PHYSIVITIS

POST-QUANTUM READINESS GUIDE

Preparing for the Post-Quantum Era

A practical migration guide for business leaders, CISOs and security teams, with focused guidance for the **healthcare** and **financial services** sectors.

Physivitis Ltd • Free resource • Edition 2026

Foreword

For most of the digital age we have been able to take encryption for granted. It quietly protects our payments, our medical records, our communications and the integrity of the software we depend on, and it does so well enough that few people outside security teams ever think about it. That comfortable assumption is now coming to an end.

The public-key cryptography that underpins this trust, principally RSA and elliptic curve cryptography, rests on mathematical problems that ordinary computers cannot solve in any useful time. A sufficiently capable quantum computer changes that, and the change does not wait politely for the machine to arrive. Adversaries are already capturing encrypted data today in order to decrypt it later, which means that any information with a long secrecy lifetime is, in effect, already exposed. For sectors such as healthcare and financial services, where data must stay confidential for decades and systems stay in service for years, the implications are immediate.

At Physivitis we work at the point where deep physics becomes practical technology. We produced this guide because the transition to post-quantum cryptography is too important to be left as a specialist concern, and because the genuinely difficult part is not the mathematics but the sequencing: knowing what to do, in what order, and by when. The pages that follow translate a daunting, multi-year migration into clear and prioritised steps, grounded in the finalised NIST standards and the timelines now set by the UK NCSC, the United States and the European Union.

We have also built tools to make this work measurable rather than aspirational. USMC expresses your cryptographic posture as a single, auditable security margin, and TCBA audits a surface that conventional tooling ignores entirely: the cryptography hidden inside the parameters of the AI models organisations increasingly rely on. Both are described later in this guide. Whether or not you use them, the message is the same, and it is a hopeful one: this is a solvable problem for those who start in good time.

The organisations that begin now, methodically and without panic, will preserve the trust they have spent years earning. I hope this guide helps you be one of them.

Rene C Mugenzi - CEO

Contents

How to use this guide

This guide is written for any organisation that relies on encryption to protect data, communications, payments, identities or connected products; in practice, that is almost every organisation. It explains why the move to post-quantum cryptography matters, what the standards and regulatory deadlines require, how the challenge lands in specific sectors such as healthcare and financial services, and how to plan and execute a migration that is orderly rather than rushed. It then goes deeper, into algorithm selection, cryptographic inventory, the technical and operational impacts, governance and budget, testing, and the tools that make posture measurable.

You do not need to be a cryptographer to use it. Business leaders can read the foreword and the first four sections to understand the risk, the timeline and what it means for their sector. Security and technology teams will find algorithm guidance, an inventory framework, a phased roadmap, deep technical considerations and a quick-start checklist in the sections that follow. Where a topic is unavoidably technical, the surrounding text explains why it matters in plain terms.

> **At a glance**
>
> The threat is not only in the future; sensitive data captured today can be stored and decrypted later, once a capable quantum computer exists.
>
> International standards are finalised and regulators have set firm deadlines, with full migration expected by 2035.
>
> Exposure is highest where data must stay secret for years and systems stay in service for years; healthcare and financial services are leading examples.
>
> Migration is a multi-year programme; the most valuable steps this year are to build a cryptographic inventory, prioritise by risk, and start planning.

1. Why this matters now

For three decades the security of digital systems has rested on a small number of public-key algorithms, principally RSA and elliptic curve cryptography (ECC), supported by key-exchange methods such as Diffie-Hellman. These protect web traffic, software updates, payment systems, virtual private networks, digital signatures and much of the machinery of modern commerce. Their strength depends on mathematical problems that ordinary computers cannot solve in any practical timeframe.

A sufficiently powerful quantum computer changes that. Using Shor's algorithm it could solve those underlying problems efficiently, breaking RSA, ECC and Diffie-Hellman and undermining the confidentiality, integrity and authenticity guarantees they provide. Security professionals call such a machine a cryptographically relevant quantum computer, and the point at which its impact is felt Q-Day.

Two clarifications frame the work that follows. Symmetric algorithms such as AES, and hash functions such as SHA-2 and SHA-3, are far less affected; Grover's algorithm weakens them only modestly, and they remain usable with larger key and output sizes. The urgent problem is public-key cryptography, which is where RSA and ECC sit and where the standards effort has concentrated.

Algorithm	Quantum attack	Effect
RSA-2048 and above	Shor's algorithm	Broken; must be replaced
ECC (P-256, P-384, Curve25519)	Shor's algorithm	Broken; must be replaced
Diffie-Hellman, DSA, ECDSA	Shor's algorithm	Broken; must be replaced
AES-256	Grover's algorithm	Weakened; remains usable with larger keys
SHA-2, SHA-3	Grover's algorithm	Weakened; remains usable with larger outputs

Harvest now, decrypt later

An adversary does not need a quantum computer today to threaten your data today. Encrypted data can be intercepted and stored now, then decrypted years later once the capability exists. This strategy, harvest now, decrypt later, means that any information with a long secrecy lifetime is already exposed.

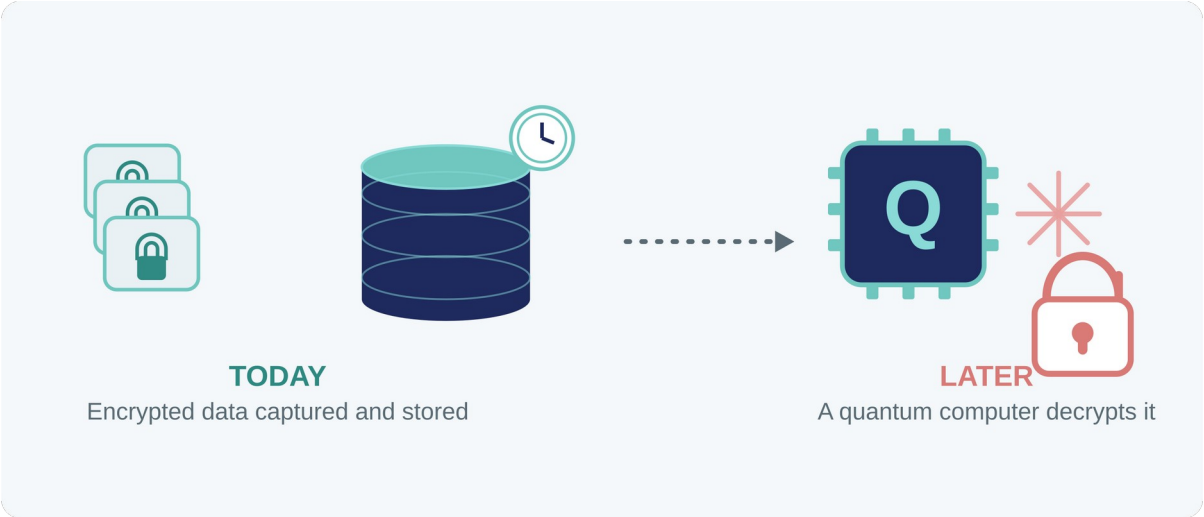

Figure 1. Harvest now, decrypt later: data captured and stored today can be decrypted once a capable quantum computer exists.

