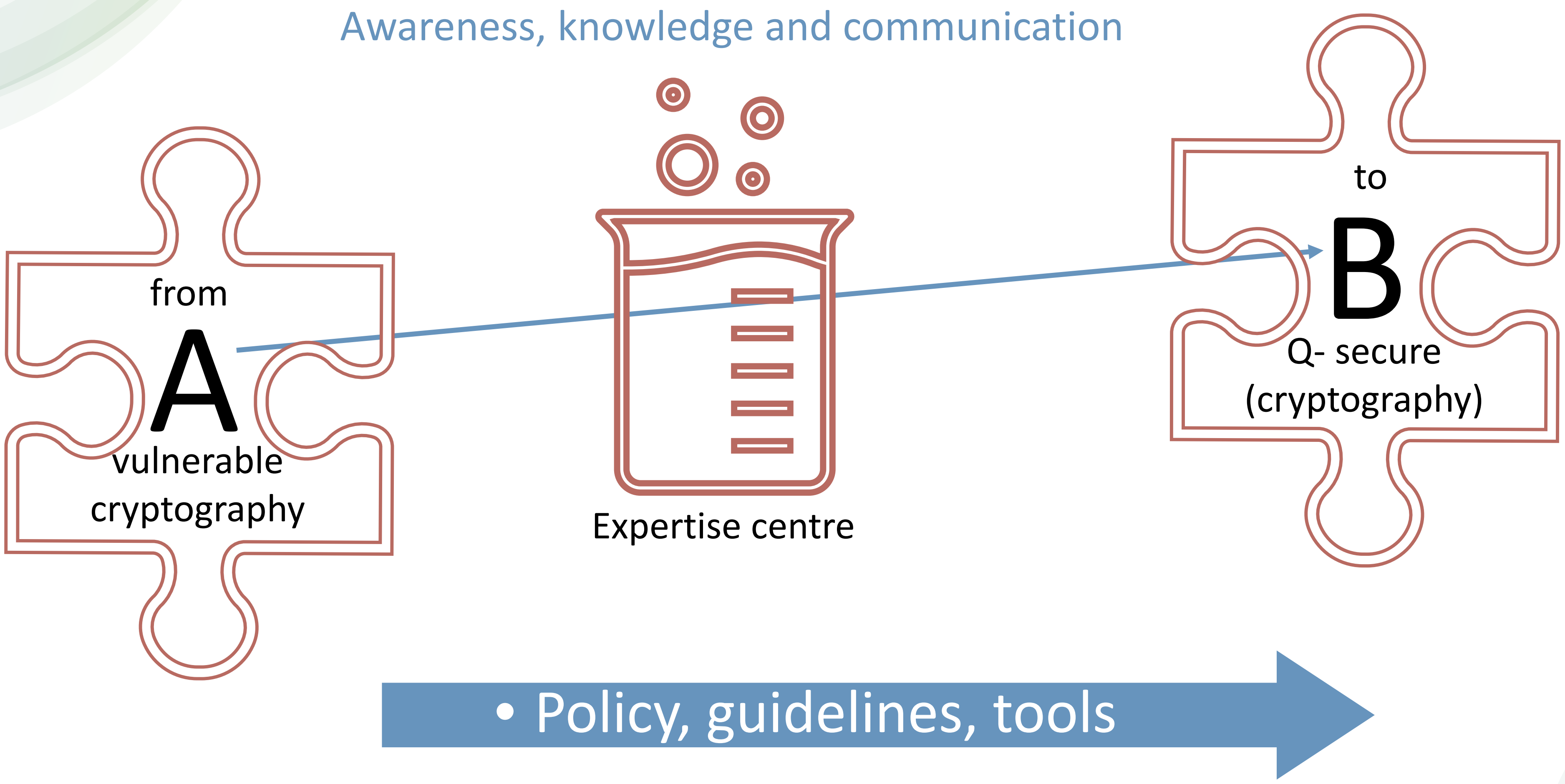
Bundesamt für Sicherheit in der Informationstechnik

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Transition to QSC – a simplified model



PQC Migration Strategy Components

Recommendation from the EU Commission

Published on April 11, 2024

Member States to develop within 2 years a comprehensive strategy for the adoption of PQC across the EU, which ensures a coordinated and synchronised transition among the different member states for the deployment of PQC in public administrations and critical infrastructures.

