QUANTUM
THINK TANK

Insight that protects. Foresight that leads

Global PQC Policy and Regulatory Landscape

By Tooba Qasim

January 2026

www.cyberlondon.com | info@cyberlondon.com

Post-quantum cryptography (PQC) has moved from research papers into the world of policy, regulation and compliance. Governments and standards bodies are no longer asking ***if*** organisations should prepare for quantum risk, but ***how fast*** they can do it. For many organisations across the UK and internationally, PQC is no longer just a technical upgrade; it is becoming a regulatory and strategic obligation.

This article gives an overview of how global policy is evolving around PQC, what major players are doing, and why UK organisations in particular need to pay attention.

PQC as a Regulatory Priority

Around the world, policymakers have accepted a core reality: once large-scale quantum computers exist, they will be able to break widely used public-key cryptography such as RSA and elliptic curve cryptography (ECC). That has direct implications for national security, critical infrastructure, financial stability, and data protection.

As a result:

- Governments are issuing directives, memoranda, and roadmaps that push organisations to **inventory cryptography**, **plan migrations**, and **adopt quantum-safe standards**.
- Standards bodies are publishing **formal specifications** for quantum-safe algorithms and deployment patterns.
- Supervisors and regulators are embedding quantum risk into broader cyber and operational resilience frameworks.

In other words, PQC is shifting from "interesting future topic" to **compliance requirement in the making**.

United States: NIST Standards and White House NSM-10

The United States is currently the most visible driver of formal PQC standards.

In August 2024, NIST released the first three fully standardised post-quantum algorithms as Federal Information Processing Standards (FIPS):

- **FIPS 203 – ML-KEM** (formerly CRYSTALS-Kyber) for key establishment
- **FIPS 204 – ML-DSA** (formerly CRYSTALS-Dilithium) for digital signatures
- **FIPS 205 – SLH-DSA** (based on SPHINCS+) as a hash-based backup signature scheme (NIST)

These standards formally define how federal agencies (and, in practice, a large part of the global ecosystem) should implement quantum-safe algorithms. They set the technical foundation that vendors, cloud providers, and enterprises are now beginning to build on.

Policy direction for the United States was clearly set by the **White House National Security Memorandum 10 (NSM-10)** in May 2022. NSM-10 instructs US agencies to prioritise the transition to quantum-resistant cryptography and calls for an organised, timely migration of vulnerable systems. (The White House)

NSM-10 is backed up by additional guidance from the Office of Management and Budget (OMB), such as Memorandum M-23-02. That memo requires federal agencies to conduct a **prioritised inventory of cryptographic systems**, identify where quantum-vulnerable algorithms are in use, and prepare for NIST PQC standards. (The White House)

From a regulatory perspective, this combination means:

- The US federal government is committed to a **structured PQC transition**, not an ad-hoc response.
- Vendors that serve the US public sector are being pushed to support PQC and hybrid schemes.
- Private sector organisations worldwide are aligning with NIST standards, because they will become the de facto global baseline.

For any organisation looking at long-term cryptographic strategy, NIST's FIPS 203/204/205 and NSM-10 together form a clear signal: **quantum-safe migration is now a matter of policy and compliance, not only of good practice**.

European Union: NIS2 and a Coordinated PQC Roadmap

In Europe, quantum risk is being woven into broader cyber resilience frameworks rather than treated as a standalone issue.

The NIS2 Directive aims to raise cybersecurity standards across critical and important entities in sectors such as energy, transport, health, digital infrastructure, banking, and public administration. It does not spell out PQC algorithms by name, but it expects organisations to implement "state-of-the-art" security, manage cryptographic risks, and ensure the resilience of essential services.

As the understanding of quantum risk matures, "state-of-the-art" is increasingly interpreted to include planning for, and eventually adopting, post-quantum cryptography.

The European Commission has also gone a step further by publishing a **Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography** in 2025. The roadmap emphasises that quantum computing threatens many existing cryptographic algorithms and calls for a timely, comprehensive transition to PQC, particularly for critical infrastructure and cross-border services. (Digital Strategy EU)

For EU-based organisations, this means:

- PQC will increasingly be part of **regulatory expectations under NIS2**, DORA (for financial services), and related frameworks.
- There is growing political pressure to move **critical infrastructure to quantum-resistant encryption by around 2030**, especially in high-impact sectors.
- National regulators are likely to issue country-specific guidance that references the EU roadmap.

Even if an organisation is not directly supervised under NIS2, its suppliers, cloud providers, or infrastructure partners might be, which in turn will push PQC requirements down the supply chain.

United Kingdom: NCSC Guidance and the UK Context

For CyberLondon and UK-based organisations, the domestic policy environment is especially important.

The UK's **National Cyber Security Centre (NCSC)** has been one of the early European voices on quantum-safe cryptography. In its 2020 whitepaper "Preparing for Quantum-Safe Cryptography," NCSC explained the quantum threat and positioned quantum-safe cryptography as the most effective mitigation (NCSC).