Examples include health and genomic records, financial and legal records, intellectual property, state and defence material, and the long-lived keys embedded in products and infrastructure. If data you transmit or store today must remain confidential beyond the next several years, the clock has already started.

Mosca's inequality: a simple test of urgency

A useful way to judge whether you are already behind is Mosca's inequality. Let X be the time your data must remain secret, Y the time it will take you to migrate, and Z the time until a cryptographically relevant quantum computer arrives. If X plus Y is greater than Z, then data you protect today will still be sensitive when it can be broken, and you are already exposed.

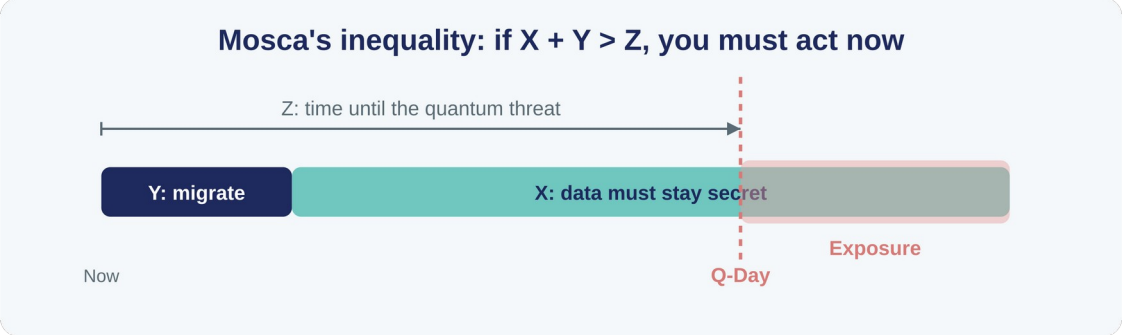

Figure 2. Mosca's inequality. Because migration (Y) is slow and data sensitivity (X) is long, the combined period easily extends past Q-Day (Z).

The practical force of the inequality is that Y, the migration time, is large for most organisations, and X, the secrecy lifetime, is large for the most sensitive data. Even under optimistic assumptions about Z, the only safe response is to begin reducing Y now by planning and inventorying, and to reduce exposure by prioritising long-lived data first.

2. The standards and regulatory landscape

The transition is no longer experimental. Standards bodies have published approved algorithms, and governments have set deadlines that will cascade into procurement requirements, industry standards and audit expectations, including for organisations not directly regulated.

Approved algorithms (NIST)

In August 2024 the United States National Institute of Standards and Technology (NIST) finalised its first three post-quantum standards after a multi-year evaluation. A further signature standard has since been submitted for publication, and an additional algorithm has been selected as a backup based on a different mathematical family.

Standard	Algorithm	Purpose
FIPS 203	ML-KEM (lattice-based)	Key establishment / encryption
FIPS 204	ML-DSA (lattice-based)	Digital signatures (primary)
FIPS 205	SLH-DSA (hash-based)	Digital signatures (stateless backup)
FIPS 206	FN-DSA (FALCON-based)	Signatures; submitted 2025, publication expected 2026
HQC	Code-based	Selected 2025 as a backup key-establishment algorithm

Parameter sets and security levels

Each algorithm offers several parameter sets at different NIST security levels, letting you trade size and speed against assurance. The defaults below suit most enterprise use; raise the level for the longest-lived secrets and root trust.

Parameter set	Type	NIST level	Typical use
ML-KEM-512	Key establishment	Level 1	Constrained or bandwidth-limited links
ML-KEM-768	Key establishment	Level 3	Recommended default for TLS and

Parameter set	Type	NIST level	Typical use
			VPN
ML-KEM-1024	Key establishment	Level 5	Maximum-assurance key exchange
ML-DSA-44	Signature	Level 2	Lighter-weight signing
ML-DSA-65	Signature	Level 3	Recommended default for signing
ML-DSA-87	Signature	Level 5	Root CAs and high-value signing
SLH-DSA	Signature (hash)	Levels 1 to 5	Firmware and long-term trust anchors

Deadlines and deprecation

Several authorities have set timelines. Treat the earliest applicable date as your planning anchor.

- **UK NCSC (the most relevant baseline for UK organisations):** its March 2025 guidance, Timelines for migration to post-quantum cryptography, sets three milestones; complete discovery and an initial migration plan by 2028, migrate your highest-priority systems by 2031, and complete migration across all systems, services and products by 2035.
- **NIST transition guidance (IR 8547):** legacy algorithms such as RSA-2048 and ECC P-256 are set to be deprecated around 2030 and disallowed within NIST standards by 2035; the guidance explicitly discourages waiting.
- **NSA CNSA 2.0:** sets a transition for United States national security systems across roughly 2030 to 2033; even outside that scope it functions as a de facto baseline because it flows through supply chains and procurement.
- **European Union:** the EU Coordinated Implementation Roadmap sets milestones, with initial measures expected around 2026 and high-priority use cases targeted for 2030; it is reinforced by the NIS2 directive, the Digital Operational Resilience Act (DORA) and the Cyber Resilience Act.
- **United States Executive Order 14306 (June 2025):** directs agencies to inventory cryptographic dependencies and requires publication of product categories that must support PQC, reinforcing the same direction of travel for vendors worldwide.

> **The convergent message**
>
> Although the wording differs, the UK, US and EU frameworks point to the same destination: a complete move away from RSA and ECC, with full migration expected by 2035 and the groundwork due far sooner.

3. Who is most exposed, and how long migration takes

Quantum risk is not evenly distributed. The organisations and systems most exposed share two characteristics: they protect data that must stay secret for many years, or they run on infrastructure with a long replacement cycle.

- Long secrecy lifetime: health, genomic, financial, legal, defence and personal data that retains value or sensitivity for a decade or more.

- Long-lived systems and products: industrial control systems, medical devices, vehicles, satellites, payment terminals and any connected hardware whose cryptography is difficult to update in the field.
- Embedded and root-of-trust keys: signing keys and certificates baked into firmware, which are costly and slow to rotate.

Migration is also slower than the transitions that preceded it. PQC involves larger key and signature sizes, hybrid schemes that combine classical and post-quantum algorithms during the transition, and coordination across an entire ecosystem of vendors and partners. Independent analyses estimate realistic enterprise timelines of roughly five to seven years for small organisations, eight to twelve years for medium organisations, and twelve to fifteen years or more for large, complex estates. Set against a 2035 endpoint, those figures explain why planning is urgent even though the final algorithms are now in hand.

This is not theoretical. Hybrid post-quantum protocols are already running in production at internet scale, including in major web browsers, content delivery networks and consumer messaging platforms, a useful signal that the standards are operational rather than speculative.

4. Sector spotlights

The principles in this guide apply everywhere, but the urgency, the regulatory pressure and the hardest practical problems differ by sector. The two profiled below sit near the top of almost every exposure ranking, because they combine long data secrecy lifetimes with long-lived systems.

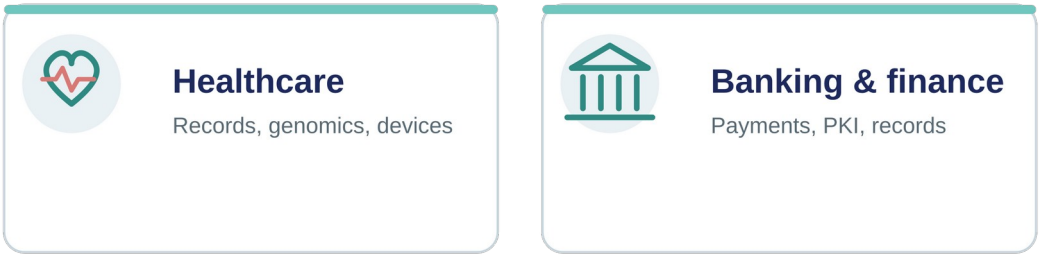

Figure 3. Two of the most exposed sectors, each combining decades-long data sensitivity with long-lived systems.

4.1 Healthcare and life sciences

Healthcare holds some of the most enduringly sensitive data in existence and runs it on equipment that stays in service for many years. Both facts make it one of the most exposed sectors, and to harvest now, decrypt later in particular. Genomic data is the extreme case: it is sensitive effectively forever, it implicates a patient's relatives, and it cannot be re-issued if exposed.

What is at risk

- Patient records and clinical data that must remain confidential for a patient's lifetime, and research and clinical-trial datasets that retain value for decades; these are exactly the archives most attractive to capture now and decrypt later.
- Electronic health record systems and patient portals, telehealth platforms, health information exchange (for example HL7 FHIR interfaces and DICOM imaging) and clinical email, all of which depend on TLS, PKI and digital signatures.

- Connected medical devices such as infusion and insulin pumps, cardiac monitors, imaging systems and remote diagnostics, which often remain in clinical use for a decade or more, with signing and authentication keys that are hard or impossible to update in the field. Here the risk is not only confidentiality but integrity and patient safety, since firmware and command authenticity guard against tampering.

Regulatory anchors

UK organisations handle special category data under UK GDPR and report against the NHS Data Security and Protection Toolkit, alongside NCSC guidance. Medical-device cybersecurity is increasingly treated as a patient-safety and liability matter, reflected in the IEEE 2621 series and in MHRA and FDA expectations. In the EU, NIS2 and the EU Coordinated Implementation Roadmap set the direction, with initial measures expected around 2026 and high-priority use cases targeted for 2030; organisations with US exposure also face HIPAA obligations and CISA guidance on harvest now, decrypt later.

Priority actions

- Inventory PKI, certificates and TLS across the clinical estate, and extend the inventory to device fleets and their firmware-signing roots.
- Prioritise long-retention data stores (records, genomics, research) and device signing keys, since these carry the longest secrecy lifetime and the slowest remediation.
- Engage device manufacturers now for their PQC firmware roadmaps and recertification timelines, and plan compensating controls such as network segmentation and monitoring for devices that cannot be updated.
- Pilot hybrid key establishment on portals, telehealth and exchange interfaces, and reduce unnecessary data retention to shrink the harvest now surface.

4.2 Banking and financial services

Financial services run on cryptography end to end, from a customer tap at a terminal to settlement between institutions, and the system is deeply interconnected. That combination makes migration both urgent and unavoidably collaborative; the sector's own working groups warn against what they call crypto-procrastination, where delay compresses the remaining work into an unrealistically short window.

What is at risk

- Customer and transaction data, identity and know-your-customer records, and market-sensitive information, much of which must stay confidential for years and is therefore exposed to harvest now, decrypt later.
- The public-key infrastructure and hardware security modules that underpin trust across online and mobile banking, together with code and firmware signing.
- Payment systems specifically: card provisioning and tokenisation, card-present and card-not-present transaction routing and authorisation, and ATM and point-of-sale estates, all of which rest on cryptographic assumptions now in scope for migration.
- Interbank messaging and settlement, for example SWIFT, and digital signatures used for contracts, instructions and digital-asset custody keys, where a compromise carries direct financial and legal-finality consequences.

Regulatory anchors

The sector's information-sharing body, FS-ISAC, has through its post-quantum working group published a financial-sector migration timeline and crypto-agility guidance, along with detailed

payment-card use cases, and it advises institutions to plan backward from the 2030 and 2035 milestones. In the EU, DORA requires firms to maintain the confidentiality, integrity and availability of their systems and to manage ICT risk, and NIS2 extends resilience obligations; a 2024 joint statement by eighteen member-state cyber agencies recommended migrating PKI and sensitive-data systems by the end of 2030. Globally, PCI DSS governs cardholder data, ISO/IEC 27001 covers information-security management, and the SWIFT Customer Security Programme is beginning to address PQC readiness, while CNSA 2.0 serves many institutions as a model timeline.

Priority actions

- Establish governance early, for example a post-quantum steering group with a named owner and a multi-year budget, and treat the migration as a programme rather than a project.
- Complete a cryptographic inventory before buying anything; you cannot migrate what you have not first discovered.
- Prioritise PKI and hardware security modules, payment authorisation paths, and long-confidentiality customer and market data.
- Coordinate explicitly with payment networks, processors, correspondent banks, cloud providers and key vendors, since no institution can migrate the shared rails alone.
- Deploy hybrid key establishment, for example ECDH combined with ML-KEM, and dual signatures during the transition, and automate certificate and key lifecycle management to support DORA and PCI evidence.

4.3 Other high-exposure sectors

Several other sectors share the same underlying profile and should plan with similar urgency.

- Government and defence: classified and diplomatic material with very long secrecy lifetimes, where CNSA 2.0 and national mandates apply directly.
- Telecommunications and critical infrastructure: long-lived network equipment and control systems, subject to NIS2 and sector regulators.
- Legal and professional services: client confidentiality obligations that can span decades.
- Energy and utilities: operational technology with very long replacement cycles and direct safety implications.

The common thread is simple: the longer your data must stay secret and the longer your systems stay in service, the sooner you must act.

5. Choosing algorithms and parameters

Once the standards are understood, most teams need a practical answer to a narrower question: which algorithm and parameter set for which job. The following profiles are sensible defaults; adjust upward in assurance for the longest-lived secrets and downward in size only where constraints genuinely demand it.

- **General-purpose TLS and VPN:** ML-KEM-768 for key establishment with ML-DSA-65 for signatures.
- **High-volume or constrained IoT:** ML-KEM-512 where bandwidth or compute is tight, accepting the lower assurance level deliberately.

- **Firmware and secure boot:** SLH-DSA, whose stateless hash-based design suits long-lived trust anchors that must remain verifiable for many years.
- **High-assurance code signing:** ML-DSA-87, or a hybrid classical-plus-post-quantum signature.
- **Internal PKI:** ML-DSA-65 for intermediate certificate authorities and ML-DSA-87 for root certificate authorities, which have the longest validity and the highest impact if compromised.

Hybrid approaches

During the transition, the prevailing pattern is hybrid cryptography, which runs a classical and a post-quantum algorithm together so that protection holds even if one is later found wanting. In key establishment this typically means combining X25519 with ML-KEM-768, often written X25519MLKEM768 in TLS 1.3; in signing it means concatenating a classical and a post-quantum signature so that both must validate. Hybrid key exchange is already supported in IETF specifications and in major browsers, which makes it a low-risk way to gain experience now.

6. Building your cryptographic inventory

You cannot migrate what you cannot see. A cryptographic inventory is the foundation of every credible programme, and the single most valuable artefact you can produce in the first year. It records where and how cryptography is used across the estate, including the parts hidden in third-party and cloud services.

Categories to map

- **Data in transit:** TLS versions and cipher suites across all endpoints, VPN protocols such as IPsec and WireGuard, API gateway and microservice communication, and database replication.
- **Data at rest:** database encryption (for example transparent data encryption and column-level encryption), file-system encryption, backup encryption, and cloud storage encryption.
- **Data in use:** container and orchestration secrets, memory encryption, and secure-enclave usage.
- **PKI and trust infrastructure:** internal certificate authorities, certificate chains and hierarchies, code and document signing, email encryption, and hardware security modules.
- **Authentication and identity:** SSH keys and key management, token and assertion signing algorithms, hardware authenticators, and directory and certificate services.

Discovery methods

- Network scanning to identify TLS versions, cipher suites and certificate types in use.
- Source-code and dependency analysis to find cryptographic libraries, supported by software bill of materials data.
- Audits of hardware security modules and key-management systems to record firmware versions and supported algorithms.
- Reviews of cloud key-management and certificate services to capture their capabilities and limits.

Classify and prioritise by risk

With the inventory in hand, rank assets so that the most exposed and slowest-to-change are scheduled first. The matrix below is a useful starting template.

Asset class	Quantum sensitivity	Priority	Complexity
Root CA keys	Critical (10 to 20 year validity)	P0	High
Code-signing keys	Critical	P0	High
IoT and device firmware	Critical (device lifetime)	P0	High
TLS edge certificates	High (1 to 2 year validity)	P1	Medium
Internal API mutual TLS	High	P1	Medium
VPN infrastructure	High	P1	Medium
Database encryption	Medium	P2	Medium
Email encryption	Medium	P2	Low

Extending a software bill of materials into a cryptography bill of materials (CBOM) lets you attach this detail to your supply chain and track posture automatically over time, rather than as a one-off spreadsheet.

7. A phased migration roadmap

The most widely endorsed approach, reflected in guidance from the UK NCSC and the joint CISA, NSA and NIST factsheet, is a phased programme anchored to milestone dates. The phases below follow the NCSC structure because it is the clearest fit for UK organisations; the activities apply equally well wherever you operate.

Figure 4. The UK NCSC three-phase migration timeline, with the headline activity for each milestone.

Phase 1: Assess and plan (now to 2028)

The goal of this phase is complete visibility and a credible plan. You cannot protect what you cannot see, and a migration plan without an inventory is guesswork.

- Establish governance: name an executive owner, form a small cross-functional team, and secure a multi-year budget line.
- Build the cryptographic inventory and CBOM described in the previous section.

- Assess and prioritise risk by data secrecy lifetime, system lifespan and exposure, so that the most at-risk systems are scheduled first.
- Engage your supply chain: ask vendors for PQC roadmaps and timelines, and make crypto-agility a procurement requirement.
- Produce the migration plan, mapping prioritised systems to the 2031 and 2035 milestones with dependencies and constraints.

Phase 2: Prioritise and upgrade (2028 to 2031)

With the plan in place, execute the highest-priority migrations first, refining as standards and tooling mature.

- Migrate the systems that protect long-lived secrets and the most exposed external services, including customer-facing systems, key establishment and high-value signing.
- Deploy hybrid cryptography so that security holds even if one algorithm is later found wanting.
- Automate certificate and key management so issuance, renewal and rotation no longer depend on manual effort.
- Validate interoperability and performance, and test thoroughly in non-production before rollout.

Phase 3: Complete migration and retire legacy (2031 to 2035)

The final phase removes quantum-vulnerable cryptography from production and embeds the ability to adapt in future.

- Complete migration across all remaining systems, services and products, including legacy and embedded estates.
- Remove RSA and ECC dependencies and retire legacy certificates and keys.
- Establish continuous monitoring and governance so cryptographic posture is tracked as a living system.
- Demonstrate compliance against relevant regimes, which for many UK and European organisations will include data protection, operational resilience and sector-specific obligations.

An illustrative implementation timeline

Within those milestones, larger organisations often find it helpful to sequence the technical work in overlapping waves. The pattern below is illustrative, not prescriptive, and compresses or extends with the size of the estate.

- Months 1 to 6, preparation: complete the inventory, classify data, stand up an isolated PQC test environment, and begin vendor engagement.
- Months 6 to 12, foundation: update cryptographic libraries to PQC-capable versions, build crypto-agility into critical applications, pilot hybrid key exchange in non-production, and begin HSM firmware upgrades.
- Months 12 to 24, PKI migration: issue hybrid certificates in test, update the internal CA hierarchy to support ML-DSA, and migrate root and intermediate keys first because of their long validity.

- Months 18 to 30, infrastructure: migrate VPN, WAN, service-mesh and database key-wrapping to PQC, and extend PQC across cloud key management.
- Months 24 to 36, applications: migrate application-level encryption, code-signing pipelines, email and document signing, and device authentication.
- Months 30 to 48, hardening: remove classical dependencies where no longer needed, complete deprecation of RSA and ECC for high-risk uses, and run red-team and side-channel assessments.

8. Foundational practices that make migration work

Cryptographic inventory and the CBOM

Every credible roadmap starts with discovery, not with buying a product. The inventory and CBOM described in Section 6 are what make everything else possible; without them, prioritisation is guesswork and progress cannot be measured.

Crypto-agility

Crypto-agility is the ability to replace cryptographic algorithms, protocols, certificates and libraries without redesigning entire systems. It is the difference between a controlled swap and a painful re-engineering effort, and it is the single most valuable design property to build now, because the algorithms will change again.

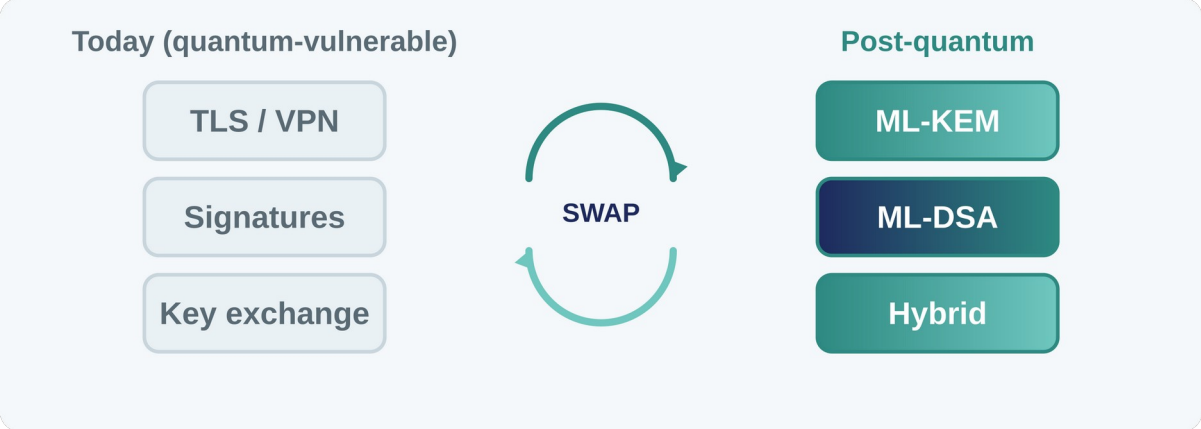

Figure 5. Crypto-agility lets you replace quantum-vulnerable algorithms with post-quantum equivalents without re-engineering systems.

Practical agility comes from abstracting cryptography behind well-defined interfaces rather than hardcoding algorithms, supporting algorithm negotiation, designing certificate formats that allow multiple signature types, ensuring hardware security modules can load new firmware, and maintaining backward compatibility during transition periods. National guidance now frames agility as a practical necessity rather than an academic ideal.

Crypto-agility maturity model

A simple maturity model helps you gauge progress and set a target. Most organisations begin at Level 1 or 2; a sensible goal is to reach Level 4 by 2028.

Level	Characteristics
1 Reactive	Hardcoded algorithms; manual, ad hoc updates
2 Defined	Inventory exists; updates are planned

Level	Characteristics
3 Managed	Automated certificate lifecycle and algorithm negotiation
4 Optimised	Real-time response and automatic algorithm fallback
5 Predictive	Continuous, risk-driven assessment and proactive migration

Hybrid deployment during transition

Hybrid schemes that run a classical and a post-quantum algorithm together provide a sensible safety margin during the migration window. They preserve protection if implementation issues or new analysis affect either algorithm, and they ease interoperability with partners migrating at different speeds.

Risk-based prioritisation

Not all cryptographic assets carry equal risk. Concentrate first on high-value, long-lifespan data and on systems whose cryptography is hardest to change later. Prioritisation is where limited budget and engineering time earn the greatest return, and it is the step most often skipped.

9. Deep technical considerations

Post-quantum algorithms are not drop-in replacements of identical size and speed. Planning for their practical characteristics avoids unpleasant surprises late in a programme.

Performance and resource impact

Post-quantum keys and signatures are larger than their classical equivalents, and some operations are slower, particularly on constrained hardware.

Parameter set	Sign	Verify	Signature size	Public key
ML-DSA-65	Fast	Fast	~3.3 KB	~2.0 KB
ML-DSA-87	Fast	Fast	~4.6 KB	~2.6 KB
SLH-DSA-128s	Slow	Fast	~8 KB	~1 KB
ML-KEM-768	n/a	n/a	n/a	~1.2 KB

The practical consequences are worth planning for: certificate chains carrying post-quantum signatures can be several times larger, TLS handshakes carry more data, signing throughput on hardware security modules may fall noticeably, constrained devices generally favour ML-DSA over the slower-signing SLH-DSA, and databases that store keys or signatures need more space. Size capacity and budget accordingly rather than discovering the impact in production.

