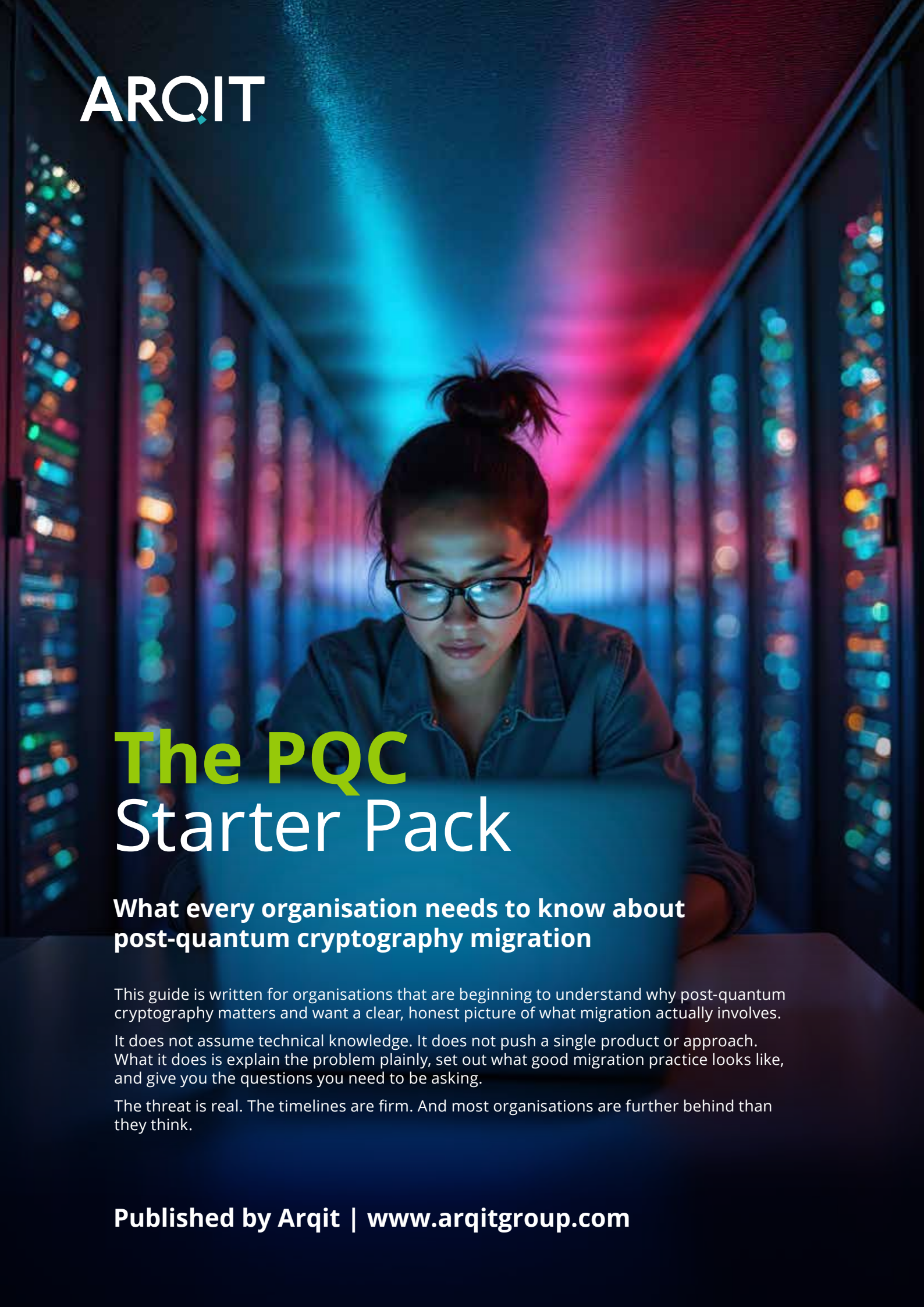

ARQIT

The PQC Starter Pack

What every organisation needs to know about post-quantum cryptography migration

This guide is written for organisations that are beginning to understand why post-quantum cryptography matters and want a clear, honest picture of what migration actually involves.

It does not assume technical knowledge. It does not push a single product or approach. What it does is explain the problem plainly, set out what good migration practice looks like, and give you the questions you need to be asking.

The threat is real. The timelines are firm. And most organisations are further behind than they think.

Published by Arqit | www.arqitgroup.com

1. The threat is already active

What quantum computing does to encryption.

Almost everything we trust online is secured by public key cryptography. When you send an email, complete a financial transaction, connect to a VPN, or authenticate a user, public key cryptography is doing the work. It generates the keys that lock and unlock data, and it relies on mathematical problems that are effectively impossible for today's computers to solve.

Quantum computers work differently. Rather than testing one answer at a time, they process multiple possibilities simultaneously. For certain mathematical problems, including the ones that underpin RSA, elliptic curve cryptography, and Diffie-Hellman key exchange, a sufficiently powerful quantum computer could find the answer in hours or minutes rather than millions of years.

When that happens, the encryption protecting your network, your data, and your customers' information stops working. Not gradually. All at once.

Cryptographically relevant quantum computers are expected within this decade. The US, UK, and EU have all set mandatory migration deadlines in response.

The more urgent problem: data is being stolen now.

The risk is not limited to what happens when quantum computers arrive. It starts today.

State-sponsored actors and sophisticated criminal groups are harvesting encrypted data now, storing it with the intention of decrypting it once quantum capability becomes available. This is known as Harvest Now, Decrypt Later, or Store Now, Decrypt Later. It does not require a quantum computer to execute. It only requires the ability to intercept and store data, which is well within the capability of multiple nation-states right now.

Data Is Being Collected: The Evidence.

Confirmed

National security agencies in the US, UK, and Europe have publicly confirmed bulk interception and retention of encrypted communications for future analysis.

FBI

FBI Director Christopher Wray has stated that China has stolen more US data than every other nation combined.

65%

of European telecoms operators surveyed by GSMA Intelligence reported a security breach in the past three years. 53% cited data loss and theft as the primary impact.

The data most at risk is data that retains value over time. That includes pharmaceutical and medical research, genomic and health records, financial transaction histories, legal and diplomatic communications, and intellectual property. If any of this data has been in transit over a public network in the past decade, it should be treated as potentially harvested.

There is no reliable way to know whether data has been intercepted passively. Standard security monitoring identifies known intrusions and observable exfiltration. It does not detect passive collection of encrypted traffic. The absence of a breach alert is not evidence of safety.

The question is not whether your data has been harvested. The question is what happens to your organisation when it becomes readable.

2. Why migration is harder than most organisations expect

Cryptography is embedded, not bolted on.

The most common mistake organisations make when they first engage with this problem is treating it as a cryptography upgrade, something that can be handled by swapping one algorithm for another and moving on.

That framing is wrong, and acting on it will create serious problems.

Cryptography is not a discrete component. It is embedded throughout modern infrastructure. It lives in network protocols, application code, firmware, certificates, key management systems, hardware security modules, cloud platforms, and third-party integrations. Many of these dependencies are undocumented. Some are invisible to the teams responsible for security.

You cannot replace what you cannot see. Most organisations cannot currently answer three basic questions: where is cryptography used, which algorithms are deployed, and what systems depend on them.

Four reasons migration consistently takes longer than planned.

1 Lack of visibility

Cryptographic usage is rarely fully documented. Legacy systems, inherited infrastructure, and third-party services all introduce dependencies that are not tracked in a central inventory.

2 Fragmented ownership

No single team owns all cryptographic decisions. Security, IT, networking, application development, and procurement all make choices that affect the cryptographic estate. Coordinating a migration across all of them is a programme management challenge as much as a technical one.

3 Hidden dependencies

Changing a cryptographic algorithm or protocol can break systems in ways that are not immediately obvious. Applications that rely on specific certificate formats, key lengths, or protocol handshakes may fail silently or stop functioning entirely.

4 Operational risk

Migration cannot simply be switched on. It requires staged deployment, testing, fallback planning, and coordination with vendors and partners. Poorly planned migrations have caused outages in critical systems.

History shows how long this takes.

Algorithm transitions have a long and instructive history. MD5 was shown to be cryptographically weak in 2005. It was still present in production systems more than fifteen years later. SHA-1 was deprecated by NIST in 2011 and remained in Microsoft solutions until 2020. NIST has set 2030 as the deadline for phasing out legacy algorithms, and has acknowledged that complex systems will need more time.

The organisations now completing SHA-1 migration started years ago. The organisations that leave PQC migration until the threat becomes visible will find they do not have the time.

6.5 yrs The average gap between where organisations currently are and where they need to be for PQC migration, according to a BSI (German Federal Office for Information Security) survey.

3. What the regulators are requiring

Government mandates are already in force.

This is not a voluntary exercise. Governments across the US, UK, and EU have set legally binding timelines for migration to post-quantum cryptography. For organisations in regulated sectors, or those supplying government contracts, compliance is not optional.

