QUANTERIOS WHITEPAPER

quanterios
cryptographic and ai security and governance

EDITION

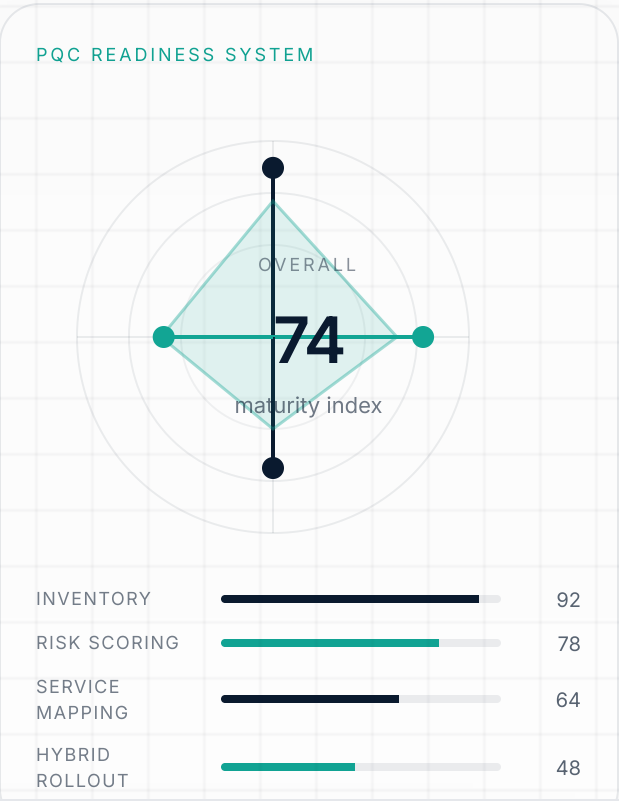
Quanterios Research 01

02 May 2026

OFFICIAL PUBLICATION | WHITEPAPER SERIES

Post-Quantum Cryptography for Regulated Enterprises

A board-to-build playbook for inventory, prioritization, hybrid rollout, and evidence before cryptographic modernization becomes a forced migration.



2030+	5	Hybrid

Cookie preferences

Set how Quanterios handles non-essential storage and measurement.

Necessary storage supports security, language, and core site operation. Analytics and any future marketing technologies stay off until you allow them.

Review cookie settings

EDITORIAL BRIEF

Executive summary

AUDIENCE

CISO, Cryptography Lead, Platform Architect, Regulatory Program Owner

FORMAT

Quanterios Whitepaper

LENGTH

24 pages

Post-quantum cryptography is no longer a research watchlist item for regulated enterprises. It is becoming a board-level modernization program with direct consequences for procurement, architecture, service resilience, and supervisory credibility.

The difficulty is not only choosing new algorithms. The real challenge is knowing where cryptography lives, which business services depend on it, how hybrid rollout should be staged, where exceptions can be tolerated, and what evidence proves the program is moving in a controlled way.

Most programs stall because organizations discover cryptography too late, treat migration as a library swap instead of a service transformation, and cannot connect technical findings to business consequence, change windows, or audit evidence.

This paper lays out a practical operating model for regulated enterprises, from cryptographic inventory and service-level prioritization to migration sequencing, exception management, vendor coordination, and evidence production.

WHAT THIS PAPER GIVES YOU

OPERATING CYCLE

Discover to evidence

WHY THIS MATTERS NOW

— Waiting increases operational drag because supplier and service dependencies keep accumulating.

ISSUE MAP

Contents

WHY THIS PAPER MATTERS

Quanterios whitepapers are designed to be carried into investor meetings, buyer reviews, partner conversations, and internal strategy sessions as

QUESTIONS THE PAPER ANSWERS

- How does PQC become an operating mandate instead of a research topic?

SECTION 01

Why PQC has moved from research topic to operating mandate

ORIENTATION

What changed is not just the science. What changed is the cost of waiting while sensitive data, supplier dependencies, and long-lived services continue to accumulate.

WHY URGENCY IS COMPOUNDING

Research	Planning
Procurement	Modernization

The market has crossed the point where post-quantum cryptography can be treated as a distant roadmap item. Standardization progress, public-sector modernization timelines, vendor pressure, and harvest-now-decrypt-later risk have turned PQC into a planning obligation for enterprise leadership teams.

For regulated organizations, the pressure is sharper because

WHAT CHANGED

- Harvester risk matters most where the sensitivity of data outlives the strength assumptions of current cryptography.

SECTION 02

The five stages of a credible enterprise PQC program

ORIENTATION

Strong programs move through five repeatable stages rather than one giant replacement project.

OPERATING MODEL

OPERATING CYCLE

Discover to evidence

01 Discover cryptography everywhere
02 Score posture and exposure
03 Prioritize by service consequence
04 Roll out hybrid migration waves
05 Prove progress with live evidence

Stage one is discovery: a living record of cryptographic assets, algorithms, implementations, dependencies, certificates, protocols, and service context across cloud, source code, infrastructure, CI/CD,

FIVE STAGES IN PRACTICE

These stages matter because each one produces the inputs for the next. Discovery without posture creates noise.

SECTION 03

Why most enterprise migrations stall before they scale

ORIENTATION

Most stalls are not caused by a lack of cryptography awareness. They are caused by hidden dependencies, fragmented ownership, and weak service-level planning.

WHERE MIGRATIONS STALL

Late discovery
Hidden certificates, appliances, and supplier code

Fragmented ownership
Security, delivery, infra, and compliance see different records

No service map
Findings are not tied to consequence or change windows

No exception logic
Temporary tolerances cannot be reviewed or expired cleanly

Most stalled migrations follow the same pattern. Teams assume they are dealing with a finite library replacement exercise, but quickly discover certificate sprawl, embedded cryptography in supplier

RECURRING STALL PATTERNS

— Unknown certificate and key usage

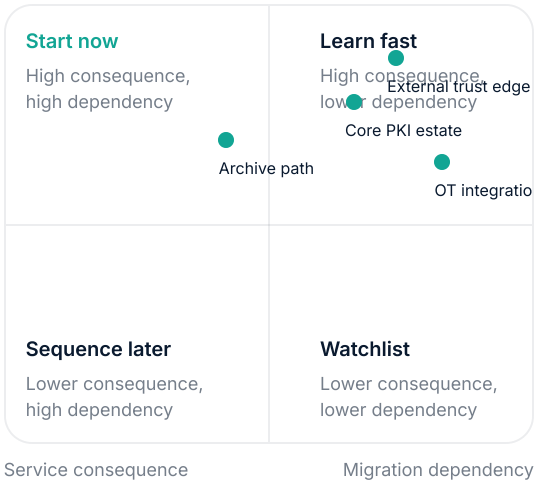
SECTION 04

How regulated enterprises should prioritize first

ORIENTATION

Early prioritization should optimize for consequence, dependency learning, and operational repeatability, not for the prettiest coverage metrics.

FIRST-WAVE PRIORITIZATION



Strong programs do not start by trying to touch every asset at once. They begin by identifying which services combine three factors: long-lived sensitivity, material operational exposure, and realistic migration dependency. That usually pushes priority toward external trust boundaries, critical internal services, certificate-heavy estates, and third-party integrations that are expensive to retrofit late.

Teams should create a first-wave migration queue based on service impact rather than raw asset count. A modest number of high-

FIRST-WAVE DISCIPLINE

- Prioritize by service consequence, not by whichever asset scanner produces the largest list first.
- Use wave one to learn migration patterns, exception needs, and breakage behavior before broad

SECTION 05

What strong governance and evidence actually look like

ORIENTATION

Good governance is not a review deck. It is a repeatable evidence system that can explain decisions, exceptions, deadlines, and residual exposure.

WHAT GOOD EVIDENCE SHOWS

1. Asset and algorithm inventory
2. Owner and service consequence
3. Migration state and exception window
4. Approval history and review cadence
5. Executed change and residual exposure

Good governance does not mean slowing delivery. It means creating a repeatable decision model: what gets prioritized first, which risks are tolerated temporarily, how exceptions are recorded, who signs off on service-level exposure, and what evidence demonstrates progress quarter over quarter.

For regulated enterprises, evidence is not a reporting afterthought. It is the mechanism that makes the program defensible. Leadership needs to see which services remain exposed, audit teams need to see that exceptions are bounded, and supervisors or customers may eventually ask how the organization approached quantum-related modernization risk in a disciplined way.

EVIDENCE REQUIREMENTS

- Evidence should connect cryptographic findings to service owners and approved remediation plans.
- Exceptions should carry explicit owner, rationale, expiry, and follow-up path.
- Quarterly program reviews should be driven from live control data rather

SECTION 06

The Quanterios point of view

ORIENTATION

PQC programs only mature once inventory, service context, orchestration, and proof are treated as one control layer rather than disconnected workstreams.

QUANTERIOS CONTROL LAYER

CBOM discovery
Continuous inventory across code, cloud, CI/CD, and edge

Posture scoring
HNDL risk, deprecated primitives, agility readiness

Migration orchestration
Wave planning, hybrid rollout, exception handling

Evidence production
Control record for executives, audit, and regulators

Quanterios takes the view that regulated enterprises need a cryptographic system of record before they can run a credible PQC program. Inventory, posture, service context, migration sequencing, and evidence should not live in separate disconnected workflows.

That is why Quanterios Crypto is designed around continuous CBOM

CONNECTED SURFACES

PQC migration

Cryptographic asset inventory

CBOM

SECTION 07

The first 90 days of a serious PQC program

ORIENTATION

The first quarter should not be spent trying to finish the migration. It should be spent building the operating discipline that makes the rest of the migration possible.

THE FIRST 90 DAYS

DAYS 1–30
Stand up the control record
Find assets, assign owners, and classify service consequence.

DAYS 31–60
Build the first wave
Model hybrid dependencies, select pilot services, and define exceptions.

DAYS 61–90
Run the first reviews
Show progress by service family and prove change windows are controlled.

In the first 30 days, the priority is to establish the system of record: what data sources feed discovery, how service ownership will be assigned, which business services matter most, and what evidence fields the program will preserve from the beginning. If these foundations are weak, every later dashboard will mislead.

In days 31 through 60, teams should identify the first migration wave and model its dependencies in detail. That means choosing representative services, validating where hybrid operation is possible, naming rollback paths, and documenting which third-party

90-DAY OPERATING GOALS

- Stand up discovery, ownership, consequence tagging, and evidence fields in the first month.
- Use the second month to model one real first-wave queue rather than auditing the entire estate indefinitely.

SECTION 08

Questions leadership and operators should ask now

ORIENTATION

A useful whitepaper should leave the reader with better questions, not only better slogans.

QUESTIONS TO ASK NOW

ENGINEERING

- Where does cryptography live beyond application source?
- Which services break under naive swaps?

PROCUREMENT

- Which vendors expose algorithm assumptions?
- What remediation commitments exist in contracts?

GOVERNANCE

- Who approves temporary exposure?
- What evidence will leadership review each quarter?

Security leaders should ask whether they can describe their top cryptographic dependencies by service family today. If not, they do

LEADERSHIP PROMPTS

The teams that ask these questions early create cleaner

EDITORIAL NOTE

EXECUTIVE DISTILLATION

What strong teams do differently

The strongest PQC programs do not wait for a perfect standards moment or a vendor miracle. They make the estate visible, connect findings to service consequence, and build a migration program that can be reviewed with evidence rather than defended with anecdotes.

That gives leadership two advantages at once: better technical sequencing and a cleaner modernization story for boards, regulators, customers, and counterparties. The earlier the organization establishes that operating discipline, the less likely it is to discover that the true critical path lives in hidden services, opaque supplier commitments, or unmanaged exceptions.

OPERATING SEQUENCE

VISIBLE
Build the control record
Inventory, ownership, service consequence, and deadlines in one place.

SEQUENCED
Run first-wave migration
Prioritize by consequence and learn through hybrid rollout.

PROVABLE
Show the evidence
Turn progress, exceptions, and residual exposure into reviewable proof.

KEY TAKEAWAYS

- Treat PQC as an enterprise operating program, not a procurement or standards note.
- Inventory plus service context is the foundation of every credible migration plan.
- Hybrid rollout should be modeled as a staged service transformation with explicit exception control and evidence.

CLOSING SPREAD

From insight to action

WHAT STRONG TEAMS DO NEXT

- Establish one living cryptographic system of record.
- Choose a first migration wave by service consequence, not raw asset count.
- Model vendor dependencies and exception paths before rollout pressure rises.
- Use live evidence to drive the quarterly program review.

QUANTERIOS OPERATING LAYER

Discovery
Continuous CBOM inventory across code, cloud, CI/CD, and edge.

Posture
HNDL scoring, deprecated primitives, and agility readiness.

Migration
Wave planning, hybrid rollout, and exception control.

Evidence
Review-ready proof for executives, auditors, and regulators.

NEXT STEP

Want to turn PQC strategy into a real migration program?

Quanterios helps regulated enterprises build the cryptographic system of record behind discovery, prioritization, hybrid rollout, and regulator-ready evidence.

Cookie preferences

Set how Quanterios handles non-essential storage and measurement.

Necessary storage supports security, language, and core site operation. Analytics and any future marketing technologies stay off until you allow them.

Review cookie settings