Side-channel resistance

Lattice-based algorithms can leak information through timing, power consumption and induced faults if implemented carelessly. Constant-time implementations are mandatory, power analysis matters most for hardware security modules and smart cards, and fault attacks must be considered for high-assurance use. The practical safeguards are to use audited or formally verified implementations, to require FIPS 203, 204 and 205 validation for production, and to commission dedicated side-channel assessments for the most sensitive environments.

Randomness and entropy

Post-quantum algorithms depend on high-quality randomness for key generation and for signature operations; weak entropy undermines otherwise sound cryptography. Ensure random number generators meet recognised entropy standards and that entropy sources are validated, especially in virtualised and embedded environments where good randomness is harder to guarantee.

Key management complexity

Larger keys and signatures, multi-tier certificate hierarchies that compound signature sizes, and finite hardware-security-module capacity all add operational complexity. Update key-management databases and escrow procedures for the larger formats, and verify storage limits and transaction rates before committing to a design.

10. Governance, people and budget

A quantum-readiness task force

Migration succeeds or stalls on ownership. Stand up a small, named task force with clear roles.

- Executive sponsor, for example the CISO or CTO, who holds budget and authority.
- Technical lead, a security architect or cryptographer responsible for algorithm selection and implementation.
- Infrastructure lead for network, hardware security module and PKI migration.
- Application lead for code changes and library updates.
- Compliance and legal for regulatory requirements and vendor contracts.
- Vendor management for third-party and supply-chain risk.

Vendor and supply-chain management

Much of your cryptography lives in products you buy, so vendor engagement is part of the critical path. Ask every significant vendor the same questions.

- What is your PQC roadmap, with specific dates rather than general intentions?
- Which NIST algorithms will you support, and by when?
- Do you support hybrid modes during the transition?
- What hardware or firmware updates will be required?
- How will you handle certificate-chain compatibility?
- What test environments will you provide for PQC validation?

Pay particular attention to certificate authorities, hardware-security-module vendors, VPN and network equipment suppliers, cloud key-management and certificate services, and browser and client software, since these sit on the critical path for most estates.

Skills and training

Different audiences need different preparation: executives need threat awareness, business risk and the regulatory timeline; security architects need algorithm theory and selection criteria; developers need secure implementation and crypto-agility patterns; operations teams need

certificate-lifecycle and hardware-security-module skills; and procurement needs vendor-evaluation criteria.

Budget and return on investment

Typical cost categories include software and library support, hardware where current modules cannot support PQC, professional services for assessment and testing, internal labour (often in the range of fifteen to twenty-five per cent of security-engineering capacity over two to three years), test infrastructure, and training. The most useful framing for boards is risk mitigation rather than cost: the cost of a quantum-enabled breach, including mass decryption of harvested data, forged signatures and a compromised PKI, far exceeds the cost of an orderly transition.

11. Testing and validation

Interoperability testing

- Test post-quantum and hybrid algorithms across client and server combinations, including browsers, mobile stacks and any constrained devices, paying attention to larger certificate sizes.

Performance benchmarking

- Establish baselines for current cryptographic operations, then measure latency for handshakes, VPN establishment and API calls under PQC, and load-test hardware security modules and databases with the larger keys and signatures.

Security testing

- Penetration-test the implementations, conduct side-channel analysis where assurance demands it, fuzz library interfaces, and apply formal verification to the most critical components where feasible.

12. Compliance, legal and regulatory

The regulatory picture is converging on the same direction set out in Section 2. NSA CNSA 2.0 frames a 2030 to 2033 transition for national security systems; FIPS 203, 204 and 205 are the federal algorithm standards; and in Europe the NIS2 directive, DORA and the Cyber Resilience Act increasingly bear on cryptographic resilience, alongside sector regimes such as PCI DSS in payments and data-protection rules in healthcare. Expect PQC readiness to feature in audits and procurement well before the final deadlines.

Contractual and insurance implications

- Update security questionnaires and due-diligence to include PQC readiness.
- Add PQC clauses to procurement contracts for security-critical software and services.
- Review cyber-insurance policies for quantum-related exclusions or expectations.
- Document transition progress so it can be evidenced in regulatory examinations.

13. Common pitfalls to avoid

- Waiting for a fixed Q-Day before acting; the harvest-now-decrypt-later threat means long-lived data is already exposed.

- Buying a product before completing an inventory; tooling cannot fix what has not been discovered.
- Treating PQC as a one-off project rather than building durable crypto-agility for future changes.
- Overlooking embedded, legacy and supply-chain cryptography, which is usually the slowest and most expensive to migrate.
- Underestimating timelines; large estates can take well over a decade, so 2035 is closer than it appears.
- Ignoring cryptography you cannot see, including primitives embedded in the AI models you increasingly depend on.

14. Measuring and assuring your posture with Physivitis tools

Physivitis develops deep-technology innovations for the quantum era, including a cybersecurity portfolio aimed squarely at the challenges in this guide. Two tools address blind spots that most programmes struggle with: turning posture into a defensible number, and seeing cryptography hidden inside AI models. Both support, rather than replace, the standards-based migration described above.

USMC: a single, auditable security margin

Every CISO faces the same question from boards, regulators and customers: are we secure, and by how much? The honest answer is usually qualitative. USMC makes it quantitative. It computes a single, auditable security margin in bits by combining six independently measurable cryptographic parameters under the Physivitis QRESB framework. A positive margin confirms a system exceeds the NIST 128-bit threshold; a negative margin shows exactly how much exposure remains and which dimension is the binding constraint.

