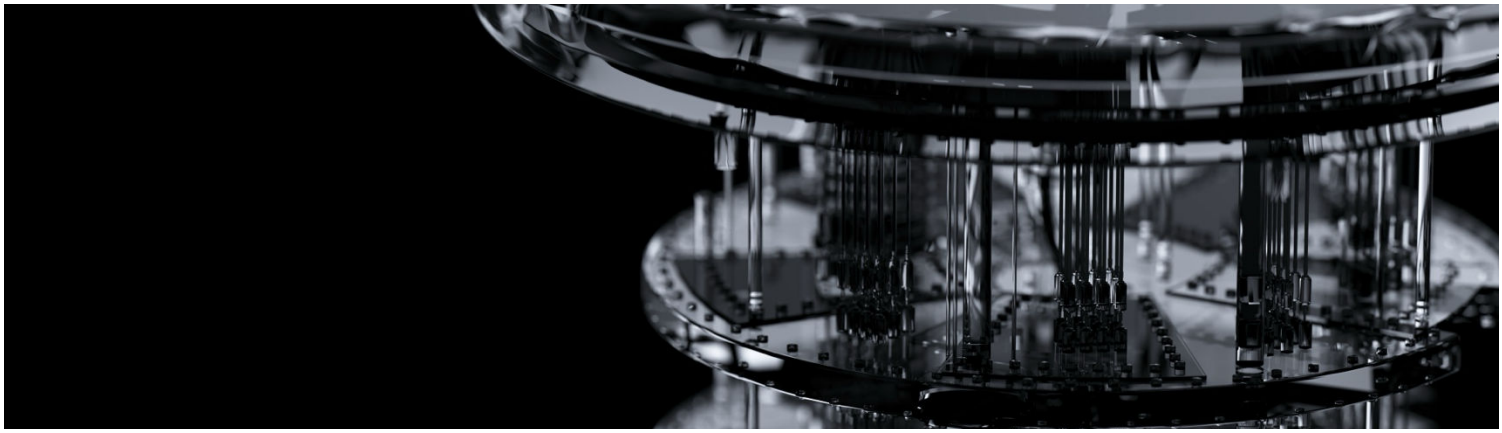
MARCH 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK



From Discovery to Deployment *- The comprehensive, phase-by-phase guide to migrating enterprise cryptography before quantum computers arrive*

Version 1.1 — March 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

PQCFramework.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

© 2026 Marin Ivezic / Applied Quantum. This work is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). You are free to share and adapt this material for any purpose, including commercial use, provided you give appropriate credit to Marin Ivezic and Applied Quantum, link to the license, and indicate any changes made.

License details: https://creativecommons.org/licenses/by/4.0/

DISCLAIMER

This framework is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of March 2026. This landscape evolves rapidly. Readers should verify current status against primary sources (NIST, NSA, ETSI, national agencies, vendor documentation) before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2025–2026. Federal agencies and their contractors should reference the final published version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Intended audience	CISOs, security architects, cryptographic engineers, program managers, risk and compliance officers, vendor/procurement teams

Assumed knowledge	Familiarity with quantum threat fundamentals (HNDL, TNFL, CRQC timelines, NIST PQC standards)
Scope	Industry-agnostic core methodology. Sector-specific adaptations included as summary notes; dedicated sector annexes planned for future publication.

VERSION HISTORY

Version	Date	Changes
1.0	June 2025	Initial publication — 8-phase lifecycle, cross-cutting sections, 5 appendices
1.1	Mar 2026	Reviewed and updated. 40+ updates including: NIST IR 8547 timeline, ML-DSA sizes, CNSA 2.0 milestones, LMS/XMSS status, SSH/TLS details, hybrid jurisdictional nuance. Added: library readiness, FN-DSA/HQC, Confidential Computing, legal risk, Q-by-Q Year 1 plan, dependency chains.

HOW TO CITE THIS FRAMEWORK

Ivezic, M. (2026). The Applied Quantum PQC Migration Framework: A Practitioner's Methodology for Enterprise Post-Quantum Cryptography Migration (Version 1.1). PostQuantum.com / Applied Quantum.

RELATIONSHIP TO OTHER GUIDANCE

This framework is an original methodology developed by Marin Ivezic and Applied Quantum. It is informed by — but not derivative of — the following standards and guidance:

- NIST FIPS 203/204/205 (ML-KEM, ML-DSA, SLH-DSA algorithm standards)
- NIST IR 8547 (Transition to Post-Quantum Cryptography Standards)

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- NIST SP 1800-38 (NCCoE Migration to Post-Quantum Cryptography)
- NIST SP 800-227 (Recommendations for Key-Encapsulation Mechanisms)
- NSA CNSA 2.0 (Commercial National Security Algorithm Suite)
- PQCC Migration Roadmap (Post-Quantum Cryptography Coalition / MITRE)
- Dutch PQC Migration Handbook (AIVD/CWI/TNO, 2nd edition)
- GSMA PQ.01–PQ.03 v2.0 (Post-Quantum Telco Network Task Force)
- ETSI TR 103 619 / TR 104 016 (Migration to Post-Quantum Cryptography)
- PKI Consortium PQCMM (Post-Quantum Cryptography Maturity Model)

Where this framework takes positions that differ from conventional wisdom or other published guidance, those positions are made explicit and defended with evidence. Key differentiators include: the Minimum Viable CBOM model, the risk-driven discovery scoping approach, and the emphasis on vendor governance as the primary external constraint on migration timelines.

ACCOMPANYING RESOURCES

Every aspect of this framework — from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance — has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Quantum Readiness Starting page: https://postquantum.com/quantum-readiness-starting/ — but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com — a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

TABLE OF CONTENTS

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

HOW TO USE THIS FRAMEWORK

This is an executable methodology for enterprise PQC migration — not a whitepaper, not a checklist, not a vendor pitch. It is structured as an 8-phase lifecycle (Phase 0 through Phase 7) with cross-cutting concerns woven throughout. Each phase defines:

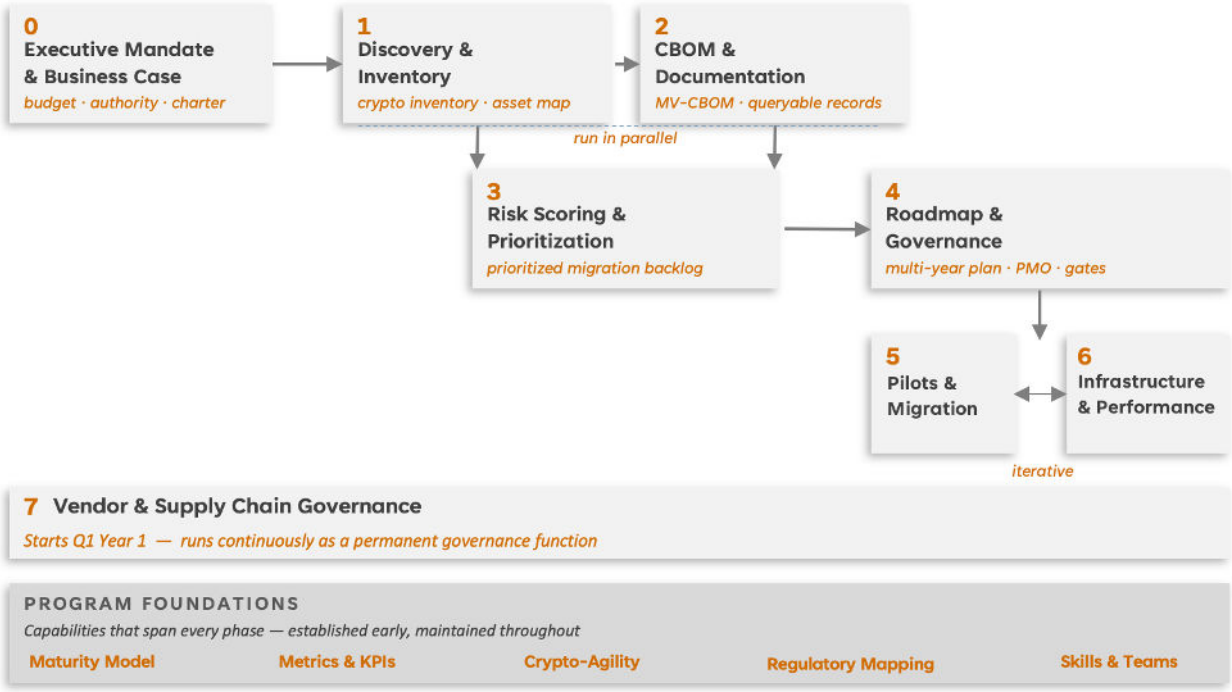
- **Prerequisites** — what must be in place before you start
- **Activities** — what you do, with enough specificity to assign to a team next Monday
- **Decision Points** — where choices branch based on your context
- **Outputs** — what you produce, with quality criteria
- **Interdependencies** — what feeds into and out of this phase
- **Common Failures** — what goes wrong and how to avoid it
- **Maturity Indicators** — how to assess whether you've done this phase well enough to proceed

Organizations should not expect to execute phases sequentially in a clean waterfall. Real programs overlap: you will be running Phase 1 discovery on some systems while executing Phase 5 pilots on others. The phase structure provides a logical dependency order, not a calendar sequence.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

FRAMEWORK ARCHITECTURE AT A GLANCE

Phases are logically sequential but operationally overlapping — real programs run discovery, documentation, pilots, and vendor engagement concurrently.



© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

REGULATORY TIMELINE CONTEXT

This framework is designed to satisfy the following converging deadlines. Note: the table below includes a mix of binding requirements, recommended roadmaps, and planning milestones at varying stages of finalization. Not every date is a legally binding deadline — readers should verify the current status and applicability of each mandate for their specific jurisdiction and sector.

Jurisdiction / Body	Key Milestone	Deadline	Status
NIST IR 8547	Deprecate quantum-vulnerable public-key algorithms (112-bit security)	After 2030	Initial Public Draft (Nov 2024)
NIST IR 8547	Disallow quantum-vulnerable public-key algorithms	After 2035	Initial Public Draft (Nov 2024)
NSA CNSA 2.0	New NSS acquisitions CNSA 2.0 compliant	2027	Binding for NSS
NSA CNSA 2.0	Software/firmware signing uses PQC	2030	Binding for NSS
NSA CNSA 2.0	Networking equipment (VPNs, routers) exclusively uses CNSA 2.0	2030	Binding for NSS
NSA CNSA 2.0	Most NSS (web, cloud, OS, and other platforms) migrated	2033	Binding for NSS
NSA CNSA 2.0	All NSS including custom/legacy systems fully migrated	2035	Binding for NSS
Australia (ASD)	Cease traditional asymmetric crypto in Australian Government systems	2030	Government guidance
NCSC UK	Discovery and planning complete	2028	National guidance

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

NCSC UK	High-priority migration complete	2031	National guidance
NCSC UK	Full migration complete	2035	National guidance
EU Coordinated Roadmap	First steps (awareness, inventories, pilots)	End of 2026	Roadmap for Member States
EU Coordinated Roadmap	High-risk migration complete	End of 2030	Roadmap for Member States
EU Coordinated Roadmap	Medium-risk migration complete	End of 2035	Roadmap for Member States
Government of Canada (CCCS)	Departmental PQC migration plans developed	April 2026	Federal government
Government of Canada (CCCS)	High-priority systems migrated	2031	Federal government
PCI DSS v4.0 Req 12.3.3	Documentation and annual review of cryptographic cipher suites and protocols in use	Required after March 31, 2025	Binding for PCI-scoped entities

The implication: organizations starting now have 4–9 years depending on jurisdiction and system criticality. A credibly planned migration for a large enterprise requires 4–15 years of execution. There is no slack in the schedule.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 0 — EXECUTIVE MANDATE & BUSINESS CASE

PURPOSE

Nothing happens without budget, authority, and organizational commitment. Phase 0 establishes the governance foundation and secures multi-year funding. This is not a formality — it is the single most common failure point. Programs that skip or underinvest in Phase 0 stall within 6–12 months when they hit their first resource conflict or political obstacle.

Phase 0 is also where the program's identity is established. PQC migration is frequently misunderstood as a narrow technology upgrade — a library swap or a certificate rotation project. In reality, it is the largest cryptographic overhaul most organizations will ever undertake, touching every application, every integration, every vendor relationship, and every data store that relies on public-key cryptography. The executive mandate must frame this accurately: this is a multi-year enterprise transformation program, not an IT project. Organizations that frame it as a project get project-level funding and project-level authority, which is insufficient for the scope of work ahead.

Parallelization note

Phase 0 is the only phase that must be substantially complete before others begin — you cannot conduct discovery without budget, tooling authority, and designated staff. However, experienced organizations often run a lightweight "Phase 0.5" concurrently with later Phase 0 activities: while the full business case and governance structure are being finalized, a small technical team can begin preliminary scoping (identifying the top 10–20 critical systems and the top 10 vendor dependencies) to generate early data points that strengthen the business case itself. This creates a virtuous cycle: early technical findings provide the evidence that secures broader executive commitment.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

None — this is the entry point.

Organizational prerequisites

- **Awareness that quantum computing poses a material risk to the organization's cryptographic infrastructure**. This is assumed for this framework's audience. If executive awareness does not yet exist, invest in education first.
- **Access to senior leadership (CISO, CIO, or equivalent) who can sponsor a board-level initiative**. The sponsor must have the organizational standing to secure multi-year budget commitments and cross-functional authority. A mid-level security manager cannot drive this program — it requires someone who can convene business unit leaders, negotiate with procurement, and report to the board.
- **Basic understanding of the organization's regulatory environment and any sector-specific quantum readiness guidance**. At minimum, the team entering Phase 0 should know which regulatory bodies govern their sector, whether any quantum-specific mandates or timelines apply (see the Regulatory Timeline Context table in this framework), and what existing compliance frameworks (PCI DSS, DORA, CMMC, etc.) may intersect with PQC migration.
- **An organizational culture that can sustain long-horizon programs**. This is less a checklist item than a reality check. Organizations that routinely cancel or defund programs after 12–18 months will struggle with PQC migration unless Phase 0 explicitly addresses funding durability. If your organization lacks this muscle, the governance structure designed in this phase must compensate — for example, by embedding PQC migration into an existing enterprise risk management cycle that has established board-level reporting cadence.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

0.1 Frame the Business Case

Structure the executive argument around four "urgency drivers" — not Q-Day predictions, which are speculative, but business pressures that are concrete and current:

1. **Regulatory and compliance deadlines.** Map the organization's specific regulatory exposure to the timeline table above. For financial services: PCI DSS v4.0 Requirement 12.3.3 already requires documentation and annual review of all cryptographic cipher suites and protocols in use, effectively mandating a cryptographic inventory. For organizations with EU operations: NIS2 and DORA create supervisory expectations. For government suppliers: CNSA 2.0 timelines apply to procurement requirements.

2. **Harvest Now, Decrypt Later (HNDL) exposure.** Identify data categories with long confidentiality requirements (10+ years): trade secrets, M&A plans, health records, national security information, long-lived financial instruments, attorney-client privileged communications. Every day these data traverse quantum-vulnerable encryption channels, adversaries can capture and store ciphertext for future decryption. This risk is active now — not contingent on a future quantum computer.

3. **Trust Now, Forge Later (TNFL) exposure.** Identify long-lived digital signatures and trust anchors: PKI root certificates (often 20+ year validity), code-signing keys, firmware signing keys, legal/regulatory document signatures, OT safety certificates. A future quantum computer could forge signatures on these artifacts, undermining trust retroactively.

4. **Client, investor, and insurer expectations.** Board directors face fiduciary duty questions. Institutional investors are incorporating quantum readiness into due diligence. Cyber insurers are beginning to include quantum preparedness in underwriting criteria. Government and enterprise procurement increasingly requires demonstrated quantum readiness.

Decision Point: If your organization holds data with >10-year confidentiality requirements AND operates in a regulated industry, the HNDL argument alone justifies immediate action. If your primary risk is signature integrity (e.g., OT/ICS environments, PKI operators), the TNFL argument drives urgency on different systems.

0.2 Build the Budget Structure

Quantum readiness is not a single project with a single budget line. Structure funding as a program with phased investment:

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Year 1 (Foundation): Inventory and discovery tooling, initial CBOM development, 2–3 hybrid pilots, vendor engagement, policy updates, team training. Illustrative range for a large enterprise: $1.5M–$4M depending on estate complexity and tooling choices — actual costs vary significantly by organization size, sector, and existing tooling maturity.

Years 2–3 (Bulk Migration): Rollout to Tier-1 systems, PKI modernization, key-lifetime reductions, dual-signing pilots, vendor upgrade coordination. This is the most capital-intensive phase.

Years 4–5 (Long Tail and Hardening): Embedded/OT systems, legacy system containment, elimination of compensating controls, crypto-agility maturation.

Key budget strategy: Align PQC migration spending to existing infrastructure refresh cycles (data center refreshes, SD-WAN upgrades, cloud migrations, PKI renewals, vendor contract renewals). This avoids "big-bang" budget spikes and makes quantum readiness an incremental cost on already-planned expenditures rather than a net-new program.

The "umbrella program" strategy: Position quantum readiness as the organizing framework for long-overdue security modernization. Many organizations need to update PKI infrastructure, improve certificate lifecycle management, modernize HSMs, improve asset inventories, and strengthen vendor governance regardless of quantum risk. Quantum readiness provides the urgency and the budget justification to do all of this under one program umbrella, with PQC migration as the binding thread.

Align with innovation, R&D, and digitization budgets. Quantum readiness has significant overlap with other strategic investment categories. If the organization has an innovation or R&D budget for quantum technology exploration (quantum computing applications, quantum sensing, quantum networking), the security workstream should be funded alongside — and ideally integrated with — that quantum exploration program. The upskilling requirements overlap substantially: teams learning about quantum computing for business applications also need to understand quantum risk. Similarly, digital transformation and IT modernization programs (cloud migration, zero trust architecture, DevSecOps maturity) share infrastructure and tooling with PQC migration. Position PQC as a mandatory security track within these broader programs rather than competing for separate budget allocation. This approach also ensures that digitization initiatives do not inadvertently create new quantum-vulnerable attack surface even as they modernize the estate.

0.2b Build the Business Case — Additional Benefit Arguments

Beyond the four urgency drivers, several additional arguments strengthen the business case:

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Regulatory trust and approval acceleration. In regulated industries (financial services, healthcare, telecoms, energy), organizations frequently require regulatory approval before launching new products, services, or technology platforms. Regulators are more likely to approve innovative initiatives from organizations that demonstrate strong security fundamentals. An organization that can present a mature quantum readiness posture — with a documented CBOM, risk assessment, and migration roadmap — signals to regulators that it manages technology risk proactively. This can strengthen the organization's credibility in regulatory engagement and may reduce friction during supervisory review of new products and services, depending on sector, jurisdiction, and the regulator involved. In financial services, for example, demonstrating quantum readiness during a new product approval process differentiates the organization from competitors who have not addressed the risk, potentially making the difference between approval and extended review cycles.

Immediate security value from cryptographic inventory. One of the most compelling near-term benefits of PQC migration is that it produces tangible security improvements from day one — before any PQC algorithm is deployed. A quantum-vulnerability-focused cryptographic inventory inevitably also surfaces classically vulnerable cryptography: deprecated TLS versions (TLS 1.0/1.1 still in production), weak key sizes (RSA-1024, DH-1024), insecure cipher suites (RC4, 3DES, export ciphers), expired or misconfigured certificates, hardcoded keys in application code, unpatched cryptographic library versions with known CVEs, and misconfigured protocols allowing downgrade attacks. These are real, present-day vulnerabilities that can be remediated immediately. Cryptographic inventories routinely uncover classically vulnerable configurations that had not been centrally tracked or prioritized for remediation — deprecated protocols, weak keys, expired certificates, and misconfigured settings that represent real, present-day risk. This makes the Phase 1 investment self-funding from a security perspective — it pays for itself in reduced classical risk before the quantum migration even begins. Frame this in the budget request: "The inventory alone will identify and enable remediation of current cryptographic vulnerabilities, reducing our classical attack surface while simultaneously preparing for quantum risk."

