Axiom Sovereign
TECHNOLOGY SOVEREIGNTY ADVISORY

EXECUTIVE & PRACTITIONER GUIDE — ORGANIZATIONS WITH LONG-LIVED SENSITIVE DATA

Post-Quantum Cryptography: What to Do Now

NIST FIPS 203-205 · Harvest-Now-Decrypt-Later Risk · 3-Phase Migration Roadmap

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

Post-Quantum Cryptography: What to Do Now

About This Guide

This guide provides business and technical decision-makers with a plain-language explanation of the post-quantum cryptography (PQC) transition, the NIST FIPS 203-205 standards, the harvest-now-decrypt-later (HNDL) threat, and a practical three-phase migration roadmap for organizations that hold long-lived sensitive data. It is designed to be read by executives and technical staff alike — the threat context is written for leadership, and the implementation guidance is written for practitioners.

Post-quantum cryptography is not a future problem for most professional services organizations that handle long-lived sensitive data. The harvest-now-decrypt-later threat model means that adversaries — primarily nation-state actors — are collecting encrypted data today with the intent to decrypt it once cryptographically-relevant quantum computers become available. For healthcare records, legal matter files, tax records, and financial data that must remain confidential for 10 or more years, that risk is present right now.

Who Should Read This Guide

Read now and act: Federal government contractors, defense contractors handling CUI or ITAR data, healthcare organizations with long-term patient records, law firms with matters spanning multiple years, and any organization subject to emerging PQC procurement requirements.

Read now and plan: CPA firms with multi-year tax records, financial services organizations, NGOs with internationally sensitive programs, and any organization considering new technology investments that will have a 7+ year lifecycle.

Monitor and track: General small businesses with standard data types and no government contracting obligations. Begin tracking PQC developments and include PQC readiness in vendor procurement criteria now.

How to Use This Guide

This guide is structured in four sections. Read them in sequence — each builds on the previous one. Section 1 explains the threat. Section 2 explains the NIST standards. Section 3 provides the migration roadmap. Section 4 identifies your urgency level based on your organization type.

Read Section 1 to understand the threat: The harvest-now-decrypt-later threat is conceptually simple but its implications are significant. Understanding why this matters for your specific data types is the foundation for making the right investment decisions.

Read Section 2 to understand the standards: NIST FIPS 203, 204, and 205 are the official PQC standards. You do not need to understand the mathematics — but you do need to understand which algorithms replace which existing cryptographic functions, and what "post-quantum ready" means from a procurement perspective.

Use Section 3 as your migration framework: The three-phase roadmap gives you a sequenced approach: discover what cryptography you have first, then plan your migration, then execute. Start with Phase 1 regardless of your urgency level — you cannot migrate what you have not inventoried.

Use Section 4 to determine your timeline: The urgency matrix maps your organization type to a recommended action timeline. Use this to set expectations with leadership and establish your migration program budget.

SECTION 1: THE THREAT — WHY THIS MATTERS NOW

Understanding Post-Quantum Cryptography

The encryption that protects your data today — RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange — relies on mathematical problems that classical computers cannot solve in practical time. A classical computer would need billions of years to factor a 2048-bit RSA key. A sufficiently powerful quantum computer, using Shor's algorithm, could factor the same key in hours or minutes.

Quantum computers powerful enough to break today's encryption — often called cryptographically relevant quantum computers (CRQCs) — do not yet exist at scale. The most widely cited estimate places this capability in the 2029–2035 timeframe, though some security agencies have used more conservative estimates. However — and this is critical — you do not need quantum computers to exist today for the threat to be real today.

The Harvest-Now, Decrypt-Later Threat

The harvest-now, decrypt-later (HNDL) attack strategy is straightforward: intercept and store encrypted data today, then decrypt it when quantum capability becomes available. This strategy is viable because: (1) network traffic and encrypted data can be collected at scale with existing technology, (2) storage costs are near zero, and (3) the adversary does not need to decrypt the data immediately — they just need it to still be valuable when they can decrypt it.

Nation-state actors — particularly China, Russia, and Iran — are assessed by the intelligence community to be collecting encrypted data today with the explicit intent of future decryption. The U.S. government's response — OMB M-23-02, NSA CNSA 2.0 Suite, and the NSA's directive to begin migrating national security systems to PQC — reflects a serious assessment of this threat as real and present, not theoretical.

What Does This Mean for Your Organization?

