



One PQC journey for IT and OT

Secure, Assure and SOAR connect infrastructure context, application evidence and governed response so each migration decision has an owner and can be rechecked.

The transition problem

PQC migration is a program of evidence, ownership and controlled change. Leaders need to know which services matter, where cryptography lives, what can change safely and which proof closes each decision.

Secure

Establish infrastructure identity, services, exposure and accountable estate ownership.

Leaves: A scoped estate record and the questions that still need evidence.

Assure

Examine application source, dependencies, cryptographic use and engineering evidence.

Leaves: An owned source-level remediation plan.

SOAR

Investigate operational signals, rehearse choices and govern authorized response.

Leaves: A defensible decision, execution boundary and fresh verification.

01 / Scope

Choose critical services and information lifetimes.

02 / Map

Connect assets, services, repositories and owners.

03 / Change

Design the cryptographic and operational migration.

04 / Govern

Preserve authority, exceptions and recovery.

05 / Verify

Recheck the changed service with fresh evidence.

ESTATE CONTEXT

What exists and what remains unseen.

SOURCE EVIDENCE

Where cryptography is implemented.

DECISION RECORD

Who may act and under which boundary.

MIGRATION PROOF

What changed and what remains classical.

One portfolio, three accountable decisions: know the estate, change the application and govern the operation.

EVIDENCE



ACCOUNTABLE OWNER



DECISION



FRESH VERIFICATION



Discover the cryptographic estate

The first milestone is a bounded view of critical assets, applications, trust relationships and information lifetimes - with every relationship supported or visibly unresolved.

Start with the information that must remain trustworthy

Prioritize by information lifetime, operational consequence, migration duration and external dependency. Long-lived data and difficult-to-change OT systems may require action before a cryptographic failure becomes urgent.

Secure: infrastructure context

Scope assets, services, identity confidence, software evidence, collection limits and accountable owners.

Assure: source evidence

Locate cryptographic roles in source and dependencies; retain exact code, scan scope and review status.

External records

Add supplier, platform and device statements only with explicit provenance, freshness and owner validation.

Build a migration register leaders can use

SERVICE AND OWNER

Critical service, BU, accountable owner and business consequence.

INFORMATION LIFETIME

How long confidentiality, authenticity or integrity must endure.

CRYPTOGRAPHIC ROLE

Key establishment, signature, certificate, protocol or stored-data dependency.

EVIDENCE AND FRESHNESS

Observed, source-linked, supplier-declared or inferred; timestamp and scope.

MIGRATION PATH

Target standard, compatibility boundary, testing and recovery plan.

DECISION STATE

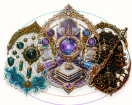
Investigate, plan, change, verify, accept temporarily or retire.

Boundary to retain

Secure planning examples do not establish customer cryptographic use. Source, customer, supplier and platform evidence keep separate provenance until the asset-service-repository relationship is verified.

Outcome: leadership sees which migration questions are supported, which are assumed and who must close each gap.

OBSERVED	➤	SOURCE-LINKED	➤	SUPPLIER-DECLARED	➤	UNRESOLVED
----------	---	---------------	---	-------------------	---	------------



Move from inventory to verified migration

Application and infrastructure evidence meet at the service boundary: what must change, who owns it, how operations stay safe and what proves the result.

Turn verified evidence into migration work

Assure connects cryptographic findings to exact source, dependencies and engineering owners. Secure supplies service and infrastructure context after the asset-service-repository relationship is verified. SOAR preserves the operational decision and its authority boundary.

Prepare the change

Name the cryptographic role, target standard, compatibility window, supplier dependency, data that must remain readable and recovery condition.

Change through ownership

Use the authorized source, certificate, protocol, firmware or configuration process. Keep approval, exceptions and temporary measures explicit.

Verify the service

Collect fresh source, build, deployment and infrastructure evidence. Recheck dependent services and record remaining classical dependencies.

IT migration

Coordinate code, libraries, certificates, identity systems and deployment pipelines. Use staged compatibility and fresh post-deployment checks.

OT migration

Account for supplier firmware, maintenance windows, safety constraints, long service lives and limited rollback. Preserve operational continuity and compensating controls.

Proof of migration

BEFORE

Verified implementation and dependency baseline.

CHANGE

Approved artifact, target and execution record.

AFTER

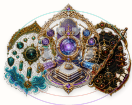
Fresh evidence that the intended control is active.

RESIDUAL

Exceptions, classical dependencies and next review.

A PQC claim is credible when the changed implementation, dependent service and remaining gaps are visible together.





Govern the transition with evidence

A staged program preserves operational control while standards, suppliers and systems evolve - and gives leadership a defensible basis to fund, sequence and verify the next move.

Keep operations safe during a long transition

SOAR can bring supported evidence into an investigation, compare choices through replay or controlled rehearsal, and prepare a bounded action for human approval. Temporary containment may reduce a specific exposure; it does not replace PQC migration or make previously exposed data quantum-safe.

Govern by business unit

Keep scope, permissions, evidence and exceptions separate. Map shared services and interdependencies explicitly.

Measure progress

Report critical-service coverage, freshness, unresolved dependencies, accepted exceptions and verified migrations.

Decide in stages

Expand, narrow, pause or stop from reproducibility, operational effort, control readiness and residual risk.

Cross-product intelligence

Products can stand alone. Joined views require supported adapters, a common review window and explicit asset-service-repository identifiers; similar names do not prove a relationship.

Urgent operating posture

Compress scope to the critical service and highest-consequence exposure. Prepare a reversible compensating control, preserve approval and recovery, then verify both service health and the original condition.

The operating controls

PROVENANCE

Origin, time basis and collection or source boundary.

AUTHORITY

Named owner, permitted target, approval and expiry.

RECOVERY

Rollback condition and accountable operator.

VERIFICATION

Fresh evidence of the intended result and side effects.

The destination is crypto-agility: critical dependencies are known, each change has an owner and every migration result can be rechecked.