Competitive differentiation and market access. By the late 2020s, demonstrating quantum resilience will become a market signal of forward-thinking security. Government and enterprise procurement increasingly requires demonstrated quantum readiness. Organizations that can respond to "Are you quantum-ready?" with documented evidence gain competitive advantage in sales cycles, particularly in financial services, healthcare, defense, and critical infrastructure sectors.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

0.3 Establish Governance Structure

Role	Responsibility	Reporting
Executive Sponsor (CISO or CIO)	Visible owner; clears roadblocks; briefs board quarterly	Board / Risk Committee
Steering Committee (SteerCo)	Cross-functional: Security, Enterprise Architecture, AppDev, Infrastructure/NetSec, PKI/Identity, Compliance/Legal, Procurement, Business Unit reps	Monthly to Sponsor
Quantum Readiness Program Manager (QRPM)	Day-to-day leader; runs plan, risk log, KPIs; coordinates workstreams	Weekly to SteerCo lead
Workstream Leads (one per domain)	Execute phase activities within their domain	Weekly to QRPM

Workstream structure (8 streams):

1. Inventory & Discovery (Crypto-BOM ownership)
2. Network & TLS/VPN (hybrid rollouts)
3. PKI & Code Signing (roots, issuers, toolchains)
4. Applications & Platforms (libraries, service mesh, cloud)
5. Embedded/IoT/OT (gateways, compensating controls)
6. Policy/Compliance/Procurement (standards, clauses)
7. Vendor Orchestration (roadmaps, SLAs)
8. Education & Change Management (training, comms)

Decision cadence:

- Weekly PMO: track milestones, blockers, vendor responses
- Monthly SteerCo: approve roadmap changes, funding asks, target dates, risk acceptance
- Quarterly Board/Risk Committee: KPIs, exceptions, budget status

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

0.4 Draft the Program Charter

A one-page charter document covering:

- **Purpose:** Quantum-safe migration and crypto-agility
- **Scope:** TLS/VPN, PKI/code-signing, applications/platforms, embedded/OT, policy/procurement, vendors, training
- **Success criteria:** Stop new HNDL exposure; protect long-lived trust anchors; meet 2030/2035 regulatory timelines; embed crypto-agility as organizational capability
- **Cadence:** Weekly PMO; monthly SteerCo; quarterly board
- **Escalation path:** Sponsor decides on funding/dates; risk acceptance decisions are documented and auditable

0.5 Conduct Initial Scoping Assessment

Before launching full discovery, perform a rapid (2–4 week) scoping assessment to establish program boundaries:

1. Identify the top 20 revenue-generating or mission-critical systems
2. For each, determine: primary cryptographic protocols in use, data sensitivity classification, number of dependent systems, vendor ownership vs. internal control
3. Estimate the approximate size of the cryptographic estate (number of TLS endpoints, certificates, VPN tunnels, HSM-protected keys, code-signing pipelines)
4. Identify the 5–10 vendors whose PQC readiness will most constrain the migration timeline

This scoping assessment becomes the input for Phase 1 prioritization and helps calibrate Year 1 budget and staffing.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Approved program charter	Signed by executive sponsor; reviewed by SteerCo
Multi-year budget commitment	Minimum 3-year funding approved; aligned to refresh cycles
Governance structure	SteerCo membership confirmed; QRPM appointed; meeting cadence established
Initial scoping assessment	Top 20 systems identified; estate size estimated; critical vendor dependencies mapped
Board briefing deck	Delivered at board/risk committee level; documented in minutes

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 0 is the framework entry point with no dependency on prior phases.

Feeds into

- **Phase 1** — The scoping assessment (Activity 0.5) determines discovery priorities and initial system targeting. The approved budget enables tool procurement and team staffing. The governance structure provides the authority needed to gain access to systems, repositories, and network infrastructure.
- **Phase 4** — The budget structure and multi-year commitment set the financial constraints within which the roadmap must be built. The governance model (SteerCo, RACI, escalation paths) becomes the operating framework for roadmap governance.
- **Phase 7** — The critical vendor list from the scoping assessment enables vendor engagement to begin in Q1 Year 1, before CBOM or risk scoring is complete. Procurement and legal team engagement initiated in Phase 0 provides the contracting capability needed for Phase 7.

Runs in parallel with

Late-stage Phase 0 activities (governance finalization, detailed budget approval) can overlap with early Phase 1 discovery on the highest-priority systems, as described in the Purpose section. Early technical findings from this preliminary discovery strengthen the business case — creating a virtuous cycle between Phase 0 justification and Phase 1 evidence.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **"Innovation project" framing.** Treating PQC migration as an R&D initiative or skunkworks project instead of a funded, governed program. This guarantees it will be deprioritized when competing for resources with operational imperatives.
- **Single-year budget.** Securing one year of funding and hoping to "show results" to justify the next year. PQC migration is a 4–15 year program. Without multi-year commitment, teams cannot plan realistically or retain specialized talent.
- **Missing business unit representation on SteerCo.** The migration will touch every application, every integration, every vendor relationship. Without business unit buy-in at the governance level, workstream leads face constant political resistance.
- **Delegating to vendors.** Assuming "our vendors will sort this out" and therefore not needing an internal program. This is the single most dangerous misconception. Vendors will update their products on their own timelines, optimizing for their own priorities. Without an internal program driving requirements, tracking commitments, and testing deployments, the organization has no control over its migration timeline.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0 — Unaware	No executive awareness of quantum risk; no budget discussion
Level 1 — Aware	Quantum risk acknowledged; no formal program
Level 2 — Initiated	Charter approved; QRPM appointed; Year 1 budget secured
Level 3 — Established	Multi-year budget committed; SteerCo operational; scoping assessment complete
Level 4 — Optimized	Program integrated into enterprise risk register; quantum risk reported to board quarterly alongside other strategic risks

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 1 — DISCOVERY & INVENTORY

PURPOSE

Build a comprehensive, continuously updated inventory of all cryptographic usage across IT, OT, cloud, IoT, and third-party systems. This is the foundational activity upon which every subsequent phase depends. You cannot migrate what you cannot see, and you cannot prioritize what you have not inventoried.

Major organizations should plan for this phase to take 12–24 months of dedicated team effort. The situation is further complicated by tool vendors who may imply that their products provide a complete solution. No tool provides 100% discovery on its own. A holistic approach combining automated tools, manual audits, and continuous monitoring is necessary.

Discovery is the phase where most organizations are currently stuck — not because the task is conceptually difficult, but because it exposes how little most enterprises actually know about their own cryptographic estate. The asset discovery problem that underpins cryptographic inventory is itself a longstanding IT governance gap: CMDBs are incomplete, shadow IT proliferates, cloud resources spin up without central oversight, and OT environments often have no digital inventory at all. Phase 1 must confront this honestly. Organizations that treat cryptographic discovery as an isolated exercise — separate from the broader challenge of knowing what they own and operate — will produce inventories that are incomplete from day one.

Parallelization note

Phase 1 runs in parallel with Phase 2 from an early stage: the CBOM data structure should be defined before large-scale discovery begins, so that inventory data is collected in a format that populates the CBOM directly rather than requiring later reformatting. Phase 1 also begins to generate inputs for Phase 7 (vendor dependency data) and Phase 3 (the first risk-relevant metadata). In mature programs, Phase 1 never truly ends — it transitions from a project-mode "initial discovery" into a permanent operational capability (continuous discovery) that feeds the CBOM and risk scoring processes

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

indefinitely. Organizations should plan staffing accordingly: the discovery team is not a temporary project team, it is a permanent function.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 0 outputs: approved charter, budget, governance structure, and initial scoping assessment**. The scoping assessment from Phase 0 is particularly important — it identifies the top 20–50 systems by business criticality that form the starting scope for risk-driven discovery (Activity 1.0). Without this scoping input, discovery teams default to either "boil the ocean" (try to scan everything simultaneously) or "path of least resistance" (scan whatever is easiest), neither of which produces actionable results on a useful timeline.
- **Designated workstream lead for Inventory & Discovery**. This should be someone with cross-functional access and technical credibility — typically a senior security architect or infrastructure lead. They will need to negotiate access to systems, repositories, and network segments across business units that may not initially see PQC migration as their problem.

Organizational prerequisites

- **Access to network monitoring infrastructure, code repositories, configuration management databases (CMDBs), and certificate management systems**. In practice, gaining this access is often the first political test of the Phase 0 mandate. If the discovery team cannot get read access to network taps, source code repositories, cloud account configurations, and certificate inventories, the executive sponsor needs to intervene early. Discovery that is blocked by access politics produces coverage gaps that compound through every subsequent phase.
- **At least a preliminary asset inventory or architecture documentation**. Perfect asset data is not required — if it were, most organizations could never start. But the team needs some baseline understanding of the IT and OT estate: major application platforms, network segments, data centers, cloud accounts, OT zones. If this baseline does not exist, Phase 1 must begin with an asset discovery workstream running in parallel with cryptographic discovery, and the program plan should account for the additional time this requires.
- **Budget for cryptographic discovery tooling**. Automated discovery tools (network scanners, code analyzers, certificate crawlers) are not optional — manual-only discovery is unreliable and unscalable. Tool procurement and deployment lead times should be factored into the Phase 1 timeline. Organizations that defer tool selection until after Phase 1 "starts" lose 2–3 months to procurement and deployment before any meaningful discovery occurs.
- **Cooperation agreements with OT/ICS teams (if applicable)**. OT environments require different discovery approaches, different tools, and different risk tolerances. Scanning an OT network with IT-grade tools can cause operational disruptions. The

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OT team must be engaged before any discovery activities touch industrial environments — ideally during Phase 0 scoping, but no later than the start of Phase 1.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

1.0 Risk-Driven Scoping — Decide What to Inventory First

Before launching broad discovery, apply an 80/20 prioritization to determine where to focus initial effort. Attempting to discover everything simultaneously is the most common cause of inventory paralysis. The architecture-first approach (aligned with the Minimum Viable CBOM model in Phase 2) concentrates initial discovery where risk concentrates, delivering an actionable inventory quickly, then expanding systematically to comprehensive coverage.

Step 1 — Identify Tier-1 systems using existing organizational knowledge. You do not need a cryptographic inventory to know which systems matter most. Use existing sources — revenue data, business impact assessments, regulatory scope documents, incident history, architecture diagrams — to identify the top 20–50 systems by business criticality.

Step 2 — Classify by exposure type. For those Tier-1 systems, rapidly classify:

- Internet-exposed flows where adversaries can easily harvest encrypted traffic (external TLS, partner VPNs, email gateways) — these face immediate HNDL risk
- Long-lived secrecy data where the confidentiality requirement exceeds 10 years (health records, trade secrets, financial instruments, legal records) — these have the highest HNDL value
- Long-lived trust anchors where signature validity extends 5+ years (PKI roots, code-signing keys, firmware signing) — these face TNFL risk

Step 3 — Assign discovery priority tiers.

- **Discovery Priority A:** Internet-exposed + handles long-lived secrecy data or trust anchors → Discover these first (target: 30–60 days)
- **Discovery Priority B:** Internal Tier-1 systems with significant data sensitivity → Discover next (target: 60–120 days)
- **Discovery Priority C:** Everything else → Discover on an ongoing basis (target: 6–12 months)

This approach delivers 70–80% of risk coverage with 20–30% of total discovery effort. You will identify the highest-priority migration targets quickly while comprehensive discovery continues in the background. The initial discovery output (Priority A systems) is sufficient to begin Phase 2 CBOM population and Phase 3 risk scoring on the most critical systems, while the broader inventory catches up.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

1.1 Establish Three Parallel Inventory Tracks

Quantum readiness requires integrated discovery across three domains, each with distinct methodologies but deeply interdependent results:

Track A — Cryptographic Inventory: Identifies and documents all uses of cryptography — algorithms, key sizes, protocols, libraries, certificate chains, and key lifetimes. This is the primary PQC-specific deliverable.

Track B — Sensitive Data Discovery and Classification: Identifies, catalogs, and classifies all sensitive data by confidentiality requirements and retention periods. This determines which cryptographic protections have the highest HNDL urgency.

Track C — Systems and Assets Inventory: Catalogs all hardware and software assets, their criticality classifications, vendor ownership, and lifecycle status. This determines migration feasibility and sequencing.

These three tracks must be coordinated through a single governance structure, even if executed by different teams using different tools. The intersection of all three — "this system (Track C) protects this sensitive data (Track B) using this vulnerable algorithm (Track A)" — is what enables defensible prioritization in Phase 3.

1.2 Deploy Cryptographic Discovery — Layered Approach

No single discovery technique covers all cryptographic usage. Deploy a combination:

Layer 1 — Network Traffic Analysis (Passive) Deploy passive monitoring on network taps or SPAN ports to capture TLS/SSH/IPsec handshakes and extract negotiated cipher suites, certificate chains, key sizes, and protocol versions. This reveals what is actually negotiated in production, not what is configured.

Coverage: External-facing TLS, internal east-west TLS/mTLS, VPN tunnels, SSH sessions. Limitation: Cannot see encrypted payloads, application-layer cryptography, or data at rest.

Layer 2 — Static Code Analysis Scan source code repositories for cryptographic API calls, hardcoded algorithms, key generation patterns, and library imports. Target both first-party code and third-party dependencies.

Coverage: Application-layer cryptography, embedded algorithm choices, library dependencies. Limitation: Cannot detect runtime behavior, dynamically loaded crypto, or third-party binaries without source.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Layer 3 — Configuration and Certificate Scanning Enumerate all TLS certificates from certificate management systems and CT logs. Scan network device configurations (load balancers, firewalls, VPN concentrators, proxies) for cipher suite configurations. Query cloud provider APIs for KMS key metadata, managed certificate configurations, and encryption-at-rest settings.

Coverage: Certificate inventory, configured (vs. negotiated) cipher suites, cloud encryption settings. Limitation: Shows configured policy, not actual runtime negotiation.

Layer 4 — Runtime and Binary Analysis For systems without source code access (vendor appliances, legacy binaries, embedded firmware), use runtime instrumentation, binary analysis, or memory dump analysis to identify cryptographic operations.

Coverage: Vendor black-box systems, legacy applications, embedded devices. Limitation: Requires specialized skills; may not be feasible for all systems.

Layer 5 — Manual Investigation Interview application owners, review architecture documentation, examine vendor security documentation, and audit HSM/KMS usage logs. This catches cryptographic usage that automated tools miss: custom protocols, proprietary encryption, embedded hardware crypto, and undocumented integrations.

Coverage: Everything automated tools miss. Limitation: Labor-intensive; dependent on institutional knowledge.

Decision Point — Tool Selection:

The cryptographic discovery tooling market is evolving rapidly. Rather than selecting based on a static vendor list, evaluate tools across the following capability categories. An effective discovery program requires coverage across multiple categories, as no single tool covers all of them:

Category 1 — Dedicated Cryptographic Discovery Platforms. Purpose-built tools that combine multiple discovery methods (network monitoring, code scanning, configuration analysis) into an integrated platform with CBOM output. These platforms are designed specifically for PQC readiness and provide the most quantum-relevant output. The vendor landscape includes established security companies (such as SandboxAQ, IBM, Keyfactor — which acquired both InfoSec Global and CipherInsights — CryptoNext Security, and Palo Alto Networks) as well as emerging specialists. This category is evolving quickly — new entrants and capability expansions appear regularly.

Category 2 — Network Traffic Analysis and Protocol Inspection. Tools that passively capture and analyze TLS/SSH/IPsec handshakes to determine negotiated cipher suites, certificate chains, and protocol versions. Some dedicated cryptographic platforms include

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

this capability; alternatively, network security monitoring tools and TLS inspection appliances can be repurposed.

Category 3 — Static Code Analysis (SAST) with Cryptographic Detection. Tools that scan source code for cryptographic API calls, hardcoded algorithms, key generation patterns, and library imports. Some general-purpose SAST tools can be configured with custom rules for cryptographic detection; dedicated crypto-focused scanners provide more targeted results.

Category 4 — Software Composition Analysis (SCA) and SBOM Generation. Tools that enumerate third-party library dependencies and generate Software Bills of Materials. When combined with cryptographic vulnerability databases, SCA output reveals which libraries contain quantum-vulnerable cryptographic implementations and which applications depend on them.

Category 5 — Certificate and PKI Discovery. Tools that enumerate all TLS/X.509 certificates across the estate, including internal CA-issued certificates, cloud-managed certificates, and CT log monitoring for external certificates. Certificate management platforms and PKI vendors typically provide this capability.

Category 6 — Cloud Security Posture Management (CSPM). Tools that query cloud provider APIs to enumerate encryption configurations, KMS key metadata, managed certificate settings, and storage encryption status across multi-cloud environments.

Category 7 — Binary Analysis and Reverse Engineering. Specialized tools for analyzing compiled binaries and firmware to detect cryptographic operations in vendor products where source code is unavailable. Also includes runtime instrumentation and memory analysis tools. This is the most specialized category and is typically needed only for Layer 4 (embedded/third-party) discovery.

Category 8 — Extracting Cryptographic Metadata from Existing Security Tools. Some organizations can extract significant cryptographic intelligence from security tools already deployed — SIEM logs (TLS handshake data), vulnerability scanners (crypto-related CVEs), endpoint protection platforms (library version data), and network monitoring solutions (protocol version data). This approach avoids deploying new tools entirely for initial discovery and can provide rapid baseline coverage.

For a comprehensive and current analysis of specific vendors within these categories, including capability comparisons and selection guidance, see "Cryptographic Inventory Vendors and Methodologies" on PostQuantum.com (https://postquantum.com/post-quantum/cryptographic-inventory-vendors/). The vendor landscape evolves rapidly; specific product capabilities and vendor positioning may change significantly between publication cycles.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Recommendation: Deploy tools from at least Categories 1–2 for broad automated coverage AND supplement with Category 7/8 approaches for difficult-to-reach systems AND conduct manual investigation (Layer 5) for the top 20 critical systems identified in Phase 0 scoping. No tool alone achieves completeness. Prioritize tools that produce output in CycloneDX CBOM format or that integrate with your selected CBOM tooling from Phase 2.

1.3 Map the Cryptographic Estate

For every cryptographic instance discovered, record:

Field	Description	Example
System/Asset ID	Unique identifier, linked to CMDB	APP-0142
Cryptographic Function	What the crypto does	Key exchange, signing, encryption at rest
Algorithm	Specific algorithm in use	RSA-2048, ECDHE-P256, AES-256-GCM
Key Size	Key length in bits	2048, 256, 384
Protocol	Transport/application protocol	TLS 1.2, SSH 2.0, IPsec IKEv2
Library/Implementation	What provides the crypto	OpenSSL 3.0.12, BoringSSL, Java 17 JCA
Certificate Details	Issuer, validity, chain depth	DigiCert G2, expires 2025-11-01, chain depth 3
Key Lifetime	How long keys persist	Session (ephemeral), 1 year, 20 years (root CA)
Data Sensitivity	Classification of protected data	Confidential, Restricted, Public
Quantum Vulnerability	Vulnerable to Shor, Grover, or neither	Shor (RSA key exchange), not applicable (AES-256)

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Owner	Responsible team/individual	Platform Engineering / J. Smith
Vendor Dependency	Whether migration requires vendor action	Yes — Vendor X controls firmware
Control Posture	Whether organization controls both endpoints	Full control / Partial / No control

1.4 Address the Asset Discovery Problem

Cryptographic inventory depends on knowing what assets exist. Most organizations significantly underestimate their cryptographic footprint. A typical enterprise assumes it has dozens of TLS endpoints; discovery reveals hundreds. RSA is assumed to be only in web servers — it is actually in VPN concentrators, email gateways, IoT devices, backup systems, and embedded firmware.

Why asset discovery is a prerequisite, not an afterthought. You cannot perform a cryptographic scan on a system you do not know exists. The asset discovery problem is the dirty secret that underpins the entire quantum readiness program. Organizations frequently discover during Phase 1 that their existing asset registers are significantly incomplete — particularly for cloud resources, developer-provisioned services, and OT/IoT devices. This is not a quantum-specific problem, but quantum readiness forces organizations to confront it because the consequences of missing assets are more severe (a single undiscovered, unmitigated cryptographic endpoint is a potential quantum-era breach vector).

Comprehensive asset discovery sources — go beyond the CMDB:

The CMDB is rarely complete or current. Supplement it with every available data source:

1. **Configuration Management Database (CMDB).** The starting point, but not the ending point. CMDBs are often stale, incomplete, and biased toward officially provisioned infrastructure. Use as a baseline, then validate and extend.
2. **IT Asset Management (ITAM) databases.** Organizations often maintain separate asset management systems from their CMDB, particularly for hardware lifecycle tracking, software licensing, and financial asset registers. These may capture assets the CMDB misses, especially hardware that was procured but not formally onboarded into configuration management.
3. **Procurement and purchasing records.** Procurement systems (purchase orders, invoices, receiving records) provide a historical trail of every hardware and software

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

acquisition. Cross-referencing procurement data against CMDB and ITAM records reveals assets that were purchased but never formally registered — a surprisingly common occurrence, especially for departmental purchases, project-specific hardware, and lab/test equipment.

4. **Cloud management consoles and APIs.** Cloud estates (AWS, Azure, GCP, and other providers) must be queried directly through their APIs and management consoles. Cloud resources are frequently provisioned outside of traditional CMDB workflows, especially in organizations with decentralized cloud access. Use cloud security posture management (CSPM) tools or native cloud inventory services (AWS Config, Azure Resource Graph, GCP Cloud Asset Inventory) to enumerate all cloud resources, including those in non-production accounts that may still process real data.

5. **Network scanning and traffic analysis.** Active network scanning (Nmap, Shodan for external exposure, asset discovery scanners) and passive traffic analysis (NetFlow, DNS query logs, DHCP logs) reveal devices actively communicating on the network that may not appear in any register. This is particularly important for discovering rogue devices, shadow IT, and IoT endpoints.

6. **Certificate Transparency (CT) logs.** For externally visible TLS certificates, CT logs provide a comprehensive record of every certificate issued for the organization's domains. This reveals subdomains and services the organization may not have formally registered.