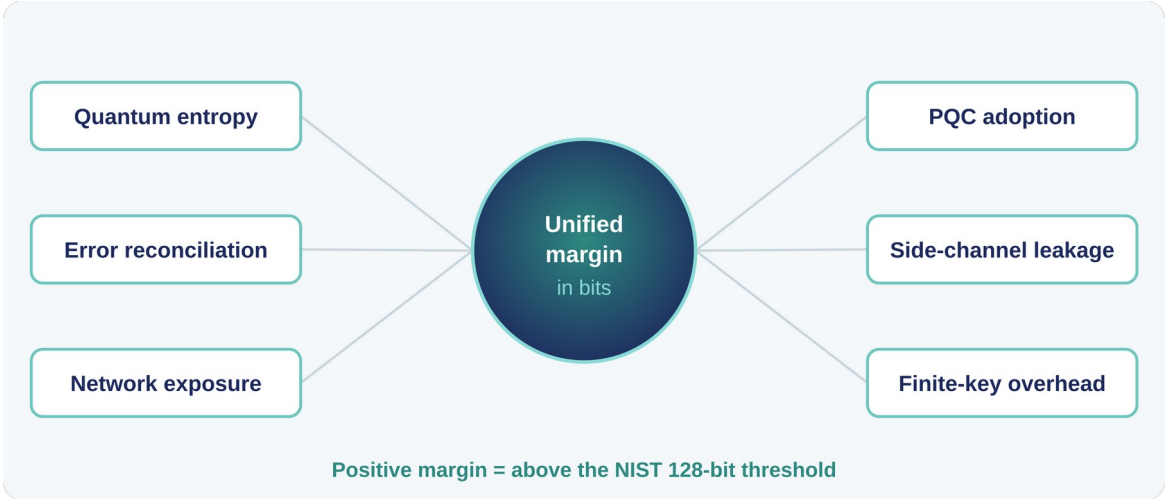

Figure 6. USMC combines six measurable dimensions into one auditable security margin in bits.

The six dimensions

- **Quantum entropy:** the actual entropy available from your quantum or classical random number sources.
- **Post-quantum cryptography:** your adoption of NIST-standardised PQC algorithms across key exchange and signatures.

- **Error reconciliation:** the security loss from reconciliation protocols and information leakage in quantum key distribution.
- **Side-channel leakage:** the reduction attributable to implementation-level side-channel vulnerabilities.
- **Network topology exposure:** the attack surface presented by your network architecture to external adversaries.
- **Finite-key overhead:** the penalty from operating with finite, rather than asymptotically large, key blocks.

How it works

1. Enter your cryptographic configuration across the six components; guided defaults and tooltips make this accessible without deep cryptographic expertise.
2. The QRESB engine combines the components into a unified, auditable margin in bits.
3. Review the verdict; a positive margin confirms you meet the threshold, while a negative margin shows where your exposure lies and which component is the binding constraint.
4. Export a timestamped, branded PDF report with verdict interpretation, regulatory compliance mapping and per-dimension assessment, ready to attach to board reports, compliance documentation or regulatory submissions.

USMC suits organisations where posture must be measurable and defensible: financial institutions migrating under regulatory pressure, government and defence contractors, quantum communication operators, critical infrastructure operators, telecommunications providers and security consultancies. Within this guide, it directly supports the risk-based prioritisation of Phase 1 and the ongoing assurance and evidence required through Phases 2 and 3.

Explore USMC at physivitis.tech/services/usmc

TCBA: auditing the cryptography inside AI models

Every CISO has a software bill of materials and can list the cryptographic libraries their code depends on. Almost none can answer a different question: what cryptographic primitives live inside the weights of the AI models we run? Embedded cryptography in model parameters is not theoretical; it can arise by intentional placement, by incidental learning from training data, or by adversarial insertion during fine-tuning or quantisation. TCBA is an audit primitive for exactly this surface, built for the regulatory perimeter created by the EU AI Act, DORA and the Cyber Resilience Act.

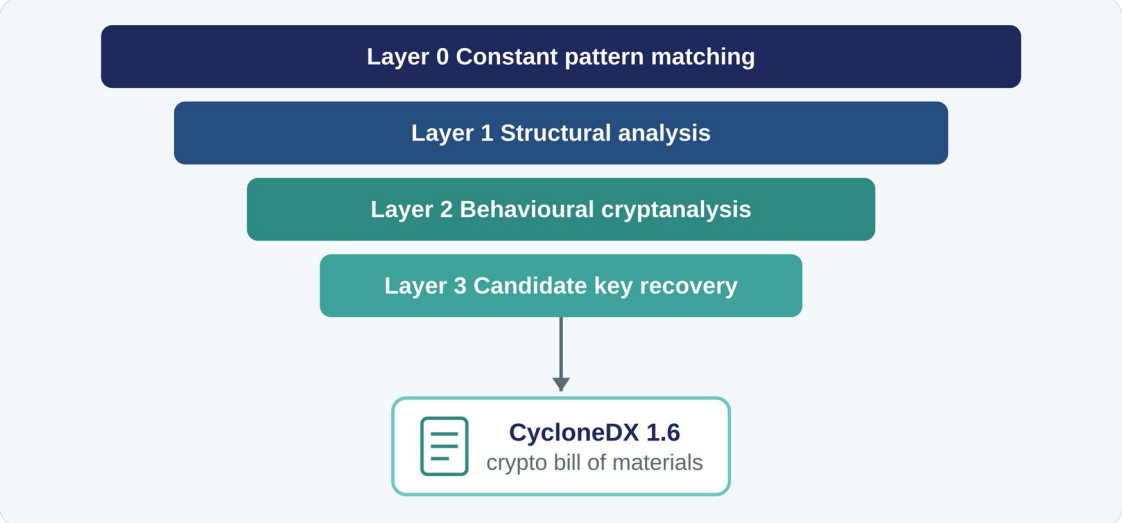

Figure 7. TCBA scans a model across four layers and emits a CycloneDX 1.6 cryptographic bill of materials.

TCBA scans a model artefact across four detection layers, each more expensive than the last, so that earlier layers narrow the search space for later ones and deep analysis stays tractable on full-size production models.

- **Layer 0, constant pattern matching:** identifies known cryptographic constants within raw tensor bytes and within integer projections of floating-point values at numerical scales of 255, 256 and identity, catching primitives embedded as scaled floats, not only as direct byte patterns.
- **Layer 1, structural analysis:** singular value decomposition of weight matrices, two-dimensional FFT, bit-plane decomposition of quantised tensors, and graph matching against substitution-permutation, Feistel, sponge and Merkle-Damgard templates.
- **Layer 2, behavioural cryptanalysis:** treats the model as a callable function and applies avalanche tests against the strict avalanche criterion, differential probing, linear approximation search and algebraic degree estimation. Available on the Enterprise tier.
- **Layer 3, candidate key recovery:** authorisation-gated recovery of candidate key material for detected primitives, with procedures for AES key schedules, RSA exponents and elliptic-curve scalars. Defence and Forensics tier only.