More recently, NCSC has updated its guidance in light of NIST's new standards. In its "Next steps in preparing for post-quantum cryptography" paper and subsequent communications,

NCSC acknowledges the publication of ML-KEM, ML-DSA, and SLH-DSA, and encourages organisations to start planning migrations rather than waiting for "Q-day." (NCSC)

In March 2025, NCSC issued new guidance and public messaging that explicitly calls on large organisations and operators of critical national infrastructure to transition to post-quantum cryptography by around **2035**, following a phased roadmap (identify by 2028, prioritise by 2031, complete by 2035). Media coverage in outlets like *The Guardian* and the *Financial Times* reinforced that the UK government views quantum risk as a serious, time-bound challenge.

For UK organisations, particularly those in critical sectors or with bespoke IT systems, this has several implications:

- PQC is no longer only a **technical curiosity**; it sits firmly within the UK's national cyber strategy.
- Regulators and sectoral bodies (for example in finance, energy, and telecoms) are increasingly likely to ask for evidence of **PQC planning, cryptographic inventories, and migration strategies**.
- Organisations that operate across both the UK and EU will need to align **NCSC guidance with NIS2 obligations** and the EU's PQC roadmap.

For organisations operating in the United Kingdom, NCSC guidance is a natural reference point. It also represents an important opportunity: UK-based organisations that move early can position themselves as leaders, shaping best practice and influencing how regulators and industry bodies interpret "quantum-safe" within their respective sectors.

ETSI and the Standards Ecosystem

Beyond governments, standards bodies play a central role in turning PQC concepts into practical, interoperable technology.

In Europe, the **European Telecommunications Standards Institute (ETSI)** has been working on quantum-safe cryptography for more than a decade. Its Quantum-Safe Cryptography (QSC) work, now part of ETSI TC CYBER, produces technical specifications, reports, and frameworks that guide industry adoption. (ETSI)

Recent ETSI work includes:

- Updates to **TS 103 744** on hybrid quantum-safe key establishment, describing how to combine classical and PQC algorithms within real-world protocols.

- Technical reports such as TR 103 965, TR 103 966, and TR 104 016, which cover the impact of quantum computing on security proofs, deployment considerations for hybrid schemes, and frameworks for quantum-safe migration. (NIST Computer Security Resource Center)

These documents are important because they move the discussion from "which algorithm" to "how do we actually deploy this in complex, existing systems?" They provide guidance on hybrid modes, protocol integration, performance considerations, and repeatable migration patterns.

For organisations building large-scale infrastructures, ETSI specifications often sit alongside IETF, ISO, and national guidance. Together, they form a **technical backbone** for policy objectives such as those in NSM-10, NIS2, and NCSC roadmaps.

More Regulation Is Coming

The current regulatory and policy signals are only the beginning. Several trends are emerging:

- **Deadlines and milestones:** The US, EU, and UK are starting to talk about dates like 2030 and 2035 as informal or formal targets for completing migration in critical sectors. (Digital Strategy EU)
- **Integration into broader frameworks:** PQC will likely be embedded in cyber regulations such as DORA, sector-specific supervisory expectations, and future updates to data protection guidance.
- **Supply-chain pressure:** Even where there is no explicit PQC regulation yet, large regulated entities will drive requirements down to their vendors, cloud providers, and technology partners.
- **Audit and assurance:** In time, "Are you quantum-safe?" may become a standard audit question, much like "Do you patch regularly?" or "Do you encrypt data at rest and in transit?"

For forward-looking organisations, the safest assumption is that **quantum-safe migration will become an explicit compliance topic**, not just a recommendation, especially for critical infrastructure, finance, healthcare, and government.

The Road Ahead

From a policy and regulatory standpoint, the message is increasingly consistent across the US, EU, UK, and international standards bodies: **do not wait for quantum computers to arrive before acting**. The combination of NIST standards, NSM-10, NIS2, NCSC guidance, and ETSI technical work is building a global expectation that serious organisations will plan and execute a quantum-safe transition over the next decade.

PQC is no longer just about algorithms. It is about governance, compliance, resilience, and long-term trust in digital systems. The organisations that recognise this today will be the ones that navigate tomorrow's quantum era with confidence.

For the wider UK cyber ecosystem, the transition to post-quantum cryptography presents both a challenge and an opportunity. The challenge lies in translating high-level national and international policy into practical steps: developing cryptographic inventories, planning migration programmes, and aligning with evolving standards. The opportunity, however, is significant. Organisations that act early can help shape what "good" looks like in practice and influence how sector regulators, policymakers, and technical communities interpret quantum-safe expectations in the years ahead.

Quantum Think Tank aims to support this shift by helping to raise awareness, convene experts, and strengthen the national conversation around quantum-safe transformation. Its mission is to contribute to a stronger, more connected UK cyber ecosystem, one that is prepared to adopt PQC responsibly, collaboratively and at scale. By bringing together practitioners, researchers, policymakers, and innovators, **Quantum Think Tank** seeks to play a constructive role in guiding the UK toward a secure and future-ready digital environment.

About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring