

Post-quantum cryptography (PQC) migration workshop report

No organisation can navigate the migration alone; key takeaways from our first PQC migration workshop.

In December 2025, the NCSC and Vodafone, with the [National Cyber Advisory Board](#), hosted the first UK government and industry workshop focused on post-quantum cryptography (PQC) migration. The event brought together security leaders and those responsible for PQC in their organisations from across industry, academia and government. This energising and inspiring day reinforced a simple but critical point; **no organisation can navigate the shift to PQC alone**.

However, you can only fit so many people in a room. So this blog aims to bring insights from the day to a wider audience.

Why PQC migration matters

[As the NCSC has explained](#), in the future, a sufficiently powerful quantum computer will be able to break the public key cryptography that protects our networks and systems today. The mitigation to this threat is to migrate these systems to use PQC algorithms, which are based on mathematical problems that are not vulnerable to attack by quantum or classical computers.

The NCSC has set out [key milestones for migration to PQC](#), which are intended to drive immediate action. While future targets appear distant, 2028 and 2031 will come round quickly, and organisations need to act now to stay ahead. This is because migration to PQC is **not** just a technical challenge; it's a global strategic resilience imperative across industries and governments.

Why bring organisations together?

There is no shortage of guidance on migration to PQC. But guidance alone is not enough. Making the PQC transition efficiently and securely requires close collaboration between experts in cryptography, cyber security and network operations, as well as those who understand the technical and business realities of the organisation undergoing change.

For this reason, the workshop was designed to **connect** experts across disciplines, **share** real-world approaches and challenges, and **build momentum** for action through collaboration. In doing so, the following key themes emerged from the workshop.

1

Engaging the board and building the business case

One of the strongest themes was the importance of executive sponsorship. PQC needs to be framed as a business risk and resilience priority, with a clear articulation of *'why now?'* and *'what is at stake if action is delayed?'*

The workshop identified the following approaches that can help engage the board:

- **Emphasise the cost of delay:** A strong message was that starting sooner will likely reduce future costs and complexity. Initiating planning and following recommended timelines can help to spread effort over time and reduce the risk of a costly, compressed transition later.
- **Connect to broader benefits:** Link PQC effort to other organisational goals. For instance, a PQC migration programme can help address existing issues like legacy systems and overall cyber resilience.
- **Make it organisation-specific:** Consider what your organisation's priorities are, and how PQC migration may fit into them. This could include availability of systems, legal compliance, or simply the bottom line.
- **Identify a senior sponsor:** This could be a CTO, CIO, CISO or another individual who understands the requirement and can represent it to their peers at board level.
- **Use peer and industry benchmarks:** Board members often respond to what peers are doing.
- **Do the pre-work:** Consider what activities can be undertaken in advance of (or alongside) engaging the board, to strengthen the business case. This could include engaging with the supply chain, doing initial discovery

exercises or identifying critical assets. Understanding this background will help to make both the risk and the ask more concrete.

- **Prioritise:** Prioritise migration of systems where a breach would have the greatest impact (such as those processing the most valuable data) as well as systems that take the longest time to migrate (such as when there's a dependency on long-lived hardware).
- **Lay out a phased roadmap:** Break the migration plan into clear phases with timelines, targets, required investments and skills/capabilities required for each phase. A step-by-step roadmap gives a structured view of how PQC migration will unfold, setting expectations on budget and resources whilst building confidence that there is an actionable plan. The NCSC's guidance on [PQC migration timelines](#) includes suggestions on how to go about PQC migration planning.

2

Supply-chain readiness is critical

An organisation's quantum readiness is dependent on its supply chain and the readiness of suppliers. A key theme from the workshop was the importance of building PQC into supplier security assessments and sourcing. Participants emphasised the need to:

- **Engage suppliers early:** Discussing PQC migration with suppliers should happen as soon as possible. Understanding (and influencing) your suppliers' PQC roadmaps, as well as making your requirements known, is key to developing a realistic migration plan. Without supplier alignment, even well-planned migration strategies risk falling behind.
- **Make your requirements clear:** An efficient and economical PQC migration will often take advantage of natural technology refresh cycles. This relies on products with PQC functionality (or the ability to be upgraded to PQC) being available when technical updates are planned.

3

Transparency and collaboration

Migration to PQC is a complex process that requires expertise and experience across a wide range of topics. Ultimately, collective progress will determine national resilience. No single individual will have all the answers, so we need to work together. Participants highlighted the value of:

- **Industry transparency:** Organisations undertaking PQC migration could publish blogs and reports on plans, approaches, progress and challenges. This would be valuable for organisations who are further behind in the process, particularly those with smaller security teams. Suppliers publishing their plans and progress would allow their customers to manage their own planning. Understanding challenges and lessons learned would help the NCSC to understand key technical issues that would benefit from further government guidance and support.
- **Cross-sector collaboration:** Much of the approach to (and lessons learned from) PQC migration can be applied across sectors. Opportunities for cross-sector collaboration would enable sharing of best practice and re-use of proven approaches.
- **A united voice from industry and government:** Organisations are more likely to invest in (and commit to) PQC migration if their competitors and partners are doing the same. Additionally, the UK will only be resilient to the threat from a quantum computer if all our key services, organisations and suppliers migrate. A united and consistent message from industry and government will support this.
- **Workshops, events and conferences:** Events like this one are valuable for bringing together those who are involved in PQC migration, sharing expertise and learning from the experience of others.

What's next?

The NCSC are keen to maintain the momentum of the workshop, and ensure that the conversation – and the action – continues. We are working with National Cyber Advisory Board to shape continued conversations on PQC across industry and government. If you are responsible for PQC migration in your organisation, and you would like to express interest in contributing to future discussions to share expertise and experiences, please get in touch using the [PQC workshop feedback form](#)

A final thought

We strongly encourage those of you with responsibility for cryptography and security to continue to progress your planning on PQC migration in your own organisations and sectors. The first steps (**discovery, prioritisation and roadmap development**) should be happening **now**, and will define success later.

Meeting the threat from quantum computing may sound like a far-off challenge, but preparing for it is a priority **today**. By planning your migration now, and working together, we can help build a quantum-safe future for the UK that protects our critical systems, services and data.

Flo D, NCSC Deputy CTO for Cyber Policy and Assessments

Lizzie Moseley, Vodafone Cyber Strategy & Content Manager

WRITTEN BY



Flo D
NCSC Deputy CTO for Cyber Policy and Assessments



Lizzie Moseley
Vodafone Cyber Strategy & Content Manager

PUBLISHED

22 July 2026

WRITTEN FOR

Cyber security professionals

PART OF BLOG

NCSC publications