Objectives (excerpt)

1. Foster the transition to PQC
2. Define coordinated implementation roadmap for the EU
3. Enable Member States to define national PQC implementation roadmaps
4. Synchronise efforts of Member States
5. Implement measures to support the transition

Creation of the workstream

Kick-off in September 2024

25 EU member states

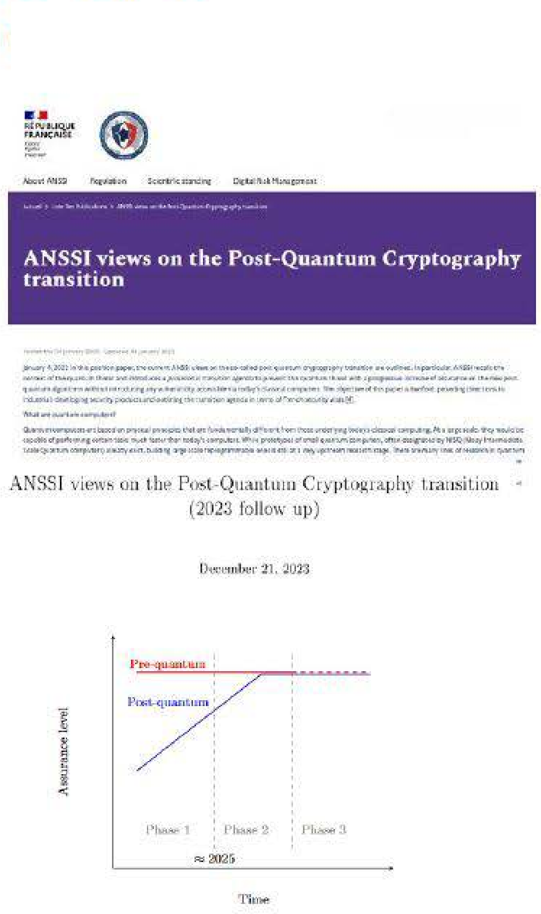
+ EU Commission and ENISA