7. **DNS zone files and records.** Internal and external DNS records reveal hostnames and services that may not appear in asset registers. Stale DNS records can also point to decommissioned but still-reachable services.

8. **Physical walkthroughs and site surveys.** For organizations with significant OT, manufacturing, or physical infrastructure, physical walkthroughs of data centers, control rooms, factory floors, building management system closets, and network distribution rooms are essential. Physical inspection frequently reveals connected devices — cameras, sensors, building management controllers, access control panels, legacy terminals, embedded systems — that do not appear in any IT asset register because they were provisioned by facilities management, building owners, or OT teams operating independently from IT. For OT-heavy organizations (utilities, manufacturing, oil and gas, transportation), physical walkthroughs are not optional — they are the only reliable way to discover the full embedded device population.

9. **Service desk and incident records.** Tickets referencing systems that do not appear in the CMDB indicate unregistered assets. Incident response records may reference systems encountered during investigations that were previously unknown.

10. **Third-party and vendor-managed systems.** Many organizations host vendor-managed systems (managed security services, outsourced applications, co-located equipment) that do not appear in internal asset registers because the vendor maintains them. These systems still process organizational data and use cryptographic protocols that are in scope for quantum readiness.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

11. **Mergers and acquisitions history.** Acquired entities frequently bring entire technology estates that were never fully integrated into the acquirer's CMDB. Post-M&A environments are notorious for hidden systems, particularly legacy infrastructure from the acquired organization that was "going to be decommissioned" but never was.

Decision Point: If your organization cannot produce a reasonably complete asset inventory (>80% coverage of IT systems, >60% of OT systems), you have a foundational problem that must be addressed before or in parallel with cryptographic discovery. Consider whether the quantum readiness program should include an asset discovery workstream, or whether it should be a prerequisite funded separately. In practice, the quantum readiness program often becomes the forcing function that finally drives asset inventory completeness — this is another example of quantum readiness producing immediate security value beyond quantum-specific risk.

1.5 Integrate with Existing Data Sources

Do not build the cryptographic inventory from scratch in isolation. The organization already possesses significant relevant data across multiple systems. Integrating with these sources saves effort, improves accuracy, and ensures the cryptographic inventory inherits existing business context that would otherwise need to be re-gathered:

- **CMDB:** Asset ownership, lifecycle status, criticality classification, configuration baselines, relationships between components
- **IT Asset Management (ITAM) databases:** Hardware models, firmware versions, software licenses, asset lifecycle stage (active, end-of-life, decommissioned-but-still-running)
- **Business Impact Assessments (BIAs):** Criticality classifications, recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime. BIAs are particularly valuable for Phase 3 risk scoring because they provide pre-existing, business-validated criticality ratings that do not need to be re-derived. If a system is classified as "Critical" in the organization's BIA, that classification should flow directly into the quantum risk scoring model rather than being re-assessed independently
- **Data classification registers:** If the organization has already classified data by sensitivity (as many regulated organizations have), this feeds directly into HNDL risk scoring without re-doing data discovery from scratch
- **Certificate Management Systems:** Certificate inventory, expiry dates, issuer relationships, certificate chain structure, renewal history

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **SBOM (Software Bill of Materials):** Library versions, dependency trees, known vulnerabilities in dependencies
- **Vulnerability Management:** Known CVEs in cryptographic libraries; historical vulnerability scan data showing which systems have had crypto-related findings
- **Cloud Security Posture Management (CSPM):** Cloud encryption configurations, KMS key policies, managed certificate inventory across multi-cloud
- **Network Security Monitoring:** Traffic flows, protocol negotiations, connection metadata
- **Enterprise Architecture repositories:** Application portfolio management databases, technology reference architectures, integration maps showing system-to-system connections
- **Procurement systems:** Vendor product catalogs with version information, contract records showing which vendor products are in use, license entitlements
- **Service catalogs and API registries:** Published APIs and services with their protocol and authentication requirements
- **Identity and access management (IAM) systems:** Authentication method inventory (which systems use certificate-based auth, which use SAML/OIDC with crypto dependencies)
- **Backup and disaster recovery systems:** Encryption-at-rest configurations for backup infrastructure; key management for backup encryption

The more existing data sources you integrate, the faster and more accurate the cryptographic inventory becomes. Each source fills a different gap and provides different business context that enriches the CBOM and accelerates Phase 3 risk scoring.

1.6 Establish Continuous Discovery

The cryptographic inventory is a living data set, not a one-time exercise. Cryptographic posture changes constantly — new applications are deployed, libraries are updated, certificates are issued and rotated, vendors release firmware updates, cloud configurations change, and shadow IT continues to appear. An inventory that is not continuously maintained begins to decay within weeks and becomes dangerously unreliable within months.

Continuous discovery is also a prerequisite for crypto-agility (the end-state goal described in the Cross-Cutting section). An organization that cannot maintain current visibility into its cryptographic posture cannot claim to be crypto-agile, because it cannot

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

verify that algorithm changes have been applied or detect when systems drift from policy.

1.6.1 CI/CD Pipeline Integration

Integrate cryptographic scanning into the software development and deployment pipeline so that every new deployment is automatically assessed for cryptographic impact:

- **Pre-commit / code review gates:** SAST rules that flag new introductions of quantum-vulnerable cryptographic API calls (e.g., direct RSA key generation, ECDH without hybrid wrapping, deprecated cipher suite configuration). These gates should not block development in early program phases but should generate warnings that feed into the CBOM. As the program matures, consider making quantum-vulnerable introductions a build-break for Tier-1 systems.
- **Dependency scanning in build pipelines:** SCA tools that flag when a dependency update introduces or changes cryptographic library versions. When a library version change alters the set of available algorithms, this should trigger a CBOM review.
- **Container image scanning:** For containerized deployments, scan images for cryptographic libraries and configurations. Container orchestration platforms (Kubernetes) should have admission controllers or policy engines that can flag containers without compliant cryptographic configurations.
- **Infrastructure-as-Code (IaC) scanning:** For cloud-native organizations, scan Terraform, CloudFormation, Pulumi, and similar IaC templates for cryptographic configuration (TLS policies, encryption-at-rest settings, KMS key types). Block or flag IaC deployments that create resources with quantum-vulnerable-only encryption.
- **CBOM auto-generation on deployment:** Each production deployment should automatically generate or update CBOM entries for the deployed component. This can be achieved through integration between CI/CD metadata (component name, version, deployment target) and the CBOM system.

1.6.2 Passive Network Monitoring (Continuous)

Maintain ongoing passive monitoring of network traffic to capture cryptographic protocol negotiations in production:

- Deploy network taps or SPAN port monitoring at key network aggregation points (data center borders, cloud transit gateways, VPN concentrators, internet edge).
- Configure monitoring to capture TLS ClientHello/ServerHello messages, SSH key exchange, IPsec IKE negotiations — extracting negotiated cipher suites, protocol versions, certificate chains, and key sizes.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- Establish baselines for "normal" cryptographic behavior and alert on deviations: unexpected use of deprecated algorithms, new TLS endpoints appearing that were not in the CBOM, certificate chain changes, protocol downgrades.
- For organizations with dedicated cryptographic discovery platforms (Category 1 tools from Section 1.2), many of these platforms provide continuous passive monitoring as a built-in capability.

1.6.3 Change Management Integration

Make cryptographic impact assessment a standard component of the change management process:

- Add a "Cryptographic Impact" field to change advisory board (CAB) submission templates. Every change request should answer: "Does this change introduce, modify, or remove any cryptographic component? Does it affect algorithm selection, key material, certificate chain, or cryptographic library version?"
- For changes that do affect cryptographic components, require CBOM update as a condition of change approval and post-implementation review.
- Use change management tools (ServiceNow, Jira Service Management, etc.) to automatically tag cryptography-relevant changes and route them to the Inventory & Discovery workstream for CBOM reconciliation.
- Integrate inventory updates into the change management workflow so that asset tag changes, new deployments, decommissioning events, and configuration changes are all reflected in the cryptographic inventory promptly.

1.6.4 Scheduled Full-Estate Rescans

Even with CI/CD integration, passive monitoring, and change management integration, drift will occur. Schedule periodic full-estate rescans to catch what continuous mechanisms miss:

- **Quarterly:** Full network scan of all known subnets to detect new endpoints, changed configurations, and certificate expirations. Reconcile results against the CBOM; flag discrepancies for investigation.
- **Semi-annually:** Deep scan including code repository sweeps, cloud configuration audits, and HSM/KMS audit log reviews. This is particularly important for catching gradual drift in application-layer cryptography that passive network monitoring cannot see.
- **Annually:** Comprehensive re-assessment including manual investigation of the top critical systems, physical walkthroughs of OT/embedded environments, and third-party/vendor cryptographic re-verification.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **Event-triggered:** Conduct unscheduled rescans after significant events — major system deployments, M&A integrations, data center migrations, vendor product upgrades, cryptographic vulnerability disclosures (e.g., a new CVE in OpenSSL or a NIST algorithm parameter change).

1.6.5 External Monitoring and Intelligence

Complement internal discovery with external monitoring:

- **Certificate Transparency (CT) log monitoring:** Continuously monitor CT logs for certificates issued against the organization's domains. This detects rogue or unauthorized certificate issuance and reveals shadow IT services with TLS certificates.
- **External attack surface monitoring:** Use external attack surface management (EASM) tools to discover internet-facing endpoints and their TLS configurations from an adversary's perspective.
- **Cryptographic vulnerability intelligence:** Subscribe to cryptographic vulnerability feeds (NIST NVD, vendor security advisories, crypto-specific mailing lists) and automatically cross-reference new disclosures against the CBOM. When a vulnerability is disclosed in a cryptographic library, instantly determine which CBOM entries are affected.
- **Standards and algorithm monitoring:** Track NIST, IETF, ETSI, and national agency announcements for algorithm deprecation notices, parameter changes, and new standardization. When a standard changes (e.g., NIST deprecation timeline acceleration), automatically re-flag affected CBOM entries for Phase 3 re-scoring.

1.6.6 Alerting and Response Framework

Define a tiered alerting model for cryptographic posture changes:

Alert Level	Trigger	Response	Timeline
Critical	Newly discovered system using deprecated/broken crypto (e.g., TLS 1.0, RSA-1024) in production; unknown internet-facing TLS endpoint detected	Immediate triage; assess whether this is active exploitation risk; remediate or isolate within 72 hours	Same day
High	Quantum-vulnerable algorithm introduced in new Tier-1 deployment without documented	Workstream lead review; CBOM update;	Within 1 week

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

	justification; certificate expiry approaching without renewal plan	remediation plan within 2 weeks	
Medium	New cryptographic library version detected that changes available algorithms; CBOM drift detected in quarterly rescan	Investigate; update CBOM; assess impact on migration timeline	Within 1 month
Informational	New non-critical system discovered with standard cryptographic configuration; routine certificate rotation completed	Log in CBOM; no action required unless pattern indicates broader issue	Next scheduled review

1.6.7 Organizational Culture and Training

Continuous discovery depends on organizational culture as much as tooling:

- Train developers and engineers to recognize and report cryptographic decisions in their work. Run awareness programs so that teams understand why documenting cryptographic choices matters and how to flag them through the established channels.
- Designate "crypto champions" in each major platform or application team who serve as the Inventory & Discovery workstream's point of contact and who proactively flag cryptographic changes within their team's domain.
- Establish feedback mechanisms (dedicated Slack/Teams channel, regular office hours, internal wiki) where anyone in the organization can report cryptographic observations that should be captured in the inventory.
- Include cryptographic inventory maintenance in performance objectives for the crypto champions and the Inventory & Discovery workstream lead. What gets measured gets done.

1.6.8 Measuring Discovery Effectiveness

Track the health of your continuous discovery capability with these operational metrics:

Metric	Target	What It Indicates
CBOM freshness	≥90% of entries updated within last 90 days	Whether the inventory is being maintained

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Discovery-to-CBOM lag	New system appears in CBOM within 5 business days of deployment	Whether CI/CD integration is working
Drift rate	<5% discrepancy between CBOM and quarterly rescan results	Whether continuous mechanisms are catching changes
Unknown-unknowns closure	Reduce gap register by 20% per quarter	Whether the organization is systematically closing discovery gaps
Time-to-detect	New unauthorized crypto endpoint detected within 7 days	Whether passive monitoring is effective

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Risk-driven scoping document	Tier-1 systems identified; discovery priorities A/B/C assigned; scoping rationale documented
Cryptographic asset inventory	Priority A systems: ≥90% coverage within 60 days; Priority B: ≥70% within 120 days; ≥90% of all Tier-1 systems within 12 months
Classical vulnerability findings	All classically vulnerable cryptography (deprecated algorithms, weak keys, expired certs, misconfigured protocols) identified and reported to security operations for immediate remediation
Sensitive data map (integrated)	All data classified by confidentiality requirement and retention period
Systems and assets register (integrated)	All assets classified by criticality and vendor dependency; cross-referenced with BIA classifications
Discovery gap register	Documented list of systems where discovery was incomplete, with remediation plan and target dates
Continuous discovery operating model	CI/CD integration operational; passive monitoring deployed; change management integration live; quarterly rescan schedule established; alerting framework defined; crypto champions designated

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 1 depends on Phase 0 outputs (charter, budget, governance, scoping assessment) and several organizational prerequisites including system access, baseline asset knowledge, and discovery tooling budget.

Feeds into

- **Phase 2** — Inventory data is the raw material from which the CBOM is populated. The data format and field completeness of discovery outputs directly determine CBOM quality — which is why the CBOM schema should be defined before large-scale discovery begins, not after.
- **Phase 3** — The inventory is the primary input for risk scoring. System classification by business criticality (from Activity 1.0), exposure type, and data sensitivity provides the context needed to calculate priority scores.
- **Phase 7** — Discovery reveals vendor dependencies that may not have been visible during Phase 0 scoping. As each system is inventoried, the discovery team should flag vendor products that control cryptographic operations — this data feeds directly into the vendor classification matrix (Phase 7, Activity 7.1).
- **Phase 0 (feedback)** — Classical cryptographic vulnerabilities surfaced during quantum-focused discovery (deprecated protocols, weak keys, expired certificates) provide immediate near-term security wins that strengthen the business case and demonstrate program value to the executive sponsor and SteerCo.

Runs in parallel with

- **Phase 2** — CBOM structure should be defined in the first weeks of Phase 1 so that discovery data flows directly into a standardized format. Phase 1 and Phase 2 are tightly coupled and should be staffed as coordinated workstreams, not sequential handoffs.
- **Phase 7** — As discovery identifies vendor dependencies, preliminary vendor outreach (questionnaires, roadmap inquiries) should begin immediately for any vendor appearing on the critical path — particularly vendors whose products were not on the initial Phase 0 top-10 list.
- **Itself, indefinitely** — Discovery does not "complete." It transitions from project-mode initial discovery into a permanent continuous discovery capability. Staff and budget planning must reflect this.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Interview-driven inventory.** Relying on application owners to self-report cryptographic usage. People don't know what crypto their systems use. Automated discovery supplemented by manual investigation is the only defensible approach.
- **Spreadsheet-only inventory.** A static spreadsheet becomes stale within weeks. The inventory must be maintained in a queryable system (CMDB, dedicated tool, or structured database) with automated refresh.
- **Waiting for 100% completeness before proceeding.** Completeness is asymptotic. You will never find everything. Use the 80/20 risk-driven scoping (Activity 1.0) to deliver actionable results quickly, proceed to Phase 2/3, and continue discovery in parallel.
- **Ignoring OT and embedded systems.** These are often the hardest to discover AND the hardest to migrate. Excluding them from scope guarantees surprises later. Physical walkthroughs are essential for OT environments.
- **Trusting a single tool for coverage.** No cryptographic discovery tool covers all five layers (network, code, config, runtime, manual). Deploy tools from multiple categories plus manual investigation.
- **CMDB-only asset discovery.** The CMDB is rarely complete. Organizations that rely solely on the CMDB for asset discovery consistently undercount their actual estate — particularly cloud resources, shadow IT, OT devices, and vendor-managed systems. Integrate the full range of data sources described in Activity 1.4.
- **Ignoring the immediate classical findings.** A quantum-focused cryptographic inventory will inevitably surface classically vulnerable cryptography (deprecated protocols, weak keys, expired certificates). Failing to remediate these findings immediately wastes a significant source of near-term security value and undermines the business case for the program. Report and remediate classical findings in parallel with continuing quantum-focused discovery.
- **Treating discovery as a project with an end date.** Discovery is not a phase that "completes" — it is a permanent operational capability. Organizations that disband the discovery team after "finishing" the initial inventory find their CBOM becomes stale within 6 months.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No cryptographic inventory exists; no awareness of the need
Level 1	Partial manual inventory of obvious systems (web servers, VPN); CMDB-only asset register; no continuous discovery
Level 2	Risk-driven scoping complete; automated discovery deployed on Priority A systems; ≥70% Tier-1 coverage; inventory is queryable; classical vulnerabilities being remediated; multiple asset data sources cross-referenced
Level 3	≥90% coverage; continuous discovery in CI/CD and passive monitoring; integrated with CMDB, SBOM, BIA, and certificate management; change management integration live; crypto champions designated; alerting framework operational
Level 4	Real-time cryptographic posture monitoring with tiered alerting; automated drift detection; coverage spans IT, OT, cloud, and third-party; discovery effectiveness metrics tracked and reported; discovery gap register trending toward zero

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 2 — CBOM & DOCUMENTATION

PURPOSE

Transform raw inventory data into a durable, queryable, standardized Cryptographic Bill of Materials (CBOM) that serves as the single source of truth for all subsequent phases. The CBOM is the foundational artifact that makes PQC migration auditable, plannable, and measurable.

Without a structured CBOM, inventory data remains a collection of scan results, spreadsheets, and tribal knowledge scattered across teams. The CBOM transforms this raw material into a single, queryable, standardized record that answers the questions every subsequent phase asks: What cryptography does system X use? Is it quantum-vulnerable? What depends on it? Who owns it? What is its migration status? Organizations that skip or defer CBOM formalization find themselves re-discovering the same information repeatedly — every time a risk score needs calculating, a pilot needs scoping, or an auditor asks for evidence.

Parallelization note

Phase 2 should begin concurrently with Phase 1, not after it. The most common mistake is treating CBOM as something you build once discovery is "complete." In practice, the CBOM schema and tooling should be defined in the first weeks of Phase 1, so that discovery data flows directly into a structured format from the start. Phase 2 also runs in parallel with Phase 3 — as CBOM entries are populated, risk scoring can begin on the entries that are ready, rather than waiting for full CBOM completion. The Minimum Viable CBOM model (below) is specifically designed to enable this parallelism: Layer 1 and Layer 2 data can be scored and prioritized while Layer 3 and Layer 4 discovery is still underway.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 1 inventory data — at least partial**. The CBOM cannot be populated without discovery data, but it does not require a complete inventory to begin. As soon as Layer 1 (infrastructure) and Layer 2 (platform) discovery produces results, CBOM population should start. Waiting for Layer 3 and Layer 4 completeness before beginning CBOM work is a form of the completeness trap this framework warns against.
- **Phase 0 governance structure with designated data ownership**. Every CBOM entry needs an owner — someone accountable for the accuracy and currency of that record. The governance structure from Phase 0 should define how ownership is assigned (typically aligned to the system or service owner) and what "ownership" means in practice (update frequency, accuracy expectations, escalation for disputes).

Organizational prerequisites

- **A decision on CBOM format and hosting platform**. CycloneDX is the recommended standard (see Activity 2.1), but the organization must also decide where the CBOM will live — a dedicated tool, a CMDB extension, a version-controlled repository, or a purpose-built database. This decision has implications for integration with CI/CD pipelines, SBOM tooling, and reporting systems. Making this decision early avoids costly reformatting later.
- **SBOM maturity, or a plan to develop it in parallel**. The CBOM gains significant value when linked to Software Bill of Materials (SBOM) data, because SBOM reveals the dependency chains through which cryptographic libraries propagate. Organizations with no existing SBOM practice should plan to develop basic SBOM capability concurrently with CBOM, at least for Tier-1 applications.
- **CI/CD pipeline access (for organizations targeting automated CBOM updates).** If the organization intends to integrate CBOM generation into its software delivery pipeline — which is strongly recommended for Layer 3 coverage — the CBOM team needs access to CI/CD tooling and cooperation from development/DevOps teams. This access should be negotiated during Phase 0 or early Phase 1.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

THE MINIMUM VIABLE CBOM MODEL

The conventional approach to CBOM — attempting to catalog every cryptographic function call in every system before proceeding — is a completeness trap that delays migration indefinitely. The Minimum Viable CBOM (MV-CBOM) model takes an architecture-first approach organized in four layers:

- **Layer 1 — Infrastructure Cryptography**: TLS/SSH/IPsec configurations on load balancers, reverse proxies, VPN concentrators, and network devices. This layer is discoverable through network scanning and configuration review. It represents the largest attack surface for HNDL and is the most amenable to hybrid deployment.
- **Layer 2 — Platform Cryptography**: Cryptographic services provided by platforms, frameworks, and middleware — cloud KMS, HSMs, certificate authorities, identity providers, service mesh mutual TLS. This layer is discoverable through cloud API queries, HSM audit logs, and platform configuration review.
- **Layer 3 — Application Cryptography**: Cryptographic operations in application code — encryption of data at rest, digital signature generation/verification, token creation, custom protocol implementations. This layer requires code scanning and runtime analysis.
- **Layer 4 — Embedded/Third-Party Cryptography**: Cryptographic implementations in vendor products, firmware, IoT devices, and OT systems where the organization has no source code access and limited configuration control. This layer requires vendor documentation review, binary analysis, or acceptance of incomplete visibility.
- **The MV-CBOM strategy**: Achieve comprehensive coverage of Layers 1 and 2 first (weeks to months), because these layers contain the highest-exposure, most-controllable cryptographic usage. Achieve targeted coverage of Layer 3 for high-risk applications (months). Accept documented incompleteness at Layer 4, where vendor dependencies constrain visibility, and manage this through the vendor governance process (Phase 7).