The HNDL threat has immediate practical implications for any organization that holds data that must remain confidential for a decade or more. Consider:

- **Healthcare organizations:** Patient records, clinical trial data, and genomic data are subject to 6–10 year (or longer) retention requirements. Data encrypted today with RSA or ECC that is harvested and stored by an adversary could be decrypted and exposed within a decade.
- **Law firms:** Legally privileged communications and matter files spanning years or decades represent extremely high-value targets. The perpetual nature of attorney-client privilege means the value of this data does not decrease over time — making it a priority HNDL target.
- **CPA and accounting firms:** Multi-year tax records, audit workpapers, and financial planning documents contain sensitive financial data for individuals and entities. Tax data is often retained 7+ years by statute.
- **Federal contractors:** Controlled Unclassified Information (CUI) and technical data covered by ITAR/EAR represent high-priority HNDL targets for foreign intelligence services. OMB M-23-02 and emerging CMMC requirements create near-term compliance obligations.

SECTION 2: THE STANDARDS — NIST FIPS 203, 204, AND 205

NIST Background and Selection Process

The National Institute of Standards and Technology (NIST) initiated a public process in 2016 to evaluate and standardize post-quantum cryptographic algorithms. Over a six-year evaluation period involving cryptographers from around the world, NIST evaluated 69 candidate algorithms across multiple rounds of analysis. In August 2024, NIST published the first three post-quantum cryptographic standards: FIPS 203, FIPS 204, and FIPS 205.

These three standards replace the asymmetric cryptographic algorithms currently in widest use for securing communications and authenticating digital signatures. Symmetric encryption (AES) and hash functions (SHA-256 and above) are not broken by quantum computers using known algorithms — only asymmetric cryptography requires migration.

Standard	Algorithm Name	Purpose	What It Replaces	Key Characteristics
FIPS 203	ML-KEM (Kyber)	Key Encapsulation Mechanism (KEM) — establishes shared encryption keys between parties over an insecure channel.	RSA, Diffie-Hellman key exchange, Elliptic-Curve Diffie-Hellman (ECDH)	Lattice-based. Selected as primary KEM. Widely implemented in TLS, VPNs, and key exchange protocols.
FIPS 204	ML-DSA (Dilithium)	Digital Signatures — verifies the authenticity and integrity of messages, documents, and code.	RSA signatures, ECDSA (P-256, P-384)	Lattice-based. Recommended primary signature algorithm. Broader deployment expected for code signing, TLS certificates.
FIPS 205	SLH-DSA (SPHINCS+)	Digital Signatures — alternative hash-based signature scheme.	RSA signatures, ECDSA (backup/alternative option)	Hash-based. Conservative security assumptions. Larger signature sizes. Recommended as backup when lattice-based signatures face algorithm-specific concerns.

What "PQC-Ready" Means in Practice

When evaluating vendors and technology for PQC readiness, the following questions are the right ones to ask:

- Has the vendor integrated FIPS 203 (ML-KEM) into their TLS implementation and key exchange protocols?
- Does the vendor offer PQC-ready certificates for their TLS connections?
- Can the vendor provide a PQC migration roadmap and timeline?
- Does the vendor support hybrid mode (PQC alongside classical algorithms) during the transition period?
- Is the vendor's PQC implementation using the NIST-approved final standards (not draft versions)?

SECTION 3: THE MIGRATION ROADMAP — THREE PHASES

PQC migration is not a single project — it is a multi-year program. The three-phase approach below is designed to be sequenced and phased appropriately: you cannot plan migration without first completing discovery, and you cannot execute migration without a tested plan. Begin Phase 1 immediately regardless of your organization type.

PHASE 1: DISCOVER — CRYPTOGRAPHIC ASSET INVENTORY (MONTHS 1–3)

You cannot migrate what you have not inventoried. Phase 1 is the foundation of your entire PQC migration program. Many organizations discover during this phase that they have significantly more cryptographic exposure than they anticipated — particularly through third-party vendor dependencies and legacy systems.

Identify All Systems Using Asymmetric Cryptography

Map every system that uses RSA, ECC, or Diffie-Hellman. This includes: TLS/SSL certificates (every website, web application, API, and cloud service), VPN encryption, email encryption (S/MIME, PGP), document signing systems, code signing certificates, PKI infrastructure, database encryption key management, and hardware security modules (HSMs).

Document Algorithm and Key Sizes

For each system identified, document the specific algorithm and key size in use: RSA-2048, RSA-4096, P-256, P-384, etc. Systems using RSA-2048 or smaller and elliptic curves below P-384 are highest priority for migration. Systems using AES-256 for symmetric encryption are quantum-resistant and do not require migration.

Identify Long-Lived Data and High-Risk Systems

Cross-reference your cryptographic inventory against your data classification. Which encrypted data must remain confidential beyond 2033? These systems and their key management infrastructure are your highest-priority migration targets. Government contractor systems handling CUI or ITAR data may have hard deadlines established by contract or regulation.