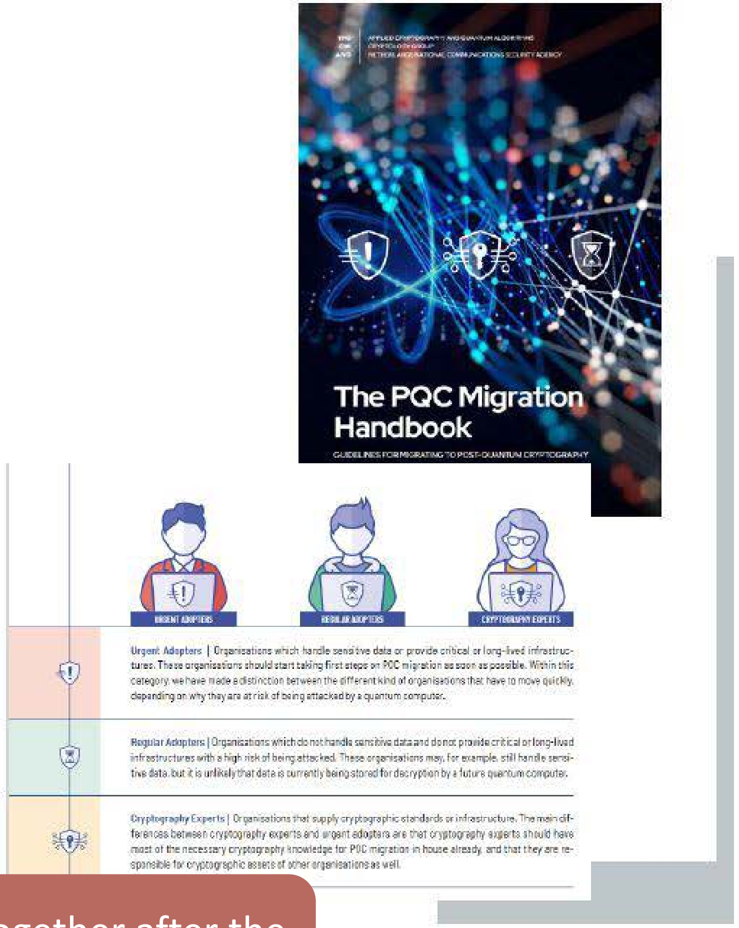
on this sailboat →

Plenary meetings of the whole workstream

Writing team DE – DK – FR – NL – SE to prepare a concept note providing a detailed outlined on the proposed approach to the elaboration of the roadmap

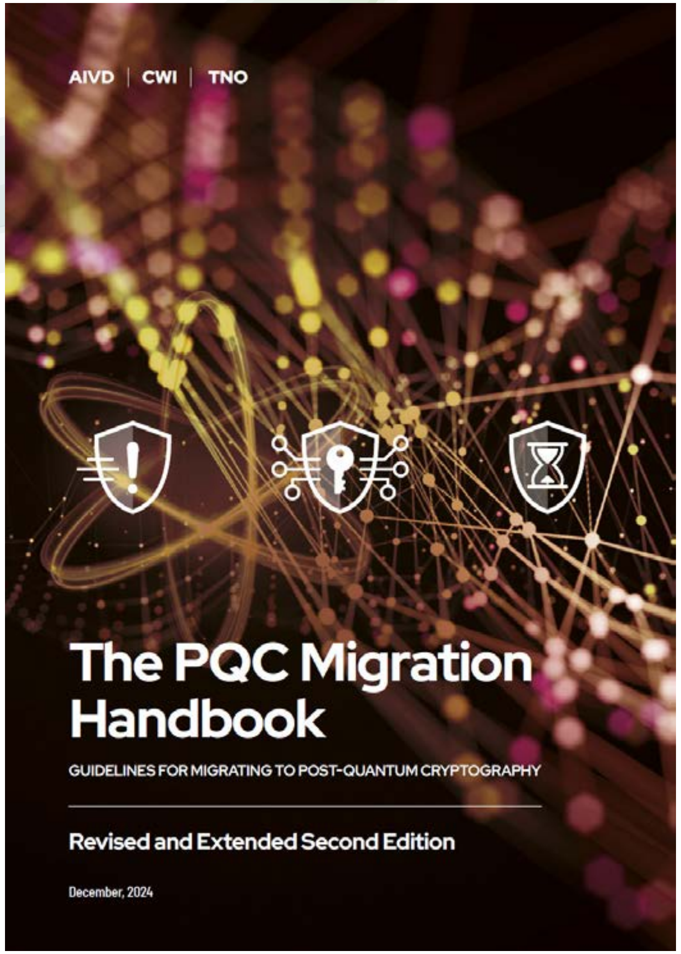
Existing publications from FR/DE/NL





DE, FR and NL started working together after the PQC Conference in Amsterdam in Nov. 2023