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

2.1 Select CBOM Format and Tooling

Recommended format: CycloneDX — the de facto standard for CBOM, with native support for cryptographic asset types including algorithms, certificates, keys, protocols, and related dependencies. CycloneDX is supported by OWASP, adopted by the PQCC, and integrated into tooling from IBM, SandboxAQ, and the Linux Foundation's PQCA (CBOMkit).

CBOM record structure (per CycloneDX):

Each CBOM entry should capture at minimum:

Field	Purpose
Component identifier	Links to asset inventory and CMDB
Algorithm OID	Unambiguous algorithm identification
Key size / security parameter	Determines quantum vulnerability class
Protocol context	Where the algorithm is used (TLS, IPsec, S/MIME, etc.)
Implementation (library + version)	Identifies patching and upgrade path
Certificate reference	Links to certificate chain for PKI-related crypto
Data classification	From Track B of Phase 1
Quantum vulnerability status	Vulnerable (Shor), weakened (Grover), safe
Migration status	Not started / Planned / In progress / Hybrid / PQC-only / Not applicable
Owner	Responsible team for migration decisions
Vendor dependency flag	Whether migration is self-controlled or vendor-dependent

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

2.2 Populate CBOM from Inventory Data

Map Phase 1 inventory data into CBOM records. This is primarily a data transformation and enrichment exercise:

1. Import automated discovery results into CycloneDX format using tool-native exporters or CBOMkit
2. Enrich with manual investigation findings for systems not covered by automated tools
3. Cross-reference with SBOM data to establish library dependency chains
4. Link to certificate management system for PKI-related entries
5. Add data classification tags from Track B of Phase 1
6. Flag vendor dependencies from Track C of Phase 1

2.3 Integrate CBOM into Operational Processes

The CBOM has no value if it is a static document. Integrate it into:

- **CI/CD pipelines:** New deployments automatically generate or update CBOM entries. Block deployments that introduce quantum-vulnerable algorithms without documented justification and migration plan.
- **Change management:** CAB reviews include CBOM impact assessment — does this change introduce, modify, or remove cryptographic components?
- **Vendor onboarding:** New vendor products must provide CBOM-compatible cryptographic documentation as a procurement requirement.
- **Audit and compliance:** CBOM snapshots at regular intervals provide audit trail for regulatory evidence.

2.4 Establish CBOM Freshness Governance

Trigger	Action
New system deployment	Auto-generate CBOM entries via CI/CD
Library version update	Update implementation version; check for algorithm changes

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Certificate renewal/rotation	Update certificate reference and validity dates
Quarterly full scan	Reconcile CBOM against latest discovery results; flag discrepancies
Vendor product update	Request updated CBOM data from vendor; update entries
Algorithm deprecation notice	Flag all CBOM entries using deprecated algorithm; trigger Phase 3 re-scoring

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
CycloneDX CBOM (Layers 1–2 complete)	100% of infrastructure and platform cryptography documented within 3 months
CycloneDX CBOM (Layer 3 targeted)	High-risk applications documented within 6 months
Layer 4 gap register	All vendor-dependent systems documented with known/unknown cryptographic usage
CI/CD integration	New deployments auto-generate CBOM entries
CBOM governance policy	Freshness rules, ownership, update triggers documented and enforced

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 2 depends on Phase 1 inventory data (at least partial), Phase 0 governance for data ownership, and several organizational prerequisites including CBOM format decisions and SBOM maturity.

Feeds into

- **Phase 3** — The CBOM is the primary data source for risk scoring. Each CBOM entry's algorithm, protocol context, data sensitivity, and migration feasibility fields are the inputs to the Phase 3 scoring model. CBOM entries that lack enriched metadata cannot be meaningfully scored — so CBOM quality directly constrains risk scoring quality.
- **Phase 5** — The CBOM's migration status field tracks pilot and production deployments, providing the authoritative record of what has been migrated, what is in progress, and what remains. Without this, migration progress reporting relies on manual tracking that becomes unreliable at scale.
- **Phase 7** — Layer 4 (embedded/third-party) CBOM gaps — where the organization cannot determine the cryptographic implementation because a vendor controls it — directly drive vendor engagement priorities. Each Layer 4 gap is a vendor question that Phase 7 must answer.
- **Phase 1 (feedback)** — CBOM analysis identifies discovery gaps: systems that should have CBOM entries but don't, dependencies that appear in one system's CBOM but whose source system hasn't been inventoried, or cryptographic usage patterns that suggest undiscovered systems. This feedback should drive targeted re-discovery.

Runs in parallel with

- **Phase 1** — CBOM structure should shape inventory data collection from the start. Discovery and CBOM population run as coordinated workstreams with a shared data model.
- **Phase 3** — As CBOM entries are enriched, risk scoring can begin on ready entries without waiting for full CBOM completion. This is particularly important for Layer 1 and Layer 2 entries, which should be scorable within weeks of initial discovery.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Completeness trap.** Insisting on 100% CBOM coverage before proceeding to risk scoring and migration. Layer 4 (embedded/third-party) will never be fully visible. Accept this, document the gaps, and manage through vendor governance.
- **CBOM as document, not system.** Producing a CBOM in a PDF or spreadsheet that is never updated. The CBOM must be a live, queryable data set integrated into operational processes.
- **Ignoring the SBOM-CBOM linkage.** CBOM entries without SBOM context miss critical dependency chains. A vulnerable algorithm in a widely-shared library affects every application that depends on it.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No CBOM exists; cryptographic documentation is ad hoc or absent
Level 1	Partial CBOM in spreadsheet form covering known systems; no standard format
Level 2	CycloneDX CBOM operational for Layers 1–2; queryable; SBOM linkage established for key applications
Level 3	CBOM covers Layers 1–3; integrated into CI/CD; freshness governance enforced; change management integration live
Level 4	CBOM is a real-time operational asset; auto-updated on deployment; Layer 4 gaps systematically managed through vendor governance; CBOM drives automated compliance reporting

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 3 — RISK SCORING & PRIORITIZATION

PURPOSE

Translate CBOM data into a defensible, sequenced migration priority list. Not all quantum-vulnerable cryptography carries equal risk or equal migration difficulty. This phase produces the prioritized backlog that drives Phase 4 roadmap planning and Phase 5 execution sequencing.

Risk scoring is where the program transitions from "what do we have?" to "what do we do first?" — and it is where organizational politics often intrude. Every business unit believes its systems are either the most critical (and therefore should be migrated first) or the least affected (and therefore should be left alone). A structured, transparent scoring model depoliticizes this conversation by replacing opinion with defensible, repeatable criteria. The QRA (Quantum Readiness Assessment) output from this phase also serves as the primary audit artifact — it demonstrates to regulators, auditors, and the board that the organization is making evidence-based decisions about migration sequencing, not simply reacting to whichever vendor or team shouts loudest.

Parallelization note

Phase 3 can begin as soon as the first CBOM entries are enriched with sufficient metadata — it does not require a complete CBOM. In practice, organizations should score Layer 1 and Layer 2 CBOM entries while Layer 3 discovery and CBOM population continue. This produces an initial prioritized backlog early enough to inform Phase 4 roadmap planning and Phase 7 vendor engagement. Risk scoring is also not a one-time activity — it must be re-run periodically (at least quarterly) as new inventory data arrives, regulatory deadlines shift, vendor PQC support timelines become clearer, and NIST standards evolve. The QRA should be treated as a living document, not a point-in-time assessment.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 2 CBOM with enriched metadata — at least for Tier-1 systems**. Each CBOM entry being scored needs, at minimum: the algorithm(s) in use, the protocol context, the data sensitivity classification of the protected data, the system's business criticality tier, and an initial assessment of migration feasibility (can this be changed, and by whom?). CBOM entries that lack these fields cannot be meaningfully scored.
- **Phase 1 inventory data sufficient to identify Tier-1 and Tier-2 systems**. The risk scoring model requires a classified system inventory to weight business impact. If Phase 1 has not yet produced a classified list of systems by business criticality, this classification must be done as a preliminary step within Phase 3.
- **Phase 0 governance structure that defines who accepts risk**. Risk scoring inevitably produces results that some stakeholders will contest. The governance model must define who has authority to accept residual risk, override priority assignments, or defer migration — and the escalation path when disagreements arise. Without this, the scoring exercise produces a document that no one acts on.

Organizational prerequisites

- **An existing risk management framework (or willingness to adopt one for this purpose)**. The risk scoring model in this phase extends ISO/IEC 27005 and NIST SP 800-30 with quantum-specific dimensions. Organizations with a mature risk management practice should integrate the quantum scoring factors into their existing framework. Organizations without one will need to establish at least a basic risk scoring methodology — which is valuable well beyond PQC migration.
- **Data classification scheme**. The "Data Sensitivity" scoring dimension requires an organizational data classification standard (e.g., Public / Internal / Confidential / Restricted). If the organization does not have one, creating a fit-for-purpose classification for PQC risk scoring is an immediate prerequisite. This is another example of how PQC migration forces long-overdue security hygiene improvements.
- **Legal counsel engagement for long-retention data**. Organizations storing encrypted data with retention periods exceeding 10–15 years (medical records, financial archives, government records, legal documents) face compounding HNDL exposure. Legal counsel should be engaged to assess whether data retention policies, contractual confidentiality obligations, or regulatory requirements create additional urgency for specific data stores. This input directly affects the risk scoring weights.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

3.1 Define Risk Scoring Model

The risk scoring model below extends established information security risk management methodologies (ISO/IEC 27005, NIST SP 800-30, NIST RMF) with quantum-specific threat dimensions. Organizations that already operate a mature risk management framework should integrate these quantum-specific factors into their existing scoring methodology rather than creating a parallel system. The weights below represent a default starting configuration; organizations should calibrate weights based on their specific risk profile, sector, and regulatory context through a structured analysis involving both cryptographic and business stakeholders.

Score each CBOM entry across four dimensions:

Dimension 1 — Data Sensitivity × Exposure Window (HNDL Risk)

Factor	Weight	Scoring
Data confidentiality requirement (years)	High	>15yr = Critical; 10–15yr = High; 5–10yr = Medium; <5yr = Low
Data volume / flow rate	Medium	High-throughput channels score higher (more harvestable material)
Accessibility to adversary	High	Internet-facing = Critical; Partner-facing = High; Internal = Medium; Air-gapped = Low

Dimension 2 — Trust Infrastructure Criticality (TNFL Risk)

Factor	Weight	Scoring
Key/certificate lifetime	High	Root CA (20yr) = Critical; Intermediate CA (10yr) = High; End-entity (1yr) = Medium
Scope of trust dependency	High	Enterprise-wide PKI root = Critical; Single-app signing key = Medium
Signature verification period	Medium	Firmware signed for 15yr lifecycle = Critical; Session auth = Low

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Dimension 3 — Migration Feasibility

Factor	Weight	Scoring
Control posture	High	Full control (both endpoints) = Easy; Shared control = Medium; Vendor-dependent = Hard
Protocol/standard maturity	Medium	PQC-capable standard exists and is implemented = Easy; Standard exists but no vendor support = Medium; No standard yet = Hard
Interoperability constraints	Medium	Internal-only = Easy; Partner ecosystem = Medium; Public internet = Harder (but proven at scale)
System age and architecture	Medium	Modern microservices = Easy; Monolithic but maintained = Medium; Legacy unsupported = Hard

Dimension 4 — Regulatory and Compliance Pressure

Factor	Weight	Scoring
Specific regulatory deadline	High	Mandatory deadline within 2 years = Critical; Within 5 years = High; General expectation = Medium
Audit exposure	Medium	External audit scope = High; Internal audit scope = Medium; Not audited = Low
Contractual requirement	Medium	Customer/partner contract requires PQC = High; Expected soon = Medium; Not required = Low

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

3.2 Calculate Priority Scores

For each CBOM entry, calculate a composite priority score:

Priority = (HNDL Risk × 0.35) + (TNFL Risk × 0.25) + (Regulatory Pressure × 0.25) + (Migration Feasibility Inverse × 0.15)

Note: Migration Feasibility is inverted — harder migrations may need earlier starts despite lower risk, because they require longer lead times. The weighting reflects that HNDL is the most immediately exploitable threat.

Decision Point — Urgency Classification:

Based on composite scores, classify each CBOM entry into migration tiers:

Tier	Criteria	Target Timeline
Tier 1 — Immediate	Critical HNDL exposure + high adversary accessibility + feasible migration (you control both endpoints)	Begin within 6 months; hybrid deployment within 12 months
Tier 2 — High Priority	High HNDL or TNFL risk + regulatory deadline within 3 years	Begin within 12 months; hybrid deployment within 24 months
Tier 3 — Standard	Medium risk + migration feasible with vendor coordination	Begin within 24 months; complete within regulatory deadline
Tier 4 — Long Tail	Lower risk OR migration currently infeasible (vendor dependency, no standard)	Monitor; compensating controls; migrate when feasible

3.3 Apply Migration Sequencing Logic

Within each tier, sequence migrations based on the following priority order (reflecting threat immediacy and technical dependencies):

1. **Key exchange systems (TLS, VPN, key establishment protocols)** — Immediately stops creating new HNDL-vulnerable sessions. This is the highest-urgency action because adversaries are harvesting encrypted traffic now.
2. **Signature and PKI systems (code signing, document signing, PKI infrastructure)** — Prevents future forgery and protects long-lived trust anchors. Digital signatures and

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PKI trust chains have long validity periods. Many signature systems depend on having secure key exchange infrastructure already in place.

3. **Data at rest** — Re-encrypt long-lived archives with strong symmetric encryption (AES-256) and implement PQC-aware key-wrapping mechanisms. This is lower urgency because data at rest requires exfiltration before it can be harvested, adding a layer of difficulty for adversaries.

3.4 Produce the Quantum Readiness Assessment (QRA)

Consolidate risk scoring into a formal Quantum Readiness Assessment document that serves as the defensible basis for migration planning and regulatory evidence:

- **Executive summary:** Overall quantum risk posture; aggregate maturity score; comparison to regulatory deadlines
- **Heatmap:** Visual representation of risk across the estate, organized by system tier and domain
- **Prioritized migration backlog:** Sequenced list of all CBOM entries with tier assignments, target timelines, and owner assignments
- **Gap analysis:** Where current posture falls short of regulatory requirements, with specific remediation actions
- **Compliance mapping:** How QRA outputs map to NIST, CNSA 2.0, ETSI, sector-specific requirements

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Scored and tiered CBOM	Every CBOM entry has a priority score and tier assignment
Quantum Readiness Assessment (QRA)	Executive summary, heatmap, prioritized backlog, gap analysis, compliance mapping
Migration sequencing recommendation	Ordered backlog ready for Phase 4 roadmap planning

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 3 depends on Phase 2 CBOM data (at least for Tier-1 systems), Phase 1 inventory with system classification, Phase 0 governance for risk acceptance authority, and organizational prerequisites including a risk management framework and data classification scheme.

Feeds into

- **Phase 4** — The prioritized migration backlog is the primary input for roadmap planning. Tier assignments determine sequencing; priority scores determine resource allocation; migration feasibility ratings identify systems that require vendor support before they can be scheduled.
- **Phase 5** — Tier assignments determine pilot selection. The highest-priority, most-controllable systems from the Phase 3 backlog become the first pilot candidates.
- **Phase 7** — Risk scoring reveals which vendor dependencies are blocking Tier-1 migration. A CBOM entry scored as "Tier-1 priority, migration blocked by vendor" translates directly into an urgent vendor engagement action with executive escalation authority.
- **Phase 0 (feedback)** — The QRA is a primary audit artifact and board reporting input. It provides the evidence the executive sponsor needs to sustain multi-year funding by demonstrating structured, defensible decision-making. QRA findings may also trigger revisions to the business case — for example, if risk scoring reveals higher HNDL exposure than initially estimated.

Runs in parallel with

- **Phase 2** — Risk scoring begins as soon as CBOM entries are sufficiently enriched, without waiting for full CBOM completion. Scoring results also feed back into CBOM prioritization, helping Phase 2 teams focus enrichment effort on the entries that matter most.
- **Itself, iteratively** — Risk scoring is not a one-time exercise. The QRA must be re-run at least quarterly as new inventory data arrives, regulatory deadlines shift, vendor timelines change, and NIST standards evolve.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Equal priority for everything.** Treating all quantum-vulnerable crypto as equally urgent. This leads to resource dilution and no meaningful progress on the highest-risk systems.
- **Ignoring migration feasibility in prioritization.** Assigning highest priority to systems that cannot be migrated yet (no vendor support, no standard) while ignoring high-risk systems that could be migrated today.
- **Static risk assessment.** Producing the QRA once and never updating it. Risk scores change as standards mature, vendor products ship, and regulatory deadlines approach.
- **Neglecting the legal and data-retention dimension.** Organizations storing long-lived encrypted data (medical records, financial archives, legal documents, government records) face a compounding legal risk: data encrypted today with quantum-vulnerable algorithms may become decryptable in the future, potentially violating data protection principles (such as GDPR's data security requirements) and contractual confidentiality obligations. The QRA should prompt a legal risk assessment alongside the technical one — evaluating whether data retention policies should be revised, whether additional protection layers (PQC key-wrapping, tokenization) should be applied to long-retention data, and whether data subjects or counterparties should be informed of the evolving risk profile. Engage legal counsel early; do not treat this as a purely technical exercise.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No quantum risk assessment exists
Level 1	Informal awareness of which systems are "probably vulnerable"; no structured scoring
Level 2	Formal risk scoring model applied to Tier-1 CBOM entries; prioritized migration backlog exists; QRA document produced
Level 3	QRA updated quarterly; all CBOM entries scored and tiered; migration sequencing drives Phase 5 execution; legal risk dimension assessed
Level 4	Continuous risk posture management; automated re-scoring when CBOM changes or regulatory deadlines shift; QRA integrated into enterprise risk register and audit cycle

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 4 — ROADMAP & GOVERNANCE

PURPOSE

Translate the prioritized migration backlog from Phase 3 into a multi-year execution plan with realistic milestones, resource allocations, vendor coordination timelines, and governance checkpoints. This phase establishes the PMO discipline to manage that complexity.

Phase 4 is where the program's ambition meets organizational reality. A prioritized backlog (Phase 3) tells you what needs to happen and in what order; a roadmap tells you when it will happen, who will do it, what it will cost, and what it depends on. The distinction matters because most PQC migration timelines are not constrained by internal execution capacity — they are constrained by vendor readiness, hardware refresh cycles, regulatory deadlines, and the availability of scarce cryptographic engineering skills. The roadmap must model these external constraints explicitly, not just internal work sequencing. Organizations that build PQC roadmaps as if they were building a software delivery plan — estimating internal effort and scheduling accordingly — discover that the actual critical path runs through vendor GA dates and hardware procurement lead times they did not account for.

Parallelization note

Phase 4 overlaps significantly with Phases 5, 6, and 7. The roadmap is not a plan you complete and then hand off for execution — it is a living instrument that is updated as pilots reveal unexpected infrastructure requirements (Phase 6), vendor timelines slip or accelerate (Phase 7), and early migration waves generate lessons that change assumptions for later waves (Phase 5). In practice, the initial roadmap is drafted as soon as the first Phase 3 risk scoring outputs are available, and it is revised quarterly thereafter. Phase 4 also activates vendor engagement (Phase 7) immediately — vendor engagement cannot wait for the roadmap to be "finished," because vendor lead times are typically the longest items on the critical path.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 3 prioritized migration backlog**. The roadmap sequences work according to the tier assignments and priority scores from Phase 3. Without a scored backlog, roadmap construction devolves into stakeholder negotiation about whose systems go first — exactly the politicization that structured risk scoring is designed to prevent.
- **Phase 0 budget structure and multi-year commitment**. A roadmap without confirmed multi-year funding is aspirational fiction. The Phase 0 budget structure — including the phased funding model and benefit tracking approach — provides the financial framework within which the roadmap must fit.
- **Phase 1/2 data sufficient to estimate migration scope**. The roadmap must include realistic effort estimates, which require at least a rough understanding of what needs to change in each system. CBOM data for Tier-1 and Tier-2 systems should be available, along with enough inventory data to identify major vendor dependencies and infrastructure constraints.