Jurisdiction	Near-term requirement	Final deadline
United States	Annual cryptographic inventories required from 2023. TLS 1.3 mandated by January 2030. RFC 8784 mandatory for classified VPN vendors.	Mitigate as much quantum risk as feasible by 2035 (NSM-10 / OMB M-23-02).
United Kingdom	NCSC advises starting high-priority upgrades by 2028.	Full PQC migration completed by 2035.
European Union	Transition begins under coordinated EU roadmap from end-2026. High-risk systems migrated by end-2030.	Full migration completed by end-2035.
Australia	ASD committed to dropping SHA-256, RSA, ECDSA and ECDH by 2030.	Full transition aligned to global PQC standards.

Beyond these mandates, the NIS2 Directive and DORA in the EU both have direct implications for cryptographic resilience. Organisations in financial services, healthcare, energy, and critical infrastructure should treat quantum-safe migration as part of their existing compliance obligations, not as a separate workstream.

4. Understanding your options

There is no single answer.

A common misconception is that post-quantum migration means choosing one new algorithm to replace the ones in use today. The reality is more nuanced. Three main approaches exist, each with different strengths, limitations, and appropriate use cases. Most organisations will need to use a combination.

Post-Quantum Algorithms (PQAs).

In August 2024, NIST standardised its first post-quantum algorithms, including ML-KEM (also known as CRYSTALS-Kyber) for key encapsulation and ML-DSA (CRYSTALS-Dilithium) for digital signatures. These are designed to resist attacks from quantum computers and will form the backbone of most long-term migration efforts.

What to know: PQAs are an important and necessary part of the solution. However, they come with caveats that any organisation should understand before treating them as the complete answer.

Security analysis is still maturing. Three algorithms were broken or compromised during the NIST standardisation process itself, including SIDH, which was broken by a classical computer in 2022. The algorithms now standardised are considered strong, but independent academic scrutiny is still ongoing.

Key sizes are significantly larger than RSA or ECC, which increases bandwidth and compute requirements. This matters for high-throughput network environments and resource-constrained devices.

Migration complexity is high. PQAs are not drop-in replacements. Protocols and services need to be re-engineered, because PQA typically places greater demands on devices and networks than traditional public key cryptography.

Deployment takes time. History shows that even after standardisation, algorithm transitions take years or decades to complete across complex infrastructure.

Most authoritative guidance, including from NIST, NSA, NCSC, and the joint paper from France, Germany, Sweden, and the Netherlands, recommends a hybrid approach: combining symmetric key methods with PQAs to provide defence in depth and reduce reliance on any single approach.

Symmetric Key Agreement (SKA).

Symmetric encryption, the kind used in AES-256, is already quantum-resistant. Unlike public key cryptography, it does not rely on mathematical problems that quantum computers can efficiently solve.

The challenge with symmetric encryption has always been key distribution: how do two parties securely agree a shared key without meeting in person or using public key methods? Historically, this required manual key couriering, which is secure but completely impractical at scale. Symmetric Key Agreement platforms solve this problem by enabling endpoints to dynamically agree symmetric encryption keys on demand, without public key cryptography and without manual distribution. The NSA has stated that pre-shared symmetric keys in a standardscompliant implementation represent a better near-term post-quantum solution than experimental post-quantum asymmetric algorithms.

Quantum Key Distribution (QKD).

QKD uses quantum physics to distribute encryption keys in a way that makes eavesdropping theoretically detectable. It is theoretically very strong.

In practice, QKD has significant limitations for most organisations. It requires dedicated, expensive hardware and specialist infrastructure. It cannot be deployed at scale across large distributed networks. Both the NSA and Germany's BSI have expressed reservations about QKD as a primary solution for most organisations, noting that its practical limitations outweigh its theoretical advantages in most deployment scenarios.

5. How to approach migration

The five stages of a structured PQC migration.

Every major guidance body, including CISA, NIST, NCCoE, the NCSC, and ENISA, converges on the same basic migration structure. The details vary, but the sequence does not. You cannot skip stages.

The five stages of a structured PQC migration

Discover

Identify every place cryptography is used across your systems and infrastructure. This includes applications, network devices, cloud platforms, certificates, firmware, key management systems, and third-party services. Use automated tooling where possible. Manual discovery is incomplete by definition. This stage is not optional: every other stage depends on it.

Assess

For each system and dataset identified, assess the risk. Prioritise by the sensitivity and longevity of the data protected, the exposure of the system to external networks, and the blast radius if the system is compromised. Data that needs to remain confidential for years or decades requires earlier action than data with a short sensitivity lifetime.