Update of NL PQC Migration Handbook



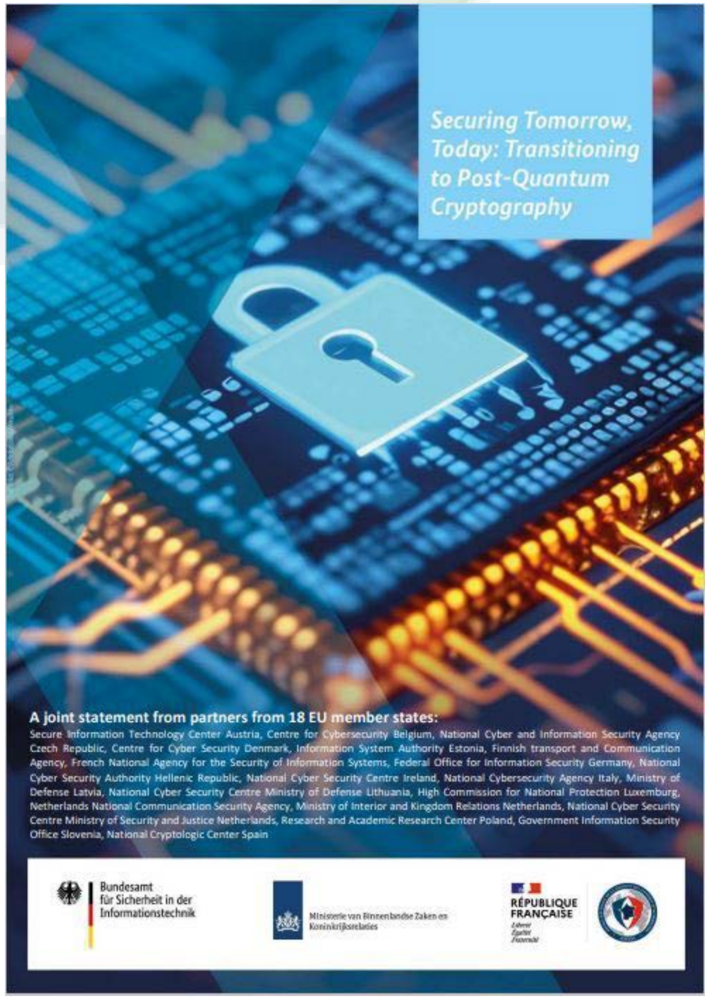
(collaboration between TNO, CWI and AIVD)

Urgent adopters should start now

→ EU member state governments are urgent adopters

- Sensitive information with a long confidentiality span (“store now, decrypt later”)
- Personal Data with a long confidentiality span: e.g. health records
- Provide systems of critical infrastructure: payment transactions, energy, transportation
- Provide systems which are built to have a long life-span: water management, chemical industry, drinking water, railroads

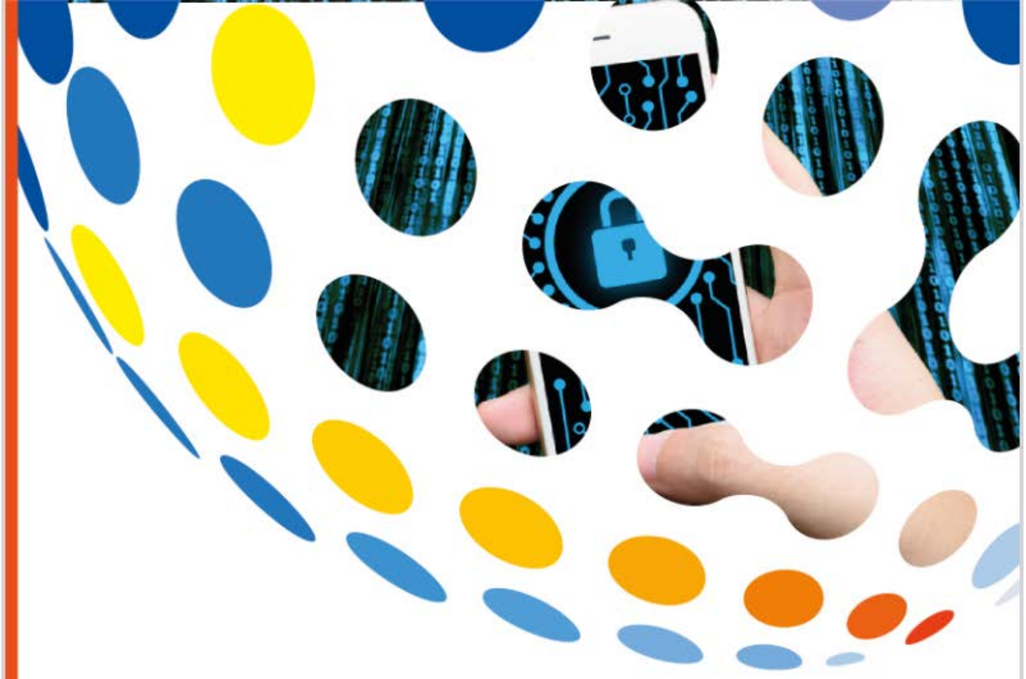
Joint EU statement – 18 member states, Nov 2024