Organizational prerequisites

- **PMO capability or access to program management professionals.** PQC migration at enterprise scale is a program, not a project. It requires program management discipline: dependency tracking across workstreams, resource management across business units, risk and issue management, and structured reporting. Organizations without existing PMO capability should plan to hire or contract program management resources specifically for this initiative.
- **Visibility into infrastructure refresh cycles, cloud migration plans, and vendor contract renewal dates**. The most cost-effective PQC migration strategy piggybacks on already-funded infrastructure changes. The roadmap team needs access to IT asset lifecycle data, cloud migration roadmaps, and procurement calendars to identify these integration opportunities. Without this visibility, the roadmap will propose standalone PQC upgrades that are more expensive and harder to fund than embedded ones.
- **Stakeholder alignment on the program's time horizon**. Phase 4 forces the organization to confront a 4–15 year execution timeline. If key stakeholders still believe PQC migration is a 12–18 month effort, the roadmap planning process will surface this gap in expectations. It is better to resolve this misalignment at the start of Phase 4 than to discover it when Year 2 budget requests are rejected.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

4.1 Define Year-1 Starter Plan (90-Day Governance Sprint)

The first 90 days set the organizational foundation. Deliver five things:

1. **Organization:** Executive sponsor and QRPM confirmed; SteerCo calendar and charter published; RACI matrix for all workstreams.
2. **People:** 10-to-20 person training cohort enrolled in PQC fundamentals; "crypto champions" designated per platform team.
3. **Plan:** Crypto-BOM v1 with ≥70% Tier-1 coverage complete; 2 hybrid pilots selected (TLS and VPN); vendor questionnaires sent to top 10 strategic vendors.
4. **Policy/Procurement:** Cryptographic policy updated (approved cipher suites include PQC hybrids; shorter key lifetimes mandated for new certificates); PQC and crypto-agility clause added to all new RFPs and contract renewals.
5. **KPI pack:** Baseline values established; Q+1 targets set; board reporting template ready.

Year 1 — Quarter-by-Quarter Detailed Plan:

Quarter	Governance & People	Discovery & CBOM	Pilots & Technical	Vendor & Policy
Q1	Appoint QRPM; convene SteerCo; publish charter and RACI; designate crypto champions; launch training cohort	Deploy Priority A discovery (internet-facing, Tier-1 systems); begin CBOM structure design; cross-reference with existing CMDB, BIA, and cert management data	Select 2 pilot targets (TLS + VPN); set up lab/staging environments; define pilot success criteria and SLOs	Send PQC roadmap questionnaires to top 10 vendors; draft updated procurement clause; begin cryptographic policy revision
Q2	First SteerCo milestone review; present initial findings to executive sponsor; refine	Complete Priority A discovery; begin Priority B; publish Crypto-BOM v1 (≥70% Tier-1 coverage); surface	Execute pilots in lab/staging; measure performance baselines; document findings	Collect vendor responses; classify vendors by PQC criticality; publish updated cryptographic

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

	RACI based on Q1 experience	and report classical vulnerabilities	and compatibility issues	policy and procurement language
Q3	Second SteerCo review; present QRA findings; request Year 2 budget refinement if needed; expand training to second cohort	Begin Phase 3 risk scoring on Priority A systems; populate CBOM migration status fields; integrate CBOM into CI/CD (initial)	Promote validated pilots to production canary (1–5% traffic); measure production SLOs; begin Wave 1 planning	Follow up with non-responsive vendors; evaluate bridging patterns for vendor-blocked systems; insert PQC clauses into upcoming contract renewals
Q4	Quarterly board report (first formal); present Year 1 achievements and Year 2 plan; finalize multi-year roadmap	Complete QRA for Tier-1 systems; Crypto-BOM v2 (≥90% Tier-1, ≥60% Tier-2); establish continuous discovery operating rhythm	Complete canary validation; begin Wave 2 (internal production); document validated migration patterns as repeatable playbooks	Vendor PQC scorecard published; escalation plan for non-compliant strategic vendors; Year 2 vendor engagement calendar set

4.2 Structure the Multi-Year Roadmap

Year	Focus	Key Milestones
Year 1	Foundation	Crypto-BOM v1; 2–4 hybrid pilots (TLS, VPN); vendor commitments secured; policy updates; team training
Year 2	Tier-1 Rollout	Hybrid/PQC deployed on all Tier-1 internet-facing endpoints; PKI key-lifetime reductions implemented; dual-sign pilots for code signing
Year 3	Bulk Migration	Tier-2 systems migrated; internal east-west traffic hybrid-enabled; HSM firmware upgrades; vendor product upgrades tracked

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Year 4	Long Tail & OT	Tier-3/4 systems addressed; OT gateway protections deployed; embedded device migration or containment; compensating controls where migration infeasible
Year 5	Hardening & Agility	Eliminate remaining compensating controls; achieve crypto-agility across the estate; transition from hybrid to PQC-only where ecosystem supports it; achieve target maturity level

4.3 Align to Infrastructure Refresh Cycles

Map migration tasks to existing planned expenditures:

Planned Refresh	PQC Opportunity
Data center network refresh	Deploy PQC-capable switches/load balancers; enable hybrid TLS at edge
SD-WAN / VPN upgrade	Require PQC support in new VPN concentrators; enable hybrid IPsec
Cloud migration wave	Configure PQC-capable TLS on cloud load balancers; use cloud-native PQC KMS
PKI renewal / CA migration	Deploy PQC-capable CA; issue hybrid/composite certificates; shorten key lifetimes
HSM replacement cycle	Procure PQC-capable HSMs (Thales Luna v7.9+, Utimaco Quantum Protect, or equivalent)
Vendor contract renewal	Insert PQC roadmap requirements, crypto-agility clauses, SLAs
Application modernization	Implement cryptographic abstraction layers; replace hardcoded algorithm calls with provider pattern

4.4 Establish PMO Structure for Scale

For programs exceeding 10,000 tasks, establish:

- **Work breakdown structure (WBS)** aligned to the 8 workstreams defined in Phase 0

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **Dependency mapping** between workstreams — see critical dependency chains below
- **Critical path analysis** identifying the longest dependency chain — this determines the minimum program duration
- **Resource leveling** to avoid overloading shared teams (especially PKI, security architecture, and vendor management)
- **Risk register** with escalation triggers (e.g., "if vendor X misses PQC GA date by >6 months, escalate to SteerCo for alternate vendor evaluation")

Critical dependency chains (must be mapped and tracked):

Understanding these dependencies prevents the most common scheduling failures:

Upstream Activity	Must Complete Before	Why
CBOM v1 (Phase 2)	Risk scoring (Phase 3)	Cannot prioritize what you haven't inventoried
Risk scoring (Phase 3)	Pilot target selection (Phase 5)	Pilots must target the highest-priority systems, not the most convenient ones
HSM firmware upgrade (Phase 6)	Application PQC migration for HSM-dependent apps (Phase 5)	Applications that depend on HSM-protected keys cannot migrate until the HSM supports PQC key types
PKI CA modernization (Phase 6)	Dual-sign / PQC certificate deployment (Phase 5)	Cannot issue PQC certificates until the CA infrastructure supports PQC algorithms
Library upgrade (Phase 5)	Application hybrid enablement (Phase 5)	Applications cannot negotiate PQC if the underlying cryptographic library does not support it
Vendor PQC GA release (Phase 7)	Migration of vendor-dependent systems (Phase 5)	Cannot migrate systems where the vendor controls the cryptographic implementation until the vendor ships PQC support

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Network middlebox testing (Phase 6)	Production hybrid deployment on affected network paths (Phase 5)	Middleboxes that cannot parse PQC handshakes will cause connection failures if not identified in advance
Procurement policy update (Phase 0/4)	New system acquisitions (ongoing)	Without PQC in procurement requirements, every new acquisition potentially creates new quantum-vulnerable debt

The typical critical path for most enterprises is: Discovery → CBOM → Risk Scoring → Roadmap → Vendor Engagement → Vendor GA Release → Pilot → Production Rollout. The vendor dependency is usually the longest segment — start vendor engagement as early as possible (Q1 Year 1) even before the full CBOM is complete.

4.5 Manage the Roadmap as a Living Instrument

The roadmap is not a static Gantt chart that you create once in Phase 4 and follow mechanically. Quantum readiness is a multi-year program operating in a rapidly evolving landscape where standards, vendor timelines, regulatory deadlines, and threat intelligence all shift.

Quarterly roadmap review (standing SteerCo agenda item):

Present KPIs alongside leading indicators:

- **Quantum technology signals:** Logical qubit milestones, resource-estimate drops for breaking RSA/ECC, gate speed improvements, major lab announcements hitting roadmap milestones earlier than expected
- **Adversary signals:** Intelligence reports on HNDL campaigns (targeted interception and archival of encrypted data), supply-chain targeting of PKI/code-signing toolchains
- **Standards and regulatory signals:** NIST/IETF/ETSI/ISO algorithm updates, parameter changes, hybrid profiles moving to RFCs, new/earlier regulatory mandates
- **Vendor milestone signals:** Vendor GA dates met or missed, new PQC-capable products entering the market, FIPS validation completions

Decision playbook for when the roadmap needs adjustment:

- If KPIs are off track → Add resources, descope lower-risk items, pull forward bridging patterns

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- If leading indicators worsen (e.g., CRQC timeline estimates shortened) → Move to accelerated track with pre-drafted resource request
- If performance issues surface at scale → Deploy offload/scale-out, adjust SLOs, extend pilot windows before broader rollout
- If a critical vendor misses a committed date → Activate the champion-challenger pattern (Phase 7); deploy bridging pattern; escalate contractually

4.6 Define Milestone Gates

Each phase transition requires a milestone gate review:

Gate	Criteria	Decision Authority
G0 → G1	Charter approved; budget committed; QRPM appointed	Executive Sponsor
G1 → G2	≥70% Tier-1 inventory complete; CBOM structure defined	SteerCo
G2 → G3	CBOM populated; risk scoring complete; QRA delivered	SteerCo
G3 → G4	Multi-year roadmap approved; Year 1 plan resourced	Executive Sponsor
G4 → G5	Pilot designs approved; success criteria defined; rollback plans documented	SteerCo
G5 → G6	Pilots validated; performance baselines established; Tier-1 rollout approved	SteerCo
G6 → G7	Infrastructure upgrades scheduled; vendor commitments tracked	QRPM

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Multi-year roadmap	5-year plan with annual milestones; aligned to refresh cycles; critical path identified
Year 1 detailed plan	Quarter-by-quarter with named owners, resource allocations, and success criteria
PMO operating model	WBS, dependency map, risk register, meeting cadence, escalation procedures
KPI dashboard	Baseline values set; targets for Q+1 defined; board reporting template operational
Policy updates	Cryptographic policy, procurement policy, change management policy updated with PQC requirements

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 4 depends on Phase 3 prioritized backlog, Phase 0 budget structure and multi-year commitment, Phase 1/2 data sufficient for scope estimation, and organizational prerequisites including PMO capability and visibility into infrastructure refresh cycles.

Feeds into

- **Phase 5** — The roadmap determines pilot selection, sequencing, resource allocation, and milestone gates. It specifies which systems are in Wave 1, what success criteria apply, and what the rollback triggers are.
- **Phase 6** — The infrastructure upgrade schedule (HSM replacement, PKI modernization, middlebox upgrades) is a roadmap deliverable. Phase 6 executes what Phase 4 plans and funds.
- **Phase 7** — The roadmap establishes the vendor engagement timeline: when each Strategic Blocking vendor must deliver PQC support to avoid becoming a critical-path blocker. This timeline gives vendor engagement its urgency and provides the basis for contractual commitments.

Runs in parallel with

- **Phases 5, 6, and 7** — The roadmap is not a plan that is "completed" and handed off. It is a living instrument, revised quarterly as pilot results (Phase 5) reveal unexpected complexity, infrastructure assessments (Phase 6) identify new constraints, and vendor timelines (Phase 7) shift. Roadmap governance (SteerCo reviews, milestone gates, contingency triggers) runs continuously alongside execution.
- **Phases 1 and 2** — Discovery and CBOM population continue throughout Phase 4 and beyond. New inventory data may reveal previously unknown systems that change the roadmap's scope or sequencing — the roadmap review process must accommodate these inputs.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Planning in isolation from refresh cycles.** Building a PQC migration plan that ignores the organization's existing hardware refresh, cloud migration, and vendor contract renewal schedules. This results in "big-bang" budget requests that get rejected and missed opportunities to embed PQC into already-funded programs.
- **Underestimating the vendor dependency on the critical path.** The longest segment of most PQC migration critical paths is waiting for vendor products to ship PQC support. Organizations that start vendor engagement in Year 2 instead of Q1 Year 1 discover too late that their timeline is vendor-constrained and cannot be compressed with internal effort alone.
- **Single-track roadmap with no contingencies.** A roadmap that assumes every vendor delivers on time, every pilot succeeds first try, and no regulatory timeline changes. Build in explicit contingency triggers and pre-drafted acceleration/deceleration plans.
- **Treating the roadmap as a project plan rather than a program plan.** PQC migration is not a project with a defined end date — it is a permanent operational capability (crypto-agility). The roadmap should transition from "migration execution" to "ongoing cryptographic posture management" by Year 4–5, not simply declare victory and disband the team.
- **Governance without teeth.** Establishing a SteerCo that meets but does not make binding decisions, approve funding, or hold workstream leads accountable. The governance structure must have decision authority over budget, timelines, risk acceptance, and vendor escalation — not just advisory status.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No migration plan exists
Level 1	Informal plan exists (spreadsheet, no governance); single-year horizon
Level 2	Multi-year roadmap approved; Year 1 plan resourced; SteerCo operational; KPI baseline set
Level 3	Quarterly roadmap reviews operational; dependency mapping maintained; refresh cycle alignment documented; vendor engagement tracked on dashboard
Level 4	Roadmap is a living instrument with quarterly updates; contingency triggers defined and tested; leading indicators monitored; program transitioning from migration execution to ongoing posture management

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 5 — PILOTS & MIGRATION EXECUTION

PURPOSE

Execute the migration through controlled pilots, validate patterns, and scale to production through waves. This phase operationalizes the roadmap from Phase 4, starting with the highest-priority, most-controllable systems and expanding systematically.

Phase 5 is where the program produces its first tangible security outcomes — systems that are actually protected against quantum cryptanalytic threats, not just inventoried and planned for. It is also where the organization confronts the gap between theoretical migration design and production reality. Pilots will surface infrastructure incompatibilities, performance regressions, middlebox failures, and interoperability problems that no amount of planning can fully anticipate. This is expected and desirable — the purpose of the pilot phase is precisely to discover these problems in a controlled setting with tested rollback procedures, rather than at scale during production deployment.

Parallelization note

Phase 5 runs concurrently with Phase 6 (Infrastructure Modernization) and Phase 7 (Vendor Governance) in a tightly coupled feedback loop. Pilots reveal infrastructure bottlenecks that feed Phase 6 requirements; infrastructure upgrades enable broader pilot scope; vendor engagement in Phase 7 unblocks systems that depend on third-party PQC support. Organizations should not wait for infrastructure modernization to be "complete" before starting pilots — early pilots on systems with existing infrastructure support generate lessons and organizational confidence that justify the infrastructure investment. Similarly, Phase 1 discovery and Phase 2 CBOM maintenance continue throughout Phase 5, as migration activities themselves generate updated cryptographic posture data that must flow back into the CBOM.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 3 tier assignments identifying pilot candidates**. Pilot targets should come from the Tier-1 priority list, not from team convenience. The risk scoring output from Phase 3 determines which systems justify the investment and risk of early migration.
- **Phase 4 roadmap with resource allocation and sequencing for the first migration wave**. The roadmap provides the timeline, staffing plan, and milestone gates that govern pilot execution. Pilots launched without roadmap context tend to be underfunded, under-measured, and disconnected from the broader program.
- **Phase 2 CBOM entries for pilot candidate systems**. Each pilot target needs a detailed CBOM profile: which algorithms are in use, at which protocol layers, with what key sizes, through which libraries, and with what dependencies on external endpoints. Without this data, pilot design is guesswork.

Organizational prerequisites

- **Cryptographic engineering skills — internal or contracted**. Pilot design and execution require hands-on cryptographic engineering capability: configuring hybrid TLS, testing PQC key exchange, validating certificate chains, profiling performance impacts. This is a specialized skill set that most organizations do not have on staff. The skills gap assessment from the Cross-Cutting section should have been addressed by this point — if it hasn't, pilot quality will suffer and timelines will slip.
- **A test environment that mirrors production topology**. Pilots must be tested in environments that include the same middleboxes, load balancers, WAFs, monitoring tools, and partner endpoints as production. A pilot that succeeds in a clean lab environment but fails in production because of an undiscovered middlebox incompatibility is a wasted effort. If a suitable test environment does not exist, building one is a Phase 5 prerequisite that should be budgeted in Phase 4.
- **Documented rollback procedures and authority to execute them**. Before any pilot goes live, the team must have a tested, documented procedure for reverting to the pre-pilot cryptographic configuration — and the organizational authority to execute that rollback without committee approval during a production incident. This means pre-approved change management windows and pre-authorized rollback triggers.
- **Library and platform readiness for PQC algorithms**. The underlying cryptographic libraries (OpenSSL, BoringSSL, Bouncy Castle, platform-native crypto APIs) must support the target PQC algorithms at the required versions. Verify this before committing to pilot targets — discovering mid-pilot that a library upgrade is needed transforms a PQC pilot into a library migration project with different risks and timelines.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

5.1 Select Pilot Targets

Choose 2–4 initial pilots based on:

- **Tier 1 priority** from Phase 3 risk scoring
- **Full organizational control** — you control both endpoints (no external partner dependency for initial pilots)
- **Measurable baseline** — current performance metrics exist for comparison
- **Representative architecture** — pilot results should be generalizable to other similar systems
- **Rollback capability** — must be able to revert to pre-pilot state if issues arise

Recommended starter pilots:

Pilot	Why First	What It Proves
Hybrid TLS on internet-facing web application	Highest HNDL exposure; well-understood protocol; strong ecosystem support	PQC key exchange works at production scale; performance impact is acceptable
Hybrid IPsec/VPN between two controlled sites	High-value internal traffic; both endpoints controlled; clear performance baseline	PQC works for site-to-site encryption; validates VPN concentrator/firewall compatibility
Internal mTLS between microservices	Covers east-west traffic; high-volume; both endpoints controlled	Service mesh PQC capability; validates library compatibility
Certificate lifecycle with shortened validity	Not PQC algorithm change, but critical dependency for PQC readiness	PKI infrastructure can handle increased rotation frequency

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

5.2 Design Hybrid Deployments

Default recommendation for most enterprises: Hybrid ML-KEM-768 + X25519 for TLS key exchange as the initial deployment. In TLS 1.3, this is deployed as the X25519MLKEM768 named group. NIST SP 800-227 discusses the related X-Wing hybrid KEM construct as a general-purpose hybrid approach.

Hybrid cryptography runs classical and post-quantum algorithms together in the same operation. For a TLS handshake, this means combining X25519 (classical ECDH) with ML-KEM-768 (post-quantum key encapsulation). Both algorithms contribute to the shared secret, so the session remains secure as long as at least one algorithm is unbroken.

Why hybrid, not pure PQC:

1. Provides immediate quantum resistance without waiting for universal PQC adoption
2. Can preserve interoperability during phased rollout when the protocol and implementation support negotiating either classical or hybrid modes — though do not assume a hybrid deployment is automatically backward-compatible across every client, middlebox, or peer without testing
3. Reduces deployment risk — protected against both known quantum threats AND unknown weaknesses in new PQC algorithms
4. Proven at large production scale — Chrome/Chromium, Cloudflare, and AWS have all publicly documented production deployments of hybrid ML-KEM-based TLS, with Cloudflare reporting that a majority of human-generated TLS traffic to its network now uses PQC-hybrid key exchange

Hybrid deployment architecture per protocol:

Protocol	Classical Component	PQC Component	Standard/Draft	Production Ready?
TLS 1.3 Key Exchange	X25519	ML-KEM-768	IETF hybrid TLS drafts; deployed as X25519MLKEM768 named group; X-Wing (NIST SP 800-227) is a related general-purpose hybrid KEM construct	Yes — documented in production by Chrome, Cloudflare, AWS
IPsec IKEv2	ECDH P-256	ML-KEM-768	RFC 9370 (hybrid IKEv2)	Yes — available in major VPN products

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

SSH	X25519	ML-KEM-768	OpenSSH 9.9+ (`mlkem768x25519-sha256`; default from OpenSSH 10.0)	Yes — available in current OpenSSH
S/MIME / Email	ECDH P-256	ML-KEM-768	IETF drafts	Limited — not yet broadly deployed
Code Signing	ECDSA P-256	ML-DSA-65	Composite signatures (IETF)	Early — dual-sign approaches available

Cryptographic library readiness — verify before committing to a deployment pattern:

The availability of PQC algorithms varies significantly across cryptographic libraries. Before designing a pilot, verify that your specific library and version supports the algorithms you plan to deploy. As of early 2026, the landscape includes:

- **OpenSSL:** Native ML-KEM, ML-DSA, and SLH-DSA support available since version 3.5 (April 2025). Earlier versions required the external Open Quantum Safe (OQS) provider, which was experimental. Organizations still on OpenSSL 1.1.x face a major upgrade before PQC is available.
- **BoringSSL / Chrome:** ML-KEM implemented in September 2024 and enabled by default in Chrome 131 — the fastest path to large-scale PQC deployment. BoringSSL's hybrid TLS support is the reference implementation for X25519MLKEM768.
- **AWS-LC:** First open-source library to achieve FIPS 140-3 validation with ML-KEM support. Critical for organizations requiring FIPS-validated PQC in AWS or federal environments.
- **Bouncy Castle (Java):** Supported NIST PQC finalists across versions released in 2022–2024, keeping pace with NIST drafts. Mature option for Java-based enterprise applications.
- **wolfSSL:** Full NIST PQC algorithm support aligned with CNSA 2.0 requirements. Strong position for embedded and IoT use cases.
- **Libsodium and MbedTLS:** As of early 2026, PQC integration is limited or still in progress. Projects dependent on these libraries may face delays and should evaluate alternatives or plan for wrappers.

