

Post-Quantum Readiness: Governance Before Migration

Working draft for review

Original text: 23 September 2026 | Candidate revision: 10 October 2026

The post quantum transition is not just a cryptography project. It is an enterprise governance and organisational resilience challenge.

Quantum capable systems may eventually undermine widely used forms of public key cryptography. Organisations therefore face a long transition involving data, applications, hardware, suppliers, contractual dependencies and systems that were never designed for rapid cryptographic change.

The first challenge is visibility. An organisation cannot govern a transition if it does not know where cryptography is used, which data must remain secure for many years, which systems are difficult to change, which suppliers control critical dependencies or who owns the relevant decisions.

That is why post quantum readiness begins before migration. It begins with governance, inventory, prioritisation, ownership and evidence. Technical specialists remain essential, but executive accountability cannot be outsourced to specialists or vendors.

The developing Lighthouse approach is intended to connect the transition to an auditable pathway: identify objectives and obligations, understand cryptographic assets and dependencies, assess long-lived data risk, identify gaps, assign owners, plan remediation and preserve evidence that change is occurring. The current example is fictional and has not received specialist review or user testing.

The broader lesson extends beyond quantum risk. Institutions need crypto agility: the capacity to understand and change cryptographic controls without rediscovering the entire environment during every crisis or standards transition.

Post quantum readiness is therefore a practical test of institutional intelligence. Can the organisation see across technology, governance, procurement and risk? Can it prove what it knows? Can it make accountable decisions under uncertainty? And can it adapt before urgency removes its choices?

Review boundary: governance and planning, not a technical implementation assessment, security certification or completed migration. Specialist review remains pending. ASD milestones are recommendations, not a universal statutory deadline.

Primary sources checked 8 October 2026:

ASD planning guidance · ASD supplier questions · NIST FIPS 203 (ML-KEM) · NIST FIPS 204 (ML-DSA)

Corrections and research enquiries: aaron@aequitasnexus.org