BSI and partners from 17 other EU member states demand transition to Post-Quantum Cryptography

city Bonn
date 27.11.2024

[Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography]



A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025

NIS COOPERATION GROUP

Contents

1 Executive Summary 2

2 Introduction and motivation 3

3 Scope and definitions 4
- 3.1 Scope 5
- 3.2 Definitions of frequently used technical terms 5

4 Timeline 6
- 4.1 Overview 6
- 4.2 The timeline in detail: Milestones, first and next steps 7

5 Estimating the quantum risk 9

6 Steps towards the PQC migration 11
- 6.1 Introduction 11
- 6.2 First Steps 11
- 6.3 Next Steps 13

7 What the EU can do 15

References 15

1 Executive Summary

Digital infrastructures require robust cybersecurity. Cryptographic systems are vital to protect the confidentiality and authenticity of data. Quantum computing will be a threat to many of the cryptographic algorithms used to achieve these protection goals. Data that is currently not quantum-safe, whether it is stored or transmitted, and that must remain confidential for a long time, may be compromised in the future by quantum computers ("store now, decrypt later" attacks). In addition, authenticity will also be jeopardised by quantum computers. The threat that quantum computing poses to cybersecurity can be countered by a timely, comprehensive and coordinated transition to post-quantum cryptography (PQC).

Consequently, on 11.04.2024, the European Commission published a "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography" [1]. For the development of this "Implementation Roadmap" the Commission recommended to establish a work stream on PQC within the NIS Cooperation Group (NIS CG).

This document is the first deliverable of the NIS CG work stream on PQC and is meant to be a first high-level paper aimed at the Member States. The set of recommendations that Member States need to implement for a synchronised transition to PQC are divided into *First Steps* that are required to initiate the transition, and *Next Steps* that should follow. The recommendations in this document include measures to ensure that all stakeholders are well informed of the quantum threat to cryptography and can exchange their knowledge and experience, at national, European and international level. It is recommended to

EU PQC Roadmap

- Targeted audience: Mainly EU Member states; also applicable to critical infrastructures & other organisations.
- Proposes a comprehensive approach for Member States' authorities to start the process

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high and medium risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high risk use cases has been completed.
   - PQC transition planning and pilots for medium risk uses cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium risk use cases has been completed.
   - The PQC transition for low risk use cases has been completed as much as feasible.

Risk-based approach

- Based on the Quantum Risk Score developed in the „PQC Migration Handbook".
- Three factors influence the risk score:
  - Quantum weakness of the algorithms,
  - Impact of a successful attack,
  - Time and effort required for the migration.
- This yields an overall quantum risk score.

0: **Risk score 0 (No risk)** | All quantum threats are adequately mitigated.

1: **Risk score 1 (Low risk)** | There is a risk on the long term, but no priority is needed at the moment.

2: **Risk score 2 (Medium risk)** | Action is needed but the current cryptography is still secure on the short term or the migration is expected to be straightforward.

3: **Risk score 3 (High risk)** | Priority is needed on the short term because the expected impact is large and/or the migration to PQC is expected to take a long time.

4: **Risk score 4 (Acute risk)** | The system is already at risk, for example because because the expected migration effort in combination with how long the data should stay secure is longer than the expected time before a quantum computer will be able to break cryptography. In this case, there is a realistic threat that needs attention immediately, possibly from management in case of high business impact.

