

PQC migration cost drivers

Sample: synthetic answers for a vendor-heavy organization. A planning worksheet, not a cost estimate.

What drives your migration effort

High	Supplier dependency Cryptography inside vendor products moves on the vendor's roadmap, not yours. Each critical supplier needs a dated plan and an attestation (QCI-QS1 gate G70).
Medium	Number of systems Every critical system needs its cryptography found, prioritized, changed and tested.
Medium	Hard-coded and legacy cryptography Algorithms fixed in code have to be rewritten, not reconfigured.
Medium	Inventory gap Without a validated inventory, every other number on this page is a guess, and QCI-QS1 caps the score at 60 (gate G60).
Medium	Team capacity Migration runs for years; without named owners, work stalls between projects.
Medium	Untested crypto agility Until one algorithm swap has been tested end to end, the effort of the rest is unknown (gate G80).

What can wait and what is late

- Data confidentiality is already late: data that must stay secret for 10 years or more can be recorded now and decrypted later.
- Supplier answers take time to collect: requests and a 60-day response window come before any migration you depend on.

What you can't size yet

- Certificates and keys in use: Your certificate-management or PKI tooling can count issued certificates and keys.
- System and dependency counts: Treat counts as estimates until a validated inventory confirms them.

Suggested first step: Supplier Readiness Pilot

Your largest driver sits with vendors. The pilot asks your critical suppliers for their plans and gives your board a one-page answer in 30 days.

Your answers

Critical systems in scope: 25 to 100

Critical suppliers: 25 to 100

Who controls most of your cryptography: Mostly vendors (core, card, cloud, SaaS)

Certificates and keys in use: Don't know

Longest period some data must stay confidential: 10 years or more

Hard-coded or legacy cryptography: Some

Cryptographic inventory: Partial

People who can work on migration: Part-time owners

Crypto-agility test (swap an algorithm end to end): Not done