Inputs and output

TCBA accepts safetensors, ONNX, PyTorch state dictionaries and GGUF artefacts, with streaming uploads to two gigabytes on the Pro tier and an on-premises appliance for larger or restricted artefacts. Every scan classifies each detected primitive as quantum-vulnerable, quantum-weakened or quantum-resilient against your chosen threat horizon, recommends a post-quantum replacement, and produces a timestamped, optionally signed CycloneDX 1.6 bill of materials in the proposed MBOM-PQC schema extension to OWASP CycloneDX, ready for conformity submissions, supply-chain registries, board packs or regulator filings.

How it works

1. Upload your artefact in safetensors, ONNX, PyTorch or GGUF format.
2. Scan across the four layers, from constant pattern matching through optional authorisation-gated key recovery.
3. Score each primitive for quantum vulnerability against your chosen threat horizon, with a recommended PQC replacement.

4. Download the CycloneDX 1.6 cryptographic bill of materials for your evidence trail.

Explore TCBA at physivitis.tech/services/tcba

Used together, USMC quantifies your cryptographic posture and TCBA surfaces cryptography that conventional inventories miss, closing two of the gaps that most readiness programmes leave open. Both are available through Physivitis; whichever tools you choose, the foundational steps remain the same: inventory, prioritise, plan, migrate in phases and build crypto-agility.

15. Quick-start checklist

If you do nothing else, work through the following in sequence.

This quarter

1. Assign an executive owner for quantum readiness and form a small cross-functional team.
2. Initiate the enterprise cryptographic inventory, beginning with your most sensitive and longest-lived data.
3. Contact your top five critical vendors for their PQC roadmaps in writing.
4. Stand up an isolated test environment for PQC algorithms.

Next quarter

1. Complete the risk classification of your cryptographic assets.
2. Select PQC algorithm profiles for each asset class.
3. Begin developer training on PQC implementation and crypto-agility.
4. Update procurement templates with PQC requirements.

This year

- Deploy hybrid PQC in non-production and issue your first hybrid certificates.
- Update hardware-security-module infrastructure for PQC support.
- Publish internal PQC standards and policies, and map your migration plan to the 2028, 2031 and 2035 milestones.
- Quantify your current exposure so you can prioritise and measure progress.

16. Glossary

Term	Meaning
PQC	Post-quantum cryptography; algorithms designed to resist attacks from both classical and quantum computers.
RSA / ECC	Widely used public-key algorithms whose security a quantum computer could break.
Shor / Grover	Quantum algorithms; Shor breaks public-key cryptography, Grover weakens symmetric algorithms and hashes.
CRQC	Cryptographically relevant quantum computer; a machine powerful enough to break current public-key cryptography.
Q-Day	The point at which a CRQC can defeat today's encryption in practice.
HNDL	Harvest now, decrypt later; capturing encrypted data today to decrypt once

Term	Meaning
	a CRQC exists.
Mosca's inequality	If the secrecy lifetime plus the migration time exceeds the time to the quantum threat, you are already exposed.
KEM	Key encapsulation mechanism; a method for establishing a shared secret, as in ML-KEM.
ML-KEM	Module-Lattice Key Encapsulation Mechanism (FIPS 203); the primary standard for key establishment.
ML-DSA / SLH-DSA	Standardised post-quantum digital signature algorithms (FIPS 204 and FIPS 205).
Hybrid	Running a classical and a post-quantum algorithm together during the transition.
Crypto-agility	The ability to change cryptographic algorithms and keys without re-engineering systems.
SBOM / CBOM	Software and cryptography bills of materials; inventories of software and of cryptographic assets.
CycloneDX / MBOM-PQC	An open bill-of-materials standard, and a proposed schema extension for model cryptography.
HSM	Hardware security module; a tamper-resistant device that stores keys and performs cryptographic operations.
DORA / NIS2	EU regimes for operational resilience and network and information security that bear on PQC readiness.

17. References and further reading

This guide draws on publicly available guidance from the following authorities. Consult them directly for the authoritative detail.

- UK National Cyber Security Centre (NCSC): Timelines for migration to post-quantum cryptography (2025).
- US National Institute of Standards and Technology (NIST): FIPS 203, 204 and 205 (2024); transition guidance IR 8547; crypto-agility paper CSWP 39; entropy guidance SP 800-90 series.
- CISA, NSA and NIST: Quantum-Readiness: Migration to Post-Quantum Cryptography (joint factsheet); NSA CNSA 2.0.
- European Union: Coordinated Implementation Roadmap for the transition to post-quantum cryptography; NIS2 directive; Digital Operational Resilience Act (DORA); Cyber Resilience Act; EU AI Act.
- Financial services: FS-ISAC Post-Quantum Cryptography Working Group, including its financial-sector migration timeline, crypto-agility guidance and payment-card use cases; PCI DSS; SWIFT Customer Security Programme.
- Healthcare: IEEE 2621 series on medical-device security; UK GDPR and the NHS Data Security and Protection Toolkit; US HIPAA.
- Standards and tooling: OWASP CycloneDX and the proposed MBOM-PQC extension; ETSI and ENISA quantum-safe guidance.

About Physivitis

Physivitis Ltd is a UK-registered deep-technology company developing innovations across quantum computing, sensing, cybersecurity, energy and advanced materials. Its cybersecurity portfolio focuses on helping organisations measure and strengthen their resilience as the cryptographic landscape shifts toward the post-quantum era.

Contact: contact@physivitis.tech

Physivitis Ltd, 71-75 Shelton Street, Covent Garden, London WC2H 9JQ. Company No. 16996492.

Disclaimer: This guide is provided for general information only and does not constitute legal, regulatory or professional security advice. Standards and deadlines may change; verify current requirements with the relevant authorities and seek qualified advice for your specific circumstances. References to standards and government guidance are for general reference and do not imply any endorsement of Physivitis or its products.