Quantum risk score following [17]	Quantum Risk Level in this document
1	low
2	medium
3 – 4	high

EU PQC Roadmap

Recommended “First steps” towards the PQC migration

- Identify and involve stakeholders
- Create dependency maps
- Perform quantum risk analysis
- Share knowledge and get involved in the EU work stream on PQC
- Support mature cryptographic asset management
- Include the supply chain
- Create a national awareness program
- Develop a timeline and an implementation plan

EU PQC Roadmap

Recommended “Next steps” towards the PQC migration

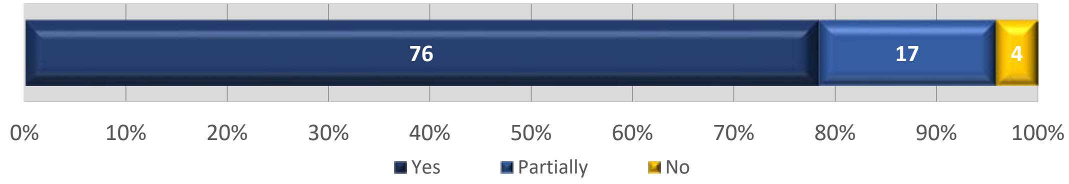
- Develop crypto-agility and quantum-safe upgrades
- Allocate resources
- Evolve the rules
- Transversal activities
- Involve the ecosystem
- Adapt certification schemes
- Establish testing centres and pilots

Public Consultation

Overview of 97 responses received

Reviewed Document

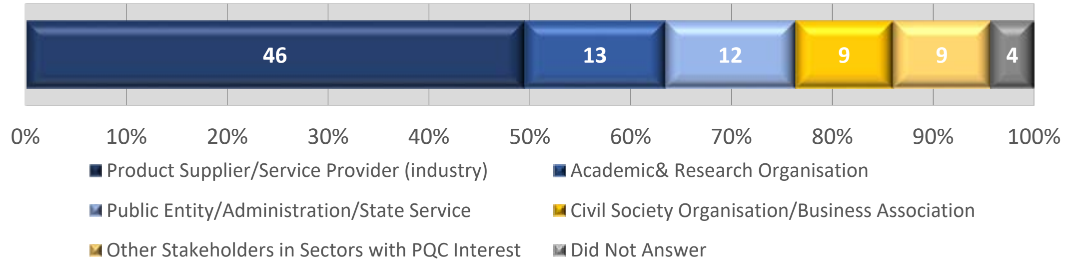
- **96%** of respondents **(n=93)** had reviewed the document; **17** of those had partially reviewed the document.



- **4** respondents had not reviewed the document and were excluded from further analysis.

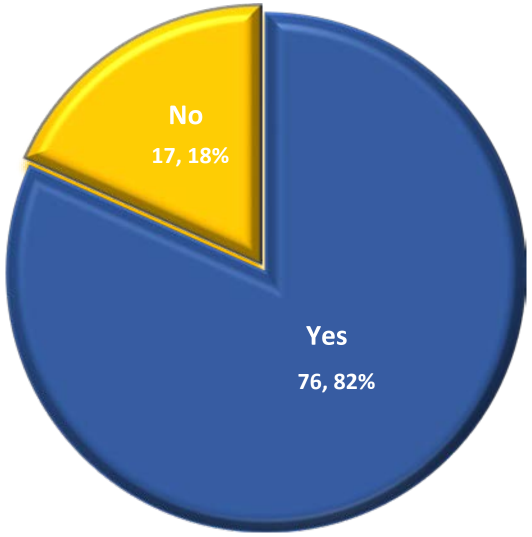
Respondents Organisation/Entity

- Almost **half** of respondents **(n=46)** were Product Suppliers or Service Providers in industry.