The key implication: library readiness is a hard constraint on migration sequencing. If your application stack depends on a library that does not yet support PQC, the migration

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

path is either (a) upgrade the library, (b) switch to an alternative library, or (c) deploy a PQC-capable gateway or proxy in front of the application as a bridge. Option (c) is often the fastest path for legacy applications.

Decision Point — Hybrid mandate divergence:

For multinational organizations, the hybrid approach debate creates compliance complexity:

- **BSI (Germany), ANSSI (France), Netherlands:** Strongly recommend or require hybrid PQ/traditional schemes (mandatory in some certification contexts)
- **NCSC UK:** Prefers a single migration to pure PQC over intermediate hybrid PKI (but accepts hybrid as interim)
- **NIST:** Permits but does not require hybrid
- **NSA CNSA 2.0:** Accepts hybrid as interim only

Recommendation for multinationals: Adopt hybrid as the default deployment pattern (satisfying the strictest requirement — continental European mandates) with the understanding that hybrid is an interim bridge to PQC-only as the ecosystem matures. This "highest common denominator" strategy satisfies all jurisdictions simultaneously.

5.3 Execute Pilots with Measurement

For each pilot, define and measure:

Performance SLOs (Service Level Objectives):

- Handshake latency: Measure p50, p95, p99 before and after hybrid enablement
- CPU utilization: Server-side and client-side overhead delta
- Connection throughput: Impact on sustained data transfer
- Error rates: Connection failures, negotiation fallbacks, compatibility issues
- Memory utilization: Impact of larger key material and expanded state

Expected performance impacts (based on industry deployments):

- TLS 1.3 hybrid key exchange (e.g., X25519MLKEM768): expect a materially larger ClientHello and roughly ~1 KB of additional key-exchange data per handshake. The real latency impact is path-, MTU-, and middlebox-dependent — treat it as a measurement exercise rather than a fixed millisecond assumption. On modern server hardware, CPU overhead for ML-KEM operations is typically negligible; the dominant factor is packetization and middlebox behavior.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- IPsec hybrid: Similar latency impact; slightly higher CPU due to larger key operations
- Signature verification (ML-DSA): Signatures are significantly larger than ECDSA — ML-DSA-44 signatures are ~2,420 bytes and ML-DSA-65 signatures are ~3,309 bytes, versus ~64 bytes for ECDSA P-256. This is where real infrastructure stress appears.

Rollback criteria: Define explicit triggers for pilot rollback:

- Error rate exceeds X% above baseline
- Latency p99 exceeds Y ms above baseline
- Any security vulnerability identified in PQC implementation
- Interoperability failure with critical downstream system

5.4 Scale from Pilot to Production Through Waves

Wave	Scope	Prerequisite
Wave 0 — Lab/Staging	Isolated test environments only	Pilot design approved
Wave 1 — Internal, Non-Critical	Internal developer tools, monitoring systems, non-critical APIs	Lab validation passed
Wave 2 — Internal, Production	Internal Tier-1 services; east-west traffic	Wave 1 metrics acceptable
Wave 3 — External, Controlled	Partner-facing APIs with cooperative counterparties	Wave 2 stable; partner coordination complete
Wave 4 — External, Broad	Public-facing web applications, customer APIs	Wave 3 stable; ecosystem compatibility validated
Wave 5 — Long Tail	Legacy systems, OT gateways, embedded devices	Vendor support available or containment strategy deployed

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

5.5 Implement Defense-in-Depth Beyond Pure PQC

PQC algorithm migration is necessary but not sufficient. Complement hybrid/PQC deployment with:

- **Tokenization:** Replace sensitive data with tokens where possible, reducing the volume of data that requires cryptographic protection. Tokenization acts as a scope reducer for PQC migration — tokenized data stores eliminate entire categories of HNDL exposure.
- **Data minimization and retention reduction:** Reduce the data protection surface by deleting data that no longer has business value. Every data record you don't store is one you don't need to re-encrypt.
- **Network segmentation:** Limit adversary ability to harvest encrypted traffic by segmenting high-value data flows into isolated network zones with enhanced monitoring.
- **AES-256 as universal symmetric default:** Ensure all symmetric encryption uses AES-256 (Grover-resistant) rather than AES-128. This is a low-effort, high-impact action that eliminates symmetric key vulnerability.
- **Key lifetime reduction:** Shorten certificate and key lifetimes where operationally feasible. A 90-day certificate limits the TNFL window compared to a 2-year certificate.
- **Confidential Computing as complementary protection:** For environments processing highly sensitive data, Confidential Computing (hardware-based Trusted Execution Environments) protects data in use — a gap that PQC alone does not address. PQC protects data in transit; AES-256 protects data at rest; Confidential Computing protects data during processing. Where available (e.g., Intel SGX/TDX, AMD SEV-SNP, ARM CCA), combining PQC transport security with Confidential Computing creates a defense-in-depth posture that is resilient against both quantum and classical platform-compromise threats.
- **Enhanced key wrapping for data at rest:** For archived data already encrypted with quantum-vulnerable key exchange, implement PQC-aware key-wrapping layers. Rather than re-encrypting entire data stores (which may be operationally infeasible for petabyte-scale archives), wrap the existing data encryption keys with PQC key encapsulation. This protects the keys without requiring data re-encryption, significantly reducing the scope of the data-at-rest migration challenge.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Pilot results reports	Performance data (before/after), compatibility findings, issues log, recommendations
Validated migration patterns	Documented, repeatable patterns for TLS, VPN, mTLS, code signing
Wave deployment plan	Sequenced deployment schedule with success criteria per wave
Rollback procedures	Tested rollback capability for each deployment pattern
Defense-in-depth implementation	Tokenization, segmentation, AES-256 defaults deployed as complementary measures

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 5 depends on Phase 3 tier assignments, Phase 4 roadmap and resource plan, Phase 2 CBOM entries for pilot targets, and organizational prerequisites including cryptographic engineering skills, a production-mirror test environment, rollback authority, and library readiness.

Feeds into

- **Phase 6** — Pilot results are the primary input for infrastructure modernization scoping. Each pilot reveals which middleboxes fail, which HSMs need PQC key support, which network paths cannot handle hybrid handshake sizes, and which PKI components require modernization. Without pilot data, Phase 6 planning is based on assumptions rather than evidence.
- **Phase 7** — Pilot findings identify specific vendor gaps: a vendor product that fails hybrid negotiation, a middlebox that drops oversized ClientHello messages, a load balancer that cannot process PQC certificate chains. These findings provide the concrete evidence needed for vendor escalation — far more effective than abstract roadmap requests.
- **Phase 2 (feedback)** — Migration execution updates the CBOM. Each system migrated to hybrid or PQC changes its CBOM entry's migration status, algorithm fields, and compliance posture. Phase 5 is where the CBOM transitions from a discovery artifact to a live operational record.
- **Phase 4 (feedback)** — Pilot results — both successes and failures — generate lessons that change roadmap assumptions for subsequent waves. Actual effort data from Wave 1 should recalibrate effort estimates for Waves 2–N.

Runs in parallel with

- **Phase 6** — Infrastructure modernization and pilot execution are iterative. Pilots reveal infrastructure issues; infrastructure upgrades enable broader pilot scope. These two phases should be staffed and governed as a tightly coupled workstream, not sequential activities.
- **Phase 7** – Vendor engagement intensifies during Phase 5 as pilots generate specific, evidence-based requirements. The feedback loop is: pilot finds vendor gap → vendor engagement escalates → vendor delivers fix → next wave proceeds.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **Phase 6 dependency note**: Phase 5 both feeds into and depends on Phase 6. Early pilots can proceed on systems where existing infrastructure is adequate. Scaled deployment depends on infrastructure readiness. This circular dependency is resolved through the wave structure: Wave 1 pilots use existing infrastructure and generate Phase 6 requirements; later waves depend on Phase 6 delivery.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Piloting the easy systems, not the important ones.** Choosing pilot targets based on convenience (the team that volunteers, the system with the friendliest owner) rather than Phase 3 risk prioritization. Pilots must prove that PQC works on the highest-priority, highest-risk systems — not that it works on a developer sandbox.
- **Skipping rollback planning.** Deploying hybrid/PQC without a tested, documented rollback path. When a pilot causes unexpected failures — and some will — the team must be able to revert within minutes, not hours or days. Define rollback triggers and test the rollback procedure before going live.
- **"Big bang" instead of waves.** Attempting to migrate all Tier-1 systems simultaneously rather than sequencing through controlled waves. Wave-based deployment (lab → internal non-critical → internal production → external controlled → external broad → long tail) allows each wave to validate assumptions and generate lessons for the next.
- **Ignoring library version as a hard constraint.** Designing a pilot for a system whose underlying cryptographic library does not yet support PQC algorithms. Verify library readiness (Section 5.2) before committing to a pilot target — otherwise the pilot becomes a library upgrade project, which has different risks and timelines.
- **Measuring only latency, ignoring compatibility.** Focusing pilot metrics on handshake latency while neglecting compatibility testing with downstream systems, middleboxes, monitoring tools, and partner endpoints. The most common production failures from PQC deployment are compatibility issues, not performance issues.
- **Treating hybrid as the end state.** Hybrid cryptography is a transition mechanism, not a permanent architecture. Organizations that deploy hybrid and declare victory will face a second migration later when hybrid is deprecated or when jurisdictions (NCSC UK, CNSA 2.0) require pure PQC. Plan the hybrid-to-PQC-only transition from the beginning.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No PQC pilots planned or underway
Level 1	Lab testing only; no production exposure
Level 2	2+ production pilots running with measured results; rollback procedures tested; validated patterns documented
Level 3	Tier-1 internet-facing systems on hybrid/PQC; wave rollout underway for Tier-2; defense-in-depth measures (tokenization, AES-256, segmentation) deployed
Level 4	Estate-wide hybrid/PQC deployment substantially complete; transitioning selected systems from hybrid to PQC-only; crypto-agility demonstrated via algorithm-swap drill

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 6 — INFRASTRUCTURE MODERNIZATION & PERFORMANCE

PURPOSE

Modernize the cryptographic infrastructure stack — PKI, HSMs, KMS, network devices, middleboxes — to support PQC operations at production scale. Address the performance, capacity, and compatibility challenges that PQC introduces to real infrastructure.

Phase 6 exists because PQC is not a "drop-in" algorithm swap — it changes the physical characteristics of cryptographic operations in ways that stress real infrastructure. ML-KEM ciphertexts are larger than ECDH key shares. ML-DSA signatures are dramatically larger than ECDSA signatures. Hybrid handshakes combine both, further increasing bandwidth and processing requirements. These changes propagate through every network path, every load balancer, every middlebox, every HSM, and every PKI component. Organizations that skip infrastructure assessment and testing discover these impacts in production — typically as intermittent failures that are difficult to diagnose because they manifest as network timeouts, dropped connections, or certificate validation errors rather than clean cryptographic failures.

Parallelization note

Phase 6 is not a discrete phase that happens after pilots — it runs iteratively alongside Phase 5. Early pilots reveal which infrastructure components need modernization; infrastructure upgrades enable broader and more ambitious pilots. PKI modernization in particular should begin early: reducing certificate lifetimes, testing dual-stack (hybrid) CA issuance, and inventorying HSM PQC capabilities are all activities that can and should start during Phase 1/2 timeframes, because they have long lead times and low risk. HSM

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

procurement alone can take 6–12 months from order to deployment, and root CA ceremonies require extensive planning. Organizations that defer all Phase 6 work until Phase 5 pilots "prove the need" lose a year or more to infrastructure procurement and deployment lead times. Phase 6 also depends heavily on Phase 7 — HSM vendors, PKI vendors, and network equipment vendors must deliver PQC-capable products on timelines that align with the migration roadmap, and vendor slippage directly delays infrastructure modernization.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 5 pilot results identifying infrastructure bottlenecks and compatibility issues.** While some Phase 6 activities can begin proactively (HSM inventory, PKI lifetime reduction), the full scope of infrastructure modernization is informed by pilot findings. Pilots reveal which middleboxes fail, which HSMs lack PQC key types, and which network paths cannot handle hybrid handshake sizes.
- **Phase 4 infrastructure upgrade budget and scheduling.** Infrastructure modernization — particularly HSM replacement and PKI re-architecture — requires significant capital expenditure and long maintenance windows. These must be planned and funded in the Phase 4 roadmap.
- **Phase 1/2 inventory data covering infrastructure-layer cryptography**. The CBOM's Layer 1 (infrastructure) and Layer 2 (platform) entries identify which PKI components, HSMs, KMS instances, and network devices are in scope for modernization.

Organizational prerequisites

- **PKI team capacity and expertise**. PKI modernization is a specialized discipline. Organizations with outsourced or minimally staffed PKI operations will need to augment capacity before undertaking dual-stack CA deployment, root CA planning, or certificate lifetime reduction at scale. PKI errors cause outages — this work must be done carefully.
- **Network architecture documentation and middlebox inventory**. Testing PQC compatibility across network paths requires knowing what sits on those paths. If the organization does not have a current middlebox inventory (firewalls, IDS/IPS, WAFs, DLP, forward proxies, TLS inspection appliances), building one is a Phase 6 prerequisite. This inventory should include firmware versions and vendor support status, as middlebox PQC compatibility often depends on specific firmware releases.
- **HSM vendor engagement (from Phase 7).** HSM PQC capability is vendor-dependent. Before planning HSM modernization, the team needs vendor-confirmed information about which HSM models and firmware versions support PQC key types, and what the upgrade or replacement path looks like. This information comes from Phase 7 vendor engagement and should be requested in Q1 Year 1 — not deferred until Phase 6 begins in earnest.
- **Performance testing infrastructure**. Quantifying PQC's impact on handshake latency, throughput, and bandwidth requires load-testing capability that mirrors production traffic patterns. If the organization lacks a performance testing environment for cryptographic operations, establishing one is an early Phase 6 investment.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

6.1 PKI Modernization

PQC introduces fundamental challenges to PKI infrastructure:

- **Certificate size explosion:** ML-DSA-65 signatures are 3,309 bytes (ML-DSA-44 is 2,420 bytes) versus ~64 bytes for ECDSA. Certificate chains carrying PQC signatures are dramatically larger.
- **Increased chain verification time:** Larger signatures require more processing for chain validation.
- **Middlebox compatibility:** Many network devices (firewalls, IDS/IPS, WAFs, DLP) inspect TLS certificate chains. Larger certificates may exceed buffer sizes or parsing limits.

PKI migration strategy:

1. **Shorten key lifetimes immediately** — Reduce root CA key lifetimes from 20+ years to 10 years; intermediate CAs to 5 years; end-entity to 90–365 days. This limits TNFL exposure and builds organizational muscle for increased rotation frequency.
2. **Deploy dual-stack CA infrastructure** — Operate PQC-capable CA alongside existing classical CA. Issue hybrid/composite certificates for systems that need both. Maintain classical-only certificates for systems not yet ready.
3. **Track Merkle Tree Certificates (MTC) for web PKI** — Google and Cloudflare's MTC initiative (live-testing in Chrome as of early 2026 under the IETF PLANTS working group) addresses the certificate size problem structurally. Instead of sending full PQC signature chains over the wire, the CA signs a Merkle tree head, and the browser receives a compact inclusion proof (often less than 1 KB). This decouples cryptographic strength from bandwidth and integrates Certificate Transparency natively. This approach is still experimental and under active IETF standardization; it is the most promising path for PQC certificate size at web scale, but should not yet be treated as a near-term compliance obligation. Track IETF progress and plan for ecosystem adoption.
4. **Test certificate chain processing** — Before any production deployment, test that all middleboxes (firewalls, WAFs, IDS/IPS, DLP systems, forward proxies) can process PQC certificate chains without failure or truncation.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

6.2 HSM and KMS Modernization

Action	Timeline	Consideration
Inventory all HSMs by model, firmware version, and PQC capability	Immediate	Many HSMs in production cannot support PQC without firmware or hardware upgrade
Upgrade HSM firmware to PQC-capable versions	As available	Thales Luna 7.8.0+ introduced initial PQC support (ML-KEM, ML-DSA); Luna 7.9 (June 2025) adds further PQC capabilities. Utimaco Quantum Protect is available as a new hardware variant (not a firmware upgrade for existing devices — budget for hardware replacement if running older Utimaco models)
Plan HSM hardware replacement where firmware upgrade insufficient	Align to refresh	Budget for 2–4 year replacement cycle
Configure cloud KMS for PQC key types	As available	AWS KMS, Azure Key Vault, Google Cloud KMS — check current PQC support status
Deploy software-based PQC key-wrapping overlay for HSMs not yet upgradeable	Bridge period	Use PQC key-wrapping around classical HSM operations as interim protection

6.3 Network Infrastructure Assessment

PQC impacts network infrastructure in several ways that must be tested before production deployment:

Handshake size impact:

- Classical TLS 1.3 handshake: ~1–2 KB
- Hybrid TLS 1.3 (X25519 + ML-KEM-768): ~2–3 KB (key exchange adds ~1 KB)

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- PQC certificate chain with ML-DSA: Can exceed 10 KB for a 3-certificate chain

Protocol-specific concerns:

Protocol	PQC Challenge	Mitigation
TLS 1.3	Larger ClientHello may fragment; some middleboxes reject oversized handshakes	Test with production middleboxes; verify MTU handling; consider TLS certificate compression
DTLS (UDP)	Larger handshake fragments; amplification concerns	Test fragmentation handling; verify anti-amplification mechanisms
IKEv2/IPsec	Larger IKE_SA_INIT messages; fragmentation across VPN concentrators	Use IKE fragmentation (RFC 7383); test with production VPN devices
QUIC	Designed for larger handshakes; generally more PQC-friendly	Test with production load balancers
Constrained IoT (CoAP, LPWAN)	Extremely limited bandwidth; PQC key sizes may be prohibitive	Consider pre-shared key approaches; gateway-based PQC termination; sector-specific protocols
Satellite / LPWAN	High latency and limited bandwidth exacerbate handshake size impact	Use session resumption aggressively; consider PQC gateway at ground station
Mobile networks	Handshake latency affects user experience; bandwidth constraints on cellular	Test on representative cellular connections; measure impact on connection establishment time

6.4 Performance Testing Methodology

For each system targeted for PQC migration, execute:

1. **Baseline measurement:** Capture current performance metrics (latency p50/p95/p99, CPU utilization, memory, throughput) under representative production load
2. **Lab validation:** Deploy hybrid/PQC in isolated test environment; measure same metrics

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

3. **Canary deployment:** Deploy to 1–5% of production traffic with A/B comparison
4. **SLO evaluation:** Compare canary metrics against defined SLOs from Phase 5
5. **Capacity planning:** If PQC deployment requires additional compute/memory/bandwidth, estimate capacity requirements for full production rollout and include in Phase 4 budget

6.5 Capacity Planning for PQC at Scale

Resource	Expected Impact	Planning Action
CPU	ML-KEM key generation/encapsulation: minimal impact; ML-DSA signature verification: moderate	Benchmark on production hardware; plan for 5–15% server CPU increase for signature-heavy workloads
Memory	Larger key material and expanded TLS session state	Minimal for most systems; test on memory-constrained devices
Network bandwidth	Hybrid handshakes add ~1 KB; PQC certificates add 2–10 KB per connection	Significant for high-volume TLS termination points (CDN edges, load balancers); calculate aggregate bandwidth
Storage	Larger certificates and keys in certificate stores; larger OCSP responses	Manageable; plan for 2–5x increase in certificate storage

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
PKI modernization plan	Dual-stack CA timeline; key lifetime reduction schedule; middlebox test results
HSM/KMS upgrade schedule	All HSMs inventoried with PQC capability status; upgrade/replacement timeline
Network compatibility report	All middleboxes tested with PQC handshakes; issues documented with mitigation
Performance baseline and projections	Before/after measurements for pilot systems; capacity plan for production rollout

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 6 depends on Phase 5 pilot results, Phase 4 budget and scheduling, Phase 1/2 infrastructure-layer inventory data, and organizational prerequisites including PKI team capacity, middlebox inventory, HSM vendor engagement data from Phase 7, and performance testing infrastructure.