Plan

Build a migration programme with clear ownership, timelines, and governance. Identify which systems can be migrated with vendor updates, which require re-engineering, and which represent hard cases with long lead times. Engage vendors early and get explicit commitments on PQC roadmaps and certification plans. Plan for crypto-agility from the start: the goal is not just to migrate once, but to build the capability to adapt as standards evolve.

Transition

Execute in controlled stages. Pilot new approaches before broad rollout. Test performance, handshake behaviour, certificate impacts, and operational tooling. Use hybrid approaches during transition, running classical and post-quantum methods in parallel, to maintain security continuity. Define clear exit criteria for retiring legacy algorithms. Do not declare success at the pilot stage.

Operate

Treat PQC migration as an ongoing programme, not a one-time project. Keep the cryptographic inventory live. Monitor for new vulnerabilities, standards updates, and implementation weaknesses. Be prepared to rotate algorithms when needed. The organisations that build this capability now will be significantly better placed than those that treat migration as a box to be ticked.

Crypto-agility: the capability that makes migration manageable

Crypto-agility is the ability to change cryptographic algorithms and key management approaches without disrupting the systems that depend on them. It is not a product. It is a design principle that needs to be built into infrastructure decisions from now on.

Without crypto-agility, every algorithm change becomes a major programme. With it, updates can be made at policy level, without hardware replacement or system re-engineering. Given that PQC standards will continue to evolve and that some algorithms standardised today may need replacing in the future, crypto-agility is not optional. It is the foundation of a sustainable long-term approach.

Four questions every organisation should answer now

1. Do we have a current inventory of where cryptography is used across our systems, networks, and third-party services?
2. Have we assessed which of our data assets are most exposed to Harvest Now, Decrypt Later risk, and how long that data needs to remain confidential?
3. Do we have a migration plan with clear ownership, timelines, and vendor commitments, and is it aligned to the regulatory deadlines that apply to our organisation?
4. Are we building crypto-agility into new systems and procurements now, so that future algorithm changes do not require another major migration programme?

If the answer to any of these is no, or not yet, that is the starting point.

6. What good looks like

Principles for a credible migration approach

Regardless of the specific tools and vendors you choose, a credible approach to PQC migration should demonstrate the following:

- **It starts with discovery.** Any approach that begins with deploying new encryption before completing an inventory of existing cryptographic usage is building on an incomplete foundation.
- **It uses hybrid methods.** Running classical and post-quantum approaches in parallel during transition maintains security continuity and reduces the risk of a single-point failure in new, less mature algorithms.
- **It is standards-based.** Solutions should conform to published standards from NIST, NSA, and relevant national agencies. Standards-based cryptography has been subject to independent scrutiny that proprietary approaches have not.
- **It is independently verified.** For any critical component of your cryptographic infrastructure, look for independent security evaluation. Vendor claims are not sufficient.
- **It integrates with existing infrastructure.** Approaches that require wholesale replacement of current network equipment and security tools are expensive, disruptive, and slow. Overlay approaches that work alongside existing infrastructure are more practical for most organisations.
- **It builds in crypto-agility.** Solutions that allow cryptographic primitives to be updated at policy level, without endpoint changes or hardware replacement, are significantly more sustainable than those that require re-engineering for every update.
- **It has no performance trade-off.** Quantum-safe encryption that significantly degrades network performance creates pressure to turn it off under load. Solutions should be validated to demonstrate negligible throughput impact.

Where to go from here

PQC migration is complex, but it is not unmanageable. The organisations that fare best are those that start early, build on accurate visibility of their current cryptographic estate, and treat migration as a programme rather than a project.

The starting point for most organisations is discovery: understanding what cryptography you have, where it is, and what it protects. Without that foundation, migration plans are guesswork.

The best time to start was two years ago. The second best time is now.

Arqit helps organisations find out where they stand

Arqit provides quantum-safe encryption software and cryptographic risk advisory services for governments, enterprises, and critical infrastructure operators. Our products integrate with existing infrastructure. No rip and replace. No performance trade-off.

Sources and further reading

US National Security Memorandum NSM-10 (2022) | OMB M-23-02 | NIST PQC Standards (2024) | NIST NCCoE PQC Migration Framework | CISA Post-Quantum Cryptography Guidance | NSA Post-Quantum Cybersecurity Resources | NCSC: Preparing for Quantum-Safe Cryptography | BSI Market Survey on Cryptography and Quantum Computing (2023) | ANSSI Post-Quantum Position Paper (2023) | Joint Paper: France, Germany, Sweden, Netherlands (2024) | GSMA Intelligence Security Survey (2024) | TNO PQC Migration Handbook | Nature: Post-Quantum Cryptography Transition (2026) | IDC: Securing Valuable and Durable Data in a Post-Quantum World (2024)