Wanted to Provide Feedback

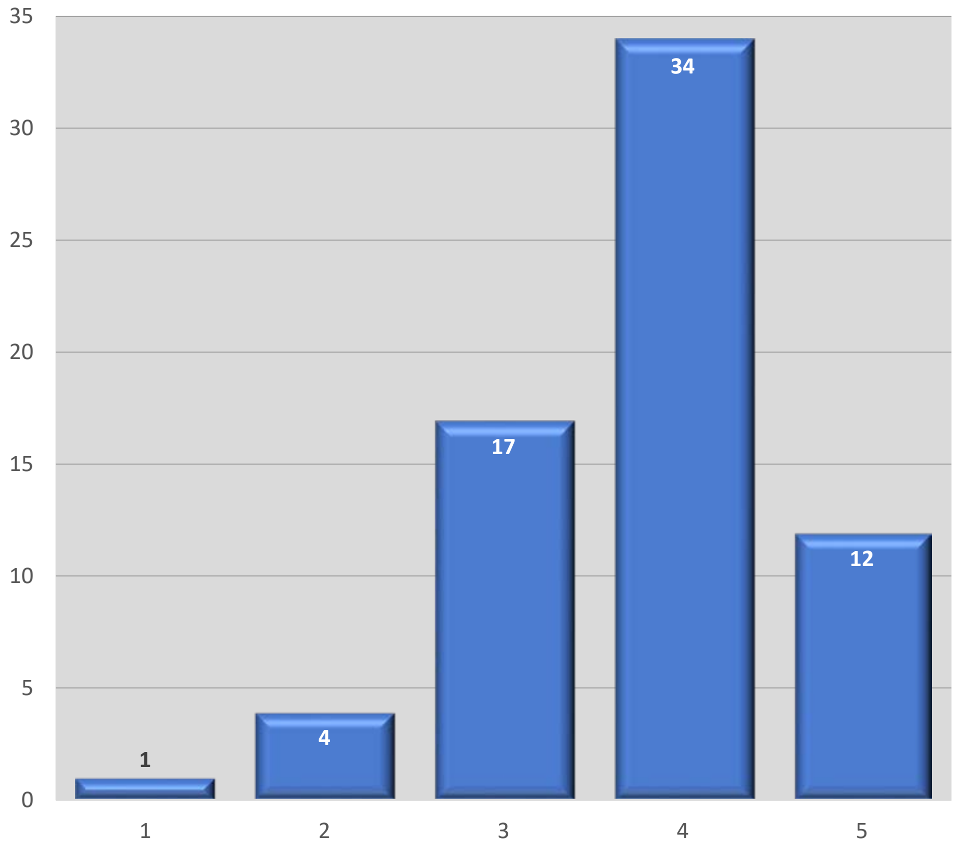
- **82%** of respondents **(n=76)** indicated they would like to provide feedback.



- Of those **73** provided an overall rating of the document and/or feedback.
- **3** provided no further feedback.

Survey Results

Overall rating of the document



- **68** respondents provided an overall rating of the document.
- **Rating scale 0 to 5, where:**
  0 is not at all clear; and
  5 is very clear and actionable
- **50%** of respondents **(n=34)** provided an overall rating of 4 suggesting the document is clear and actionable
- **12** respondents provided an overall rating of 5 indicating the document was very clear and actionable.

Consultation Feedback

64 respondents provided feedback on the most useful parts of the roadmap

Overall respondents indicate the following are most useful:

- ✓ Clear timelines and milestones
- ✓ Actionable first and next steps
- ✓ Risk-based approach
- ✓ Alignment with global best practice and consistency of timelines
- ✓ Hybrid approaches
- ✓ Crypto agility

Consultation Feedback

What areas of the roadmap required improvement or clarification?

Risk Categorisation and Threat Model

Alignment with Regulations and Policy Coherence:
CRA, CSA, NIS2, DORA, RED

Hybrids and Algorithm Guidance

Governance, Accountability, and Coordination

Sector-Specific Guidance and Use Cases

Interoperability, Dependency Chains, and Supply Chain Readiness

Testing, Pilots, and Practical Implementation Guidance

Resourcing, Awareness, and Workforce Development

Next steps

Publish FAQs on the Roadmap based on feedback

National PQC transition plans and updates in 2026

Develop with contributors: Case studies, success stories, sector-specific guidance, …

Thank you!

For stakeholders who have questions:
You can find us on LinkedIn:
@Stephan Ehlen
@David Racapé
@Anita Wehmann

For member state representatives who want to join the workstream:
Contact email address: CNECT-NIS-DIRECTIVE@ec.europa.eu