

Building a PQC Migration Roadmap

A practical, phased approach to migrating to post-quantum cryptography – grounded in discovery, prioritised by business risk, and built to survive contact with a real production environment.

Migration Is an Organisational Transformation, Not an Algorithm Swap

It's tempting to think of post-quantum migration as a technical substitution: replace RSA with ML-KEM, replace ECDSA with ML-DSA, done. In practice, cryptography is embedded across applications, infrastructure, certificate authorities, third-party integrations, and hardware that wasn't designed with algorithm changes in mind. A credible roadmap treats migration as a multi-year organisational programme with clear phases, not a single cutover.

The Six-Stage Lifecycle

Enterprise Cryptographic Exposure Management (ECEM) structures migration around a continuous, six-stage cycle:

-  Discover – identify cryptographic assets across endpoints, applications, PKI, HSMs, cloud and source code.
-  Inventory – consolidate findings into a living Enterprise CBOM.
-  Assess – score exposure using business context and recognised guidance (NIST, CNSA 2.0).
-  Prioritise – focus remediation where it reduces the most real exposure, not just the most findings.
-  Transition – execute a phased, hybrid-first migration with rollback built in.
-  Monitor – track posture continuously, since exposure changes every time infrastructure does.

Start Where Impact Is High and Blast Radius Is Low

The organisations that make real progress don't attempt to migrate everything simultaneously. They identify a small number of pilots where the security value is meaningful but the risk of disruption is contained – commonly, externally-facing TLS/mTLS endpoints and code or firmware signing workflows – and prove the approach there first.

A **hybrid-first** approach – deploying classical and post-quantum algorithms together, rather than a hard cutover – is the pattern most organisations converge on. It preserves interoperability with systems that haven't migrated yet, keeps a classical fallback available if something goes wrong, and lets real performance data (handshake latency, CPU overhead) be gathered under production-like conditions before wider rollout.

The Bottleneck Nobody Budgets For: Certificate Lifecycle

Manual certificate and key management is the single most common reason migration timelines slip. If issuing, rotating, and retiring certificates still depends on manual tickets and tribal knowledge, every pilot and every wider rollout will be gated by that process, regardless of how ready the cryptography itself is.

Automating certificate lifecycle management early – well before large-scale migration begins – removes this bottleneck before it becomes the limiting factor on everything else.

Governance: Making Progress Visible to the Board

A migration programme that only technical teams can see is a migration programme that's vulnerable to losing funding and attention. Reporting a small set of consistent metrics on a regular cadence – CBOM coverage, percentage of systems with hybrid capability, certificate automation rate, and remaining high-priority exposure – turns a multi-year technical programme into something a board can actually track and continue to sponsor.

A Realistic Timeline

Discovery and initial inventory are typically achievable within weeks using agentless tooling. A contained pilot on a chosen channel – with proper baseline measurement, gradual traffic increase, and stability validation – reasonably takes a small number of months. Scaling across an estate and embedding ongoing governance is realistically a multi-year effort for

any organisation of meaningful size. None of this is a reason to delay starting; it's the reason to start with discovery now, since the exposure clock on long-lived data is already running.

© 2026 Quantum Sentinel™. All rights reserved.

Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.

[Privacy Policy](#)

[Cookie Policy](#)

[Terms of Use](#)