

Quantum readiness is a migration programme

Quantum security and cryptographic transition — technical reading

Quantum risk is often introduced as a contest between new hardware and old encryption. An enterprise decision-maker faces a more immediate problem: cryptography is distributed across systems that no single team inventories completely. It lives in certificates, remote access, embedded devices, software updates, signatures, identity infrastructure, archival records and supplier equipment with very different replacement cycles.

The first useful quantum-readiness deliverable is not a promise of quantum advantage. It is a cryptographic dependency map linked to business criticality and data lifetime. Information that must remain confidential for decades may deserve earlier attention than a short-lived operational session. Equipment that cannot accept future cryptographic updates may create a procurement risk today even if it is not presently exposed.

A migration programme groups dependencies by protocol, algorithm, key management, ownership, firmware constraints and contractual support. Teams first establish an inventory and vendor position, then test hybrid or post-quantum approaches in a controlled environment. The evaluation includes compatibility, performance, certificate size, latency, recovery, interoperability and the practical ability to roll back.

The governing principle is crypto-agility. Customers should be able to replace algorithms and cryptographic providers without rebuilding the entire service. New contracts should require transparent cryptographic inventories, updatable components, lifetime support commitments and demonstrable migration plans. Security exceptions must have expiry dates and accountable owners.

Quantum readiness is thus an engineering and procurement discipline long before it becomes a hardware project. The outcome is a manageable migration portfolio: what to protect first, which suppliers must answer questions, which systems to modernise and how to prove that the transition has not weakened availability.