Feeds into

- **Phase 5** — Infrastructure readiness gates scaled production deployment. There is no point scheduling Wave 2 or Wave 3 migration if the PKI cannot issue hybrid certificates, the HSMs cannot store PQC keys, or middleboxes on the production path drop PQC traffic. Each Phase 6 deliverable (PKI dual-stack, HSM upgrade, middlebox clearance) unblocks a corresponding set of Phase 5 migration targets.
- **Phase 2 (feedback)** — Infrastructure modernization changes the CBOM. When an HSM is upgraded to support PQC key types, when a PKI root is re-issued with shortened lifetimes, when a middlebox firmware update enables PQC passthrough — these all update the infrastructure-layer CBOM entries and change the organization's overall cryptographic posture.

Runs in parallel with

- **Phase 5** — Infrastructure modernization and pilot execution are tightly coupled and iterative. Pilots reveal infrastructure issues; infrastructure upgrades enable broader pilot scope. This is not a sequential handoff — it is a continuous feedback loop.
- **Phase 7** — HSM, PKI vendor, and network equipment vendor timelines constrain infrastructure upgrade scheduling. Phase 6 execution depends on Phase 7 delivering vendor commitments and product availability. When a vendor misses a delivery milestone, Phase 6 must invoke a bridging strategy rather than simply delaying.

Early-start activities: Some Phase 6 activities should begin well before Phase 5 pilots produce results. HSM inventory (determining which models and firmware versions support PQC) should happen during Phase 1. PKI certificate lifetime reduction (a low-risk, high-value preparatory step) can begin as early as Phase 0/1. HSM procurement orders for models that need hardware replacement should be placed as soon as the inventory identifies the gap — lead times of 6–12 months mean that deferring procurement until "Phase 6 officially starts" adds a year to the migration timeline.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Assuming PQC is a "drop-in" library swap.** The most pervasive misconception. PQC changes key sizes, signature sizes, handshake characteristics, and certificate chain weights. Every network path, middlebox, load balancer, and TLS termination point must be tested — not just the application endpoints. Organizations that skip infrastructure testing discover in production that firewalls drop oversized ClientHello messages, IDS/IPS systems cannot parse PQC certificate chains, or WAF rules break on larger handshake payloads.
- **Ignoring middleboxes.** Firewalls, IDS/IPS, WAFs, DLP systems, forward proxies, and TLS inspection appliances sit on network paths between endpoints. Many have hardcoded buffer sizes or parsing assumptions that break with PQC-sized handshakes and certificates. Test every middlebox on every production network path — this is tedious but essential. Create a middlebox inventory as a sub-deliverable of Phase 6.
- **Deferring HSM upgrades.** HSMs are long-lead-time procurements with complex deployment procedures (key ceremony, compliance validation, high-availability configuration). Organizations that wait until Year 3 to discover their HSMs don't support PQC key types face 12–18 month delays for procurement, delivery, and deployment. Inventory HSM PQC capability in Year 1 and place orders immediately for any that need replacement.
- **Planning PKI modernization as a single event.** PKI changes (new CAs, shorter lifetimes, dual-stack operation) should be phased: start with end-entity certificate lifetime reduction (low risk, high value), then intermediate CA modernization, then root CA planning. Attempting all three simultaneously in a single maintenance window is a recipe for outages.
- **Neglecting capacity planning for high-volume TLS termination.** A CDN edge or load balancer handling millions of TLS handshakes per second will see measurable aggregate bandwidth increase from hybrid handshakes. Model the capacity impact before production deployment, not during.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No awareness of PQC infrastructure impact; no testing
Level 1	Awareness of PKI/HSM/network challenges; no concrete plans
Level 2	HSMs inventoried with PQC status; PKI modernization plan drafted; initial middlebox testing underway
Level 3	HSM upgrades in progress; PKI dual-stack operational; all production middleboxes tested; performance baselines established for Tier-1 systems
Level 4	Infrastructure fully PQC-capable across IT estate; capacity planning validated at production scale; PKI automated with shortened lifetimes; middlebox monitoring integrated into continuous discovery

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PHASE 7 — VENDOR & SUPPLY CHAIN GOVERNANCE

PURPOSE

Ensure third-party products and services support the organization's PQC migration timeline. Vendor dependencies are the single largest external constraint on migration speed. "Our vendors will sort this out" is the most dangerous misconception in quantum readiness — vendors will update on their own timelines unless contractually compelled otherwise.

Phase 7 is numbered last in the framework's logical sequence, but in practice it is one of the first activities that must begin and one of the last to finish. Vendor PQC readiness timelines are typically the longest segment of the migration critical path — longer than internal development, longer than infrastructure procurement, longer than staffing ramp-up. An organization that executes Phases 0–6 flawlessly but defers vendor engagement until Year 3 will discover that it cannot migrate its most critical systems because the underlying vendor products do not yet support PQC. The vendor engagement process (questionnaires, roadmap alignment, contract negotiation, testing) also has its own lead time: 6–18 months from first inquiry to contractual commitment for strategic vendors. Every month of delayed vendor engagement is a month added to the end of the migration timeline.

Parallelization note

Vendor engagement should begin in Q1 Year 1, as soon as the top 10 critical vendor list is available from the Phase 0 scoping assessment — you do not need a finished CBOM or a complete risk scoring to send a PQC roadmap questionnaire to your most important vendors. Phase 7 then runs continuously throughout the program, escalating in intensity as CBOM data (Phase 2), risk scoring (Phase 3), and pilot findings (Phase 5) provide increasingly specific requirements. Vendor governance does not end when migration "completes" — it transitions into a permanent function that monitors vendor

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

cryptographic posture, tracks algorithm deprecation timelines, and ensures ongoing supply chain quantum resilience. This is a permanent BAU function, not a project workstream.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PREREQUISITES

Framework prerequisites (from earlier phases)

- **Phase 0 initial scoping assessment, specifically the top 10 critical vendor list**. The scoping assessment should identify the vendors whose products sit on the critical path for Tier-1 and Tier-2 system migration. This list is the minimum input needed to begin vendor engagement — full CBOM and risk scoring data will refine and expand this list later, but waiting for that data before starting any vendor outreach wastes the program's scarcest resource: time.
- **Phase 1 vendor dependency data from inventory**. As discovery proceeds, the inventory reveals which systems depend on which vendor products for their cryptographic operations. This data feeds directly into the vendor classification matrix (Activity 7.1) and determines engagement urgency.
- **Phase 3 tier assignments determining vendor engagement urgency**. The risk scoring output tells you which vendor dependencies are blocking Tier-1 migration versus those affecting lower-priority systems. This determines where to apply executive-level escalation and contractual leverage versus standard engagement.

Organizational prerequisites

- **Procurement and legal team engagement**. Vendor governance for PQC requires contract modifications: adding PQC roadmap commitments, GA date requirements, testing obligations, and remedies for non-delivery. This requires procurement and legal involvement — security teams cannot unilaterally modify vendor contracts. Engage procurement and legal during Phase 0 and ensure they understand the program's vendor governance requirements before Phase 7 engagement begins in earnest.
- **Executive sponsor willing to escalate with vendor C-suites**. For Strategic Blocking vendors — those whose products are on the critical path and whose PQC timelines do not align with the organization's needs — engagement cannot remain at the technical or account management level. The executive sponsor must be prepared to escalate to vendor C-suite leadership, invoke contractual leverage, and if necessary authorize evaluation of alternative products. Without this executive backing, vendor engagement produces polite conversations and vague roadmap commitments that never materialize.
- **A structured vendor assessment methodology**. The organization needs a repeatable process for evaluating vendor PQC readiness: questionnaires, scoring criteria, tracking systems, and escalation triggers. Ad hoc inquiries produce inconsistent data and make it impossible to compare vendor readiness across the portfolio. The framework provides a classification matrix and questionnaire structure (Activities 7.1–7.2), but the organization must designate staff to operate this process.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **Awareness that open-source dependencies require the same governance discipline**. Many organizations focus vendor governance exclusively on commercial vendors while neglecting the open-source cryptographic libraries (OpenSSL, BoringSSL, Bouncy Castle, libsodium, language-specific crypto packages) that underpin their custom applications. These libraries have their own release cycles, PQC support timelines, and breaking change risks. The vendor governance process must include open-source dependency tracking with the same rigor applied to commercial vendors.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ACTIVITIES

7.1 Classify Vendor Portfolio by PQC Impact

Category	Criteria	Action
Strategic Blocking	Vendor product is in the critical path for Tier-1/2 migration; no PQC support = migration stops	Immediate engagement; executive-level escalation; contract leverage; parallel evaluation of alternatives
Strategic Enabling	Vendor product is PQC-relevant but alternatives exist or migration is not blocked	Standard engagement; require PQC roadmap; include in contract renewals
Non-Critical	Vendor product handles no quantum-vulnerable cryptography or protects only low-priority data	Monitor; include PQC in standard procurement language for renewals

7.2 Execute Vendor Engagement

For each strategic vendor, obtain:

1. **PQC feature matrix:** Which products support which PQC algorithms; current vs. planned
2. **GA version and dates:** When PQC support will be generally available (not beta, not "coming soon")
3. **Interoperability guidance:** Tested configurations with common counterparties
4. **Performance data:** Vendor's own benchmark data for PQC operation
5. **Fallback behavior:** What happens when a PQC negotiation fails (graceful degradation to classical, or hard failure?)
6. **CBOM data:** Cryptographic bill of materials for the vendor's product

Vendor PQC Readiness Questionnaire (core questions):

1. Which NIST-standardized PQC algorithms (ML-KEM, ML-DSA, SLH-DSA) does your product currently support?
2. For algorithms not yet supported: what is the GA date and version?
3. Does your product support hybrid/composite operation (classical + PQC simultaneously)?

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

4. Can cryptographic algorithms be changed via configuration without recompilation, reinstallation, or hardware replacement?
5. What is the performance impact of PQC operation (provide benchmark data)?
6. What testing have you done for interoperability with common ecosystem counterparties?
7. Will you provide CBOM data for your product in CycloneDX format?
8. What is your commitment timeline for FIPS 140-3 validated PQC implementations?

7.3 Insert PQC Requirements into Procurement

For all new purchases and contract renewals:

Add the following clause (adapt to legal counsel's preferred language):

"Supplier warrants that the Product/Service supports NIST-approved post-quantum cryptographic algorithms (FIPS 203, 204, and/or 205 as applicable) and provides crypto-agility (algorithm changes via configuration, not requiring recompilation or hardware replacement). Supplier will provide GA timelines, performance guidance, and interoperability matrices for PQC features. Failure to deliver PQC capability by [date] enables remedies up to and including [maintenance credits / right to replace / contract termination]."

For RFP requirements, add:

- Mandatory: NIST-standardized PQC algorithm support with published GA date
- Mandatory: Crypto-agility — algorithm selection via configuration
- Preferred: Hybrid operation support (classical + PQC)
- Preferred: CBOM data provided in CycloneDX format
- Required: FIPS 140-3 validation timeline for PQC implementations

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

7.4 Manage Vendor-as-Blocker Scenarios

When a critical vendor cannot provide PQC support within your migration timeline:

1. **Deploy bridging patterns:** Software PQC overlay (gateway TLS termination, PQC key-wrapping around classical HSM, double-encryption layer) until native vendor support arrives.
2. **Run champion-challenger:** Evaluate an alternative vendor through POC while maintaining the incumbent. Communicate the POC to the incumbent vendor as leverage.
3. **Escalate contractually:** Invoke SLA remedies, maintenance credit provisions, or right-to-replace clauses.
4. **Accept and document risk:** If no alternative exists and no bridge is feasible, formally document the residual risk in the risk register with SteerCo approval and a re-evaluation trigger date.

7.5 Establish Ongoing Vendor Governance

Activity	Cadence
Track vendor PQC roadmap status	Monthly (for strategic blocking vendors); Quarterly (for others)
Verify vendor GA commitments against actuals	At each committed milestone date
Update vendor PQC scorecard	Quarterly
Report vendor status to SteerCo	Monthly
Re-evaluate vendor classification (strategic blocking / enabling / non-critical)	Semi-annually

Vendor KPI board (report to SteerCo):

- % of strategic vendors with signed PQC commitments and dates
- Number of products with GA hybrid/PQC capability in your estate
- Age of oldest unsupported critical product (days since vendor committed and missed)
- Number of bridging patterns deployed (indicates vendor gaps being compensated)

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

OUTPUTS

Output	Quality Criteria
Vendor PQC readiness register	All strategic vendors assessed; GA dates recorded; blockers identified
Updated procurement requirements	PQC clauses in standard RFP templates and contract language
Vendor questionnaire responses	Documented responses from all strategic blocking vendors
Bridging pattern deployments	Deployed and documented for all vendor-blocked Tier-1/2 systems
Vendor governance cadence	Operating rhythm established with monthly/quarterly reviews

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

INTERDEPENDENCIES

Backward dependencies

See Prerequisites above. Phase 7 depends on Phase 0 scoping assessment (top 10 vendor list), Phase 1 vendor dependency data, Phase 3 tier assignments, and organizational prerequisites including procurement/legal engagement, executive escalation willingness, and a structured assessment methodology.

Feeds into

- **Phase 5** — Vendor GA releases gate production migration for vendor-dependent systems. A system cannot be migrated to PQC if the underlying vendor product does not yet support PQC algorithms. Each vendor GA delivery unblocks a set of Phase 5 migration targets.
- **Phase 6** — HSM, KMS, PKI, and network equipment vendor timelines constrain infrastructure upgrade scheduling. Phase 6 cannot upgrade an HSM that the vendor hasn't delivered PQC firmware for, or deploy a PKI platform whose vendor hasn't shipped PQC certificate support.
- **Phase 4 (feedback)** — Vendor timeline updates — both accelerations and delays — require roadmap revisions. A Strategic Blocking vendor that slips its GA date by 12 months changes the critical path for every system that depends on that product. The roadmap must model these vendor dependencies explicitly so that timeline changes propagate to affected milestones automatically.

Runs throughout the program: Vendor engagement is not a discrete phase with a start and end date. It begins in Q1 Year 1 with the initial top-10 vendor questionnaires and continues as a permanent governance function. As the program matures, vendor governance transitions from "getting commitments" to "verifying delivery," "testing interoperability," and eventually "monitoring ongoing vendor cryptographic posture" as part of business-as-usual supply chain risk management.

Escalating intensity over time: Early vendor engagement (Year 1) is primarily information-gathering: questionnaires, roadmap requests, classification. Mid-program engagement (Years 2–3) shifts to contractual commitment, testing, and escalation for non-delivery. Late-program engagement (Years 4+) focuses on verifying delivery, eliminating bridging patterns, and integrating vendor PQC support into standard procurement and renewal processes.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

COMMON FAILURES

- **Starting vendor engagement too late.** The vendor dependency is typically the longest segment of the PQC migration critical path. Organizations that defer formal vendor engagement until after the CBOM is "complete" lose 12–24 months. Begin vendor engagement in Q1 Year 1 using the top 10 vendor list from Phase 0 scoping — you do not need a finished CBOM to send a PQC roadmap questionnaire.
- **Accepting verbal commitments without contractual backing.** A vendor sales engineer saying "PQC is on our roadmap" is not a commitment. Insist on written GA dates, specific product versions, and contractual consequences for missed dates. Verbal assurances evaporate when vendor priorities shift.
- **Treating all vendors equally.** The vendor landscape should be triaged by criticality (Strategic Blocking / Strategic Enabling / Non-Critical). Applying the same engagement intensity to all vendors wastes resources. Focus executive-level engagement and contractual leverage on the 5–10 Strategic Blocking vendors that constrain your migration timeline.
- **No bridging strategy for vendor gaps.** When a critical vendor cannot deliver PQC on your timeline, the response cannot be "wait and hope." Define bridging patterns (PQC gateway, overlay encryption, proxy-based TLS termination) proactively so they can be deployed immediately when a vendor misses a milestone.
- **The vendor delegation trap.** Assuming that because a vendor controls the cryptographic implementation, the vendor also owns the migration risk. The vendor owns their product; the organization owns the risk to its data, operations, and regulatory compliance. Vendor readiness is a dependency to manage, not a responsibility to delegate.
- **Ignoring open-source dependencies.** Many organizations track commercial vendor PQC readiness but neglect open-source components (OpenSSL, Bouncy Castle, language-specific crypto libraries) that underpin their custom applications. These require the same tracking discipline — monitor release schedules, test upgrades, and plan for version transitions.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY INDICATORS

Level	Indicator
Level 0	No vendor engagement on PQC; assumption that "vendors will sort it out"
Level 1	Ad-hoc inquiries to a few vendors; no structured tracking
Level 2	Top 10 vendors formally engaged; questionnaires sent; responses tracked; vendor criticality classification complete
Level 3	PQC in standard procurement language; contracts include dated commitments and remedies; bridging patterns deployed for blocked systems; vendor scorecard reported to SteerCo
Level 4	All strategic vendors PQC-committed with verified delivery; bridging patterns eliminated as vendor support matures; open-source dependency tracking operational; vendor governance is permanent BAU function

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

PROGRAM FOUNDATIONS: CAPABILITIES THAT SPAN EVERY PHASE

The eight phases above describe *what* the program does and in *what order*. But several capabilities do not belong to any single phase — they operate continuously across the entire program lifecycle, shaping how every phase is executed, measured, and governed. These foundations are not optional supporting material. A program that executes the phases without building these capabilities will produce a migration that cannot be measured, cannot be sustained, cannot be staffed, and cannot satisfy regulators.

This section covers five foundational capabilities: a maturity model for benchmarking progress, metrics and KPIs for tracking and reporting, crypto-agility as the program's architectural end-state, regulatory and standards alignment for compliance mapping, and the skills and team structures needed to execute the work. Each should be established early — ideally during Phase 0 and Phase 1 — and maintained throughout the program's lifetime.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

MATURITY LEVELS

Level	Name	Description
0	**Unaware**	No organizational awareness of quantum cryptographic risk; no activities planned or underway
1	**Aware**	Quantum risk acknowledged at leadership level; initial education conducted; no formal program
2	**Initiated**	Formal program chartered; budget allocated; discovery underway; initial CBOM in development
3	**Progressing**	CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported
4	**Advanced**	Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured
5	**Optimized**	Estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational

Assessment Across Seven Domains

Domain	Level 1	Level 2	Level 3	Level 4	Level 5
Cryptographic Inventory	Awareness that inventory is needed	Partial inventory of known systems	≥70% Tier-1 coverage; automated discovery deployed	≥90% coverage; continuous monitoring; IT+OT+cloud	Real-time posture management; auto-alerting on drift
Governance & Ownership	Informal awareness	Charter exists; QRPM appointed	SteerCo operational; RACI defined; budget committed	Multi-year governance; integrated into risk register	Quantum readiness part of BAU enterprise governance

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Pilots & Deployment	No pilots	Lab testing only	2+ production pilots with measured results	Tier-1 systems on hybrid/PQC; wave rollout underway	Estate-wide deployment; transitioning to PQC-only
Vendor & Supply Chain	No vendor engagement	Ad-hoc inquiries	Top 10 vendors formally engaged; questionnaires sent	PQC in procurement; contracts include clauses; blockers managed	All strategic vendors PQC-committed; bridging patterns eliminated
Compliance & Standards	Unaware of requirements	Regulatory landscape mapped	Compliance gaps identified; remediation planned	Meeting current deadlines; evidence documented	Proactive compliance; contributing to standards development
Crypto-Agility	Hardcoded algorithms throughout	Awareness of agility need	Abstraction layers in new development	Algorithm swap via config for Tier-1 systems; automated cert lifecycle	Organization-wide agility; algorithm changes are routine operations
Risk & Prioritization	No quantum risk assessment	Basic awareness of HNDL/TNFL	Formal risk scoring; prioritized backlog	QRA updated quarterly; migration tracking against backlog	Continuous risk posture management; automated re-scoring

Self-Assessment Scoring

For each domain, score 0–5. Overall maturity level is the lowest individual domain score (the weakest domain constrains overall readiness).

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Target maturity timeline:

- End of Year 1: Level 2 across all domains
- End of Year 2: Level 3 across all domains
- End of Year 3: Level 4 across at least 5 of 7 domains
- End of Year 5: Level 4 or 5 across all domains

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

METRICS, KPIS & REPORTING

Board-Level KPI Pack (Report Quarterly)

KPI	What It Measures	Target
Coverage	% of Tier-1 endpoints using hybrid/PQC key exchange	Year 1: 10%; Year 2: 60%; Year 3: 95%
Trust	# of PKI/signing anchors with shortened lifetimes and/or PQC capability	Year 1: Root CAs assessed; Year 2: Intermediates shortened; Year 3: End-entity automated
Inventory	% of RSA/ECC locations mapped and risk-ranked in CBOM	Year 1: 70% Tier-1; Year 2: 90% all tiers; Year 3: continuous
Vendors	% of strategic suppliers with dated PQC commitments	Year 1: 50%; Year 2: 80%; Year 3: 95%
Agility	% of services that can swap key-agreement algorithm via configuration within 2 weeks	Year 1: baseline; Year 2: 30%; Year 3: 60%

Operational KPIs (Report Monthly to SteerCo)

KPI	Measurement
Migration tasks completed vs. plan	Earned value / planned value (by workstream)
Pilot performance delta	p95 latency increase vs. baseline (target: <2ms for TLS)
Discovery gap closure	% of Phase 1 gap register items resolved
Vendor milestone adherence	% of vendor GA commitments met on time
Policy compliance	% of new deployments passing PQC CI/CD check
Training coverage	% of target staff completing PQC training modules

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Evidence Dossier (for Audit and Regulatory)

Maintain a continuously updated evidence package:

- CBOM snapshots (quarterly)
- Pilot test reports with SLO data
- Vendor questionnaire responses and commitment letters
- Updated cryptographic and procurement policies
- SteerCo meeting minutes and decision records
- Training completion records
- Risk register with quantum risk entry and mitigation status

---

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

CRYPTO-AGILITY AS END-STATE ARCHITECTURE

Why Crypto-Agility, Not Just PQC

PQC algorithms will eventually need replacement too. Cryptographic algorithms have limited lifespans — SHA-1, MD5, DES, 3DES, SSL, and early TLS all fell to attacks or obsolescence. Organizations that hardcoded these algorithms faced expensive emergency migrations. The goal of PQC migration is not merely to swap RSA for ML-KEM; it is to build the organizational capability to change cryptographic algorithms routinely.

Marin's Law on Crypto-Agility: *"The effort required to change cryptography in a system is inversely proportional to the agility built into that system from the start."* Formally: **$Y \approx K / A$**, where Y is the migration effort, K is the complexity of the cryptographic estate, and A is the agility level. Systems designed for agility make algorithm changes through configuration updates and rolling deployments. Systems without agility require code rewrites, application rebuilds, and architectural redesigns.

Crypto-Agility Architecture Principles

1. **No direct algorithm calls in application code.** Applications use cryptographic providers or adapters that abstract algorithm selection. Examples: Java Cryptography Architecture (JCA) with configurable providers, OpenSSL with pluggable engines, cloud KMS APIs that abstract underlying algorithms.
2. **Algorithm selection is configuration-driven.** A policy file, environment variable, or central configuration service determines which algorithms are used. Changing from X25519 to ML-KEM-768 is a configuration change, not a code change.
3. **Dual-stack capability during transition.** Systems can negotiate both classical and PQC algorithms simultaneously (hybrid mode) and gracefully degrade if the counterparty doesn't support PQC.
4. **Automated certificate and key lifecycle management.** Certificate issuance, renewal, rotation, and revocation are fully automated. Manual certificate management at scale is incompatible with the agility requirement.
5. **Algorithm changes are tested in CI/CD.** Cryptographic configuration changes follow the same deployment pipeline as code changes: tested in staging, canary-deployed, monitored, and rollback-capable.
6. **Monitoring of cryptographic posture.** Continuous monitoring detects algorithm drift, expired configurations, and non-compliant deployments. Alerts fire when a system negotiates a deprecated algorithm.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Crypto-Agility OKRs

Objective	Key Result
Algorithm changes don't require code changes	100% of Tier-1 services use provider-pattern cryptography by Year 3
Certificate rotation is fully automated	Mean time to rotate end-entity certificate <1 hour; zero manual steps
Algorithm swap can be executed within 2 weeks	Demonstrated via drill: swap negotiated algorithm for Tier-1 service from hybrid to PQC-only within 10 business days
Cryptographic posture is continuously monitored	100% of Tier-1 endpoints reporting negotiated algorithms to monitoring system

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

REGULATORY & STANDARDS ALIGNMENT MAP

Mapping Framework Phases to Regulatory Requirements

Regulation / Standard	Relevant Phase(s)	What It Requires	Framework Output That Satisfies It
PCI DSS v4.0 Req 12.3.3	Phase 1, 2	Documentation and annual review of cryptographic cipher suites and protocols in use (purpose and location); a full CBOM is the recommended best practice for satisfying this requirement in PQC programs	CBOM; QRA; migration roadmap
NIST IR 8547 (Initial Public Draft)	All	Deprecate quantum-vulnerable public-key algorithms after 2030; disallow after 2035	Full migration execution per roadmap
NIST SP 1800-38 (NCCoE, Preliminary Draft)	Phase 1, 5, 6	Discovery methodology and interoperability/performance testing patterns from the NCCoE Migration to PQC project	Discovery results; pilot reports; compatibility testing
NSA CNSA 2.0	Phase 5, 6, 7	NSS acquisitions CNSA 2.0 compliant by 2027; networking equipment by 2030; web/cloud/OS by 2033; all NSS by 2035	Procurement requirements; vendor compliance verification
EU NIS2 / DORA / CRA	Phase 0, 1, 4	Risk management measures proportionate to risk; supply chain security; incident response	Governance structure; CBOM; vendor governance; evidence dossier
NCSC UK Timelines	Phase 1, 3, 5	Discovery by 2028; high-priority migration by 2031; complete by 2035	Phase 1 complete by 2028; Phase 5 Tier-1/2 by 2031

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ASD (Australia)	All	PQC transition plan by 2026; critical systems migrating by 2028; all Australian Government systems by 2030	Most aggressive timeline — requires immediate action on all phases
OMB M-23-02 (US Federal)	Phase 1, 4	Prioritized inventory of CRQC-vulnerable cryptographic systems with annual updates through 2035; annual funding assessments for migration	Prioritized inventory / CBOM; annual updates; progress reporting

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

SKILLS & TEAM STRUCTURE

Core Roles

Role	Skills Required	Source
Quantum Readiness Program Manager	Program/project management; stakeholder management; risk governance; basic crypto literacy	Internal senior PM with PQC training
Cryptographic Architect	Deep cryptography expertise; PKI architecture; protocol design; PQC algorithm knowledge	Internal security architect + specialized training; rare external hires
Security Engineer (PQC)	TLS/SSH/IPsec configuration; HSM management; certificate lifecycle; library evaluation	Internal security engineers with PQC training modules
Application Security Lead	Code review; SAST/DAST tooling; library management; CI/CD pipeline integration	Internal AppSec team with crypto-agility focus
OT Security Specialist	ICS/SCADA knowledge; OT network architecture; safety case management; vendor coordination	Specialized hire or partner; very scarce skillset
Vendor/Procurement Lead	Contract negotiation; RFP management; vendor relationship management; SLA design	Internal procurement with PQC requirements training

Training Approach

1. **Executive education** (1 day): Quantum threat, business case, governance responsibilities — for SteerCo, board, and senior leadership
2. **PQC foundations** (3–5 days): Algorithm overview, hybrid deployment, CBOM, risk assessment — for all workstream participants
3. **Deep technical** (ongoing): Hands-on lab exercises with hybrid TLS deployment, HSM configuration, CBOM generation — for security engineers and architects

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

4. **Crypto champion program:** Designate one "crypto champion" per platform/application team who serves as the workstream's liaison and knowledge bridge

---

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

SECTOR ADAPTATION NOTES

The core methodology above applies universally. The following notes identify sector-specific constraints and priorities:

FINANCIAL SERVICES (PAYMENTS, BANKING)

- **Highest HNDL urgency:** Cross-border payment flows (SWIFT, correspondent banking) carry data with very long confidentiality requirements
- **Regulatory pressure:** PCI DSS v4.0 Req 12.3.3 (effective March 31, 2025) requires documentation and annual review of cryptographic cipher suites and protocols in use — effectively mandating cryptographic inventory for PCI-scoped entities; G7 Cyber Expert Group roadmap (January 2026); Europol QSFF prioritization framework; BIS Papers No. 158
- **Unique complexity:** Interbank payment systems involve ~320 cryptographic function calls for a single mobile banking session; cross-border payments involve 9+ parties and 30,000+ unique cryptographic functions
- **HSM dependency:** Payment HSMs (Thales payShield, Utimaco Atalla) have specific PQC upgrade timelines that constrain migration
- **Priority:** Key exchange on external-facing payment APIs; HSM-protected key material; SWIFT interface cryptography

TELECOMMUNICATIONS

- **Scale:** 5G networks involve cryptography at every layer from radio (5G-AKA) to core (service mesh, IMS, lawful intercept)
- **GSMA guidance:** The GSMA Post-Quantum Telco Network Task Force published the PQ.01–PQ.07 series — PQ.01 (impact assessment), PQ.02 (risk management), PQ.03 v2.0 (migration guidelines with Gantt charts for VPN, TLS, PKI, and MACsec migration, including CBOM guidance and crypto-agility methodology), and PQ.07 (non-terrestrial networks). This is the most operationally detailed sector-specific PQC guidance available.
- **Unique constraints:** Roaming interfaces, lawful intercept, non-terrestrial networks (satellite, HAPS), massive IoT device populations
- **Vendor concentration:** Small number of infrastructure vendors (Ericsson, Nokia, Huawei) control cryptographic implementations across the network core

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

- **Priority:** Backhaul encryption (site-to-site); 5G core service mesh; SIM/eSIM key management

CRITICAL INFRASTRUCTURE / OT

- **Longest asset lifecycles:** OT systems (SCADA, PLCs, RTUs) often have 15–25 year lifecycles with no update mechanism
- **Safety constraints:** Any change to OT cryptography must go through safety case re-certification in many jurisdictions
- **Minimal guidance:** CISA's October 2024 OT PQC guidance and RAND's 2023 study are essentially the only available frameworks
- **TNFL priority:** Firmware signing and safety certificate integrity are the primary quantum risks in OT — a forged firmware signature could compromise physical safety
- **Priority:** Gateway-based PQC termination at OT/IT boundary; firmware signing migration; long-term plan for device refresh

GOVERNMENT & DEFENSE

- **CNSA 2.0 compliance:** Mandatory and aggressively timed — 2027 for new NSS acquisitions, 2030 for software/firmware signing and networking equipment (VPNs/routers), 2033 for web/cloud/OS platforms, 2035 for all remaining NSS including custom and legacy systems. Note: SLH-DSA is not part of CNSA 2.0; ML-DSA-87 is the designated general CNSA 2.0 signature algorithm, with LMS/XMSS permitted for specific applications.
- **Classification constraints:** Working with classified systems adds complexity for testing and deployment
- **FedRAMP/FIPS requirements:** PQC implementations in US federal and defense systems must use FIPS 140-3 validated cryptographic modules. AWS-LC's FIPS module was the first publicly available FIPS 140-3 validated implementation to include ML-KEM support. Other validated modules from Thales, Utimaco, and others are expected to follow.
- **Priority:** Comply with CNSA 2.0 milestones; ensure PQC-capable products in procurement pipeline

---

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDICES

The appendices provide quick-reference tools, decision aids, and templates that support the framework's phases without interrupting the methodology narrative. They are designed to be printed, bookmarked, or extracted for use in workshops, steering committee meetings, and vendor engagements. Where an appendix relates to a specific phase, the relevant phase text includes a cross-reference — but the appendices are also usable as standalone reference cards for practitioners who are already familiar with the framework.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDIX A: ALGORITHM QUICK REFERENCE

NIST Standard	Algorithm	Type	Primary Use	Key/Signature Size	Notes
FIPS 203	**ML-KEM-768** (formerly CRYSTALS-Kyber)	Lattice-based KEM	Key exchange (TLS, VPN, SSH)	Public key: 1,184 bytes; Ciphertext: 1,088 bytes	Default recommendation for hybrid TLS (with X25519). ML-KEM-512 for constrained environments (IoT, embedded devices with limited RAM — ML-KEM-768 requires ~18 KB heap on typical MCUs); ML-KEM-1024 for highest security. On modern server hardware, performance overhead is negligible; on constrained devices, test memory and latency impact before selecting parameter set.
FIPS 204	**ML-DSA-65** (formerly CRYSTALS-Dilithium)	Lattice-based signature	Digital signatures (PKI, code signing, document signing)	Public key: 1,952 bytes; Signature: 3,309 bytes	Default recommendation for most signature use cases. ML-DSA-44 for constrained; ML-DSA-87 for highest security.
FIPS 205	**SLH-DSA** (formerly SPHINCS+)	Hash-based signature	Digital signatures (conservative choice)	Varies widely by parameter set	Stateless hash-based; no lattice assumptions. Larger signatures but different security foundation. Recommended as backup/alternative if lattice cryptanalysis advances.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Pending standardization (NIST):

- **FN-DSA (formerly FALCON):** Draft FIPS 206. Compact lattice-based signatures suitable for bandwidth-constrained environments, though it requires complex floating-point arithmetic to implement safely. Expected to complement ML-DSA for use cases where signature size is critical.
- **HQC:** Selected by NIST in March 2025 as an additional KEM to standardize, providing a non-lattice-based alternative to ML-KEM. Worth tracking as a diversification option even though it is not yet a final NIST standard.

Already standardized (NIST Special Publication):

- **HBS (LMS/XMSS):** NIST SP 800-208 (finalized October 2020). Stateful hash-based signature schemes approved for specific use cases such as firmware and software update signing, where cryptographic state can be managed safely. These are intended for niche, tightly controlled use cases rather than as general-purpose replacements for ML-DSA or SLH-DSA.

Regional variations:

- **BSI (Germany):** Recommends hybrid schemes with ML-KEM as primary; acknowledges FrodoKEM and Classic McEliece as having undergone extensive cryptanalysis (but does not elevate them to equal co-recommendations with ML-KEM)
- **South Korea (KpqC):** Sovereign algorithms SMAUG-T, NTRU+, HAETAE, AIMer (January 2025 final selections)

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDIX B: DECISION TREE — "WHERE DO I START?"

If you have done nothing yet: → Go to Phase 0. Secure executive mandate and budget. Nothing else works without this.

If you have budget but no inventory: → Go to Phase 1. Deploy automated discovery on your top 20 systems. Simultaneously begin Phase 2 CBOM structure design.

If you have an inventory but no migration plan: → Go to Phase 3. Score and prioritize your inventory. Then Phase 4 for roadmap.

If you have a plan but no pilots: → Go to Phase 5. Select your first hybrid TLS pilot on an internet-facing system you fully control.

If you have pilots running but infrastructure isn't ready to scale: → Go to Phase 6. Assess PKI, HSM, and network device readiness.

If you're blocked on vendors: → Go to Phase 7. Classify vendors by criticality, engage formally, deploy bridging patterns.

If you don't know where you stand: → Run the Maturity Model self-assessment (Cross-Cutting section). Your weakest domain tells you where to focus.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDIX C: MOSCA'S INEQUALITY — THE DECISION FRAMEWORK

Mosca's Theorem provides the mathematical framework for migration urgency:

If X + Y > Z, you must act now.

Where:

- **X** = Security shelf-life: the number of years the data you are protecting must remain confidential
- **Y** = Migration time: the number of years required to migrate your cryptographic infrastructure to quantum-safe
- **Z** = Threat timeline: the number of years until a cryptanalytically relevant quantum computer (CRQC) exists

Practical application:

- If your data needs 15 years of confidentiality (X=15) and migration takes 5 years (Y=5), then X+Y=20. If CRQC arrives in 15 years (Z=15), you are already 5 years too late.
- The PQCC roadmap distinguishes between "urgent adopters" (X+Y>Z) and "regular adopters" (X+Y≤Z) using this inequality.
- For HNDL-exposed data, X is the data's remaining confidentiality requirement. For TNFL-exposed signatures, X is the remaining validity period of the trust anchor.

The uncomfortable reality: For most large enterprises, Y (migration time) is 4–15 years. For sensitive data with long-lived confidentiality requirements, X (shelf-life) is 10–20 years. Most credible CRQC estimates place Z at 10–20 years. The math is uncomfortably tight, and it gets worse with every year of delay.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDIX D: HYBRID APPROACH JURISDICTIONAL COMPLIANCE MATRIX

Jurisdiction	Hybrid Position	Implication for Practitioners
BSI (Germany)	**Strongly recommended** for all PQC KEMs and signatures (except standalone hash-based signatures). Mandated in BSI certification ("visa") contexts.	Hybrid should be the default design assumption in German-facing deployments
ANSSI (France)	**Strongly emphasized** in the short and medium term; Phase 2 of ANSSI's timeline keeps hybrid mandatory for long-term-security claims in ANSSI's visa framework	Hybrid is the safer default for French assurance-sensitive products
Netherlands (AIVD/CWI/TNO)	**Recommended** in the PQC Migration Handbook, especially hybrid-AND internally; this is guidance, not a legal mandate	Strong guidance toward hybrid, with explicit policy for exceptions
NCSC UK	Prefers a **single migration to fully post-quantum PKI** rather than an intermediate hybrid PKI; acknowledges hybrid as an acceptable interim measure for confidentiality and interoperability	Use hybrid selectively, especially for key exchange / confidentiality; do not treat hybrid as the UK end-state
NIST (US)	Hybrid key establishment is **allowed but not required**; SP 800-227 discusses X-Wing as an example of a general-purpose hybrid KEM	Flexibility to choose hybrid or pure PQC depending on the system
NSA CNSA 2.0	**Accepted as interim** only	Hybrid acceptable during transition; end-state must be CNSA 2.0 compliant (pure PQC)
ASD (Australia)	**Not recommended, but not prohibited**	Pure PQC preferred in the long term; hybrid used only where interoperability or resiliency justifies it

Multinational recommendation: Deploy hybrid as the default deployment pattern. This satisfies the strictest requirements (continental European agency guidance), preserves interoperability during transition, and provides defense-in-depth against unknown PQC algorithm weaknesses. Plan the architecture for eventual transition to pure PQC to satisfy NCSC UK preferences and CNSA 2.0 end-state requirements. This single approach satisfies all jurisdictions simultaneously.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

APPENDIX E: QUICK-REFERENCE CHECKLISTS

90-Day Quick Start Checklist

1. ☐ Executive sponsor identified and committed
2. ☐ QRPM appointed
3. ☐ SteerCo convened; charter published; RACI defined
4. ☐ Multi-year budget (minimum 3 years) approved or in approval process
5. ☐ Top 20 critical systems identified (Phase 0 scoping)
6. ☐ Cryptographic discovery tool selected and procurement initiated
7. ☐ Quantum risk added to enterprise risk register
8. ☐ Cryptographic policy updated to include PQC-approved cipher suites
9. ☐ Procurement policy updated to require PQC roadmaps from vendors
10. ☐ Training cohort (10–20 people) enrolled in PQC fundamentals
11. ☐ First 2 hybrid pilot targets selected
12. ☐ Vendor questionnaires sent to top 10 strategic vendors
13. ☐ KPI baseline values established; Q+1 targets set
14. ☐ Board briefing delivered and documented

Quarterly Board Report Template

- **Overall maturity level:** [0–5] with trend arrow
- **Coverage KPI:** X% of Tier-1 endpoints on hybrid/PQC (target: Y%)
- **Inventory KPI:** X% of estate mapped in CBOM (target: Y%)
- **Vendor KPI:** X% of strategic vendors with dated PQC commitments (target: Y%)
- **Trust KPI:** X PKI/signing anchors shortened/rotated this quarter
- **Key risks:** [Top 3 risks with mitigation status]
- **Key decisions required:** [Any SteerCo escalations needing board input]
- **Budget status:** On track / Variance [±X%]
- **Next quarter milestones:** [3–5 concrete deliverables]

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ABOUT THIS VERSION

This framework is a living document, versioned and updated as standards evolve, vendor products mature, regulatory deadlines shift, and practitioner experience accumulates across real migration programs. The current version reflects the state of the PQC landscape as of March 2026.

CURRENCY OF TECHNICAL REFERENCES

Vendor capabilities, HSM firmware versions, MTC/PLANTS standardization status, and tool categories cited throughout this framework reflect the market as of the publication date. The PQC vendor and standards landscape evolves rapidly — readers should verify current GA dates, FIPS 140-3 validation status, and product capabilities against original vendor sources or PostQuantum.com, which tracks these changes continuously.

STANDARDS IN PROGRESS

NIST IR 8547 (Initial Public Draft, November 2024; final expected 2025–2026) sets the deprecation and disallowance timelines referenced throughout this framework. Federal agencies and their contractors should reference the final published version — and the application-specific guidance it supersedes (SP 800-52 for TLS, SP 800-77 for IPsec, SP 800-175B for general cryptographic standards) — as these documents are updated. Similarly, CNSA 2.0 milestone dates, ETSI technical reports, and sector-specific regulatory guidance (PCI DSS, DORA, GSMA PQ series) may be updated between framework versions.

ENGAGEMENT

For questions, advisory engagement, or sector-specific framework adaptation, contact Marin Ivezic via PostQuantum.com or AppliedQuantum.com. Organizations seeking structured support for any framework phase — from executive business case development through migration execution — can engage Applied Quantum's advisory practice directly at appliedquantum.com.

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles — including regional and global leadership positions — at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators — including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com

© 2026 Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.