Assess Vendor Dependency

Identify which systems' cryptography is controlled by you vs. by your vendors. A vendor who controls the encryption for a system you depend on must migrate that system — you cannot migrate it yourself. Begin vendor conversations now. For new procurements, include PQC readiness as a selection criterion.

PHASE 2: PLAN AND PILOT — MIGRATION ARCHITECTURE DESIGN (MONTHS 4–9)

Phase 2 translates your cryptographic inventory into a prioritized migration plan and tests PQC implementations before production deployment. Hybrid mode — running PQC algorithms alongside classical algorithms simultaneously — is the standard recommended approach for the transition period.

Prioritize Systems by Risk

Classify each system from Phase 1 by migration priority. Tier 1 (highest priority): government contract systems, systems handling long-lived sensitive data subject to HNDL risk, key management infrastructure. Tier 2: customer-facing TLS connections, VPN infrastructure. Tier 3: internal systems with shorter data lifecycles.

Design Hybrid Transition Architecture

For Tier 1 and Tier 2 systems, plan for hybrid mode — implementing PQC alongside classical algorithms until ecosystem support is broad enough to migrate fully. This maintains backward compatibility with systems that do not yet support PQC while providing quantum-resistant protection for connections that do.

Test PQC Implementations in Non-Production Environments

Performance implications of PQC algorithms vary. ML-KEM has minimal performance impact relative to ECDH. ML-DSA signatures are larger than classical signatures, which may impact applications with signature size constraints. Test in staging before production deployment and document performance characteristics.

Update Procurement Requirements

Require PQC readiness evidence in all new technology procurement: RFP language should require vendors to provide a PQC migration roadmap and timeline, confirm support for FIPS 203-205, and indicate when hybrid PQC mode will be available.

PHASE 3: IMPLEMENT AND SUSTAIN — PRODUCTION MIGRATION (MONTHS 10–24+)

Phase 3 is ongoing. The pace of production migration is constrained by vendor support, ecosystem readiness, and available change windows. The goal is continuous progress with highest-priority systems migrated first, and a recurring review cycle that monitors both your own progress and the evolving threat landscape.

Migrate Highest-Priority Systems First

Begin with Tier 1 systems identified in Phase 2. For each system, follow your test plan from Phase 2, implement hybrid PQC mode, document implementation evidence, and verify that the PQC component is actually being used in production connections.

Update TLS Configurations

As browser and client ecosystem support for ML-KEM expands (Chrome and Firefox already support hybrid TLS with Kyber), configure your web servers and APIs to prefer PQC key exchange. Monitor server logs to verify PQC is being negotiated for compatible connections.

Rotate Long-Lived Certificates and Keys

As PQC-compatible certificate authorities and HSMs become available, migrate your certificate infrastructure to PQC signatures. Prioritize certificates covering systems that handle Tier 1 data. Maintain documentation of migration completion for each certificate and key.

Establish Cryptographic Agility as an Architecture Principle

The most important long-term lesson of PQC migration is cryptographic agility — the ability to change cryptographic algorithms without re-architecting systems. Incorporate this principle into your development standards and procurement criteria: new systems should be designed to support algorithm replacement without major rework.

SECTION 4: URGENCY MATRIX — WHEN SHOULD YOUR ORGANIZATION ACT?

The following matrix maps organization type to migration urgency. Use this to set expectations with leadership, establish program timelines, and prioritize budget requests.

Organization Type	Migration Urgency	Primary Driver	Recommended Action
Federal contractors handling CUI or ITAR/EAR data	IMMEDIATE (Act Now)	OMB M-23-02 mandates PQC inventory. CMMC and contract requirements expected to follow.	Begin Phase 1 cryptographic inventory now. Budget for Phase 2 in current fiscal year.
Defense contractors (NATSEC systems)	IMMEDIATE (Act Now)	NSA CNSA 2.0 Suite mandates PQC transition timeline for National Security Systems.	Initiate formal PQC program. Assign program owner. Engage PQC-specialist support.
Healthcare organizations with long-term records (hospitals, practices)	HIGH (Within 6 months)	HNDL risk on long-lived PHI. HHS anticipated to address PQC in future HIPAA updates.	Begin Phase 1. Include PQC in HHS regulatory monitoring. Update vendor contracts.
Law firms with multi-year matter files	HIGH (Within 6 months)	Perpetual attorney-client privilege makes legal data a high-value HNDL target.	Conduct Phase 1. Assess document management and email encryption. Update procurement.
CPA and accounting firms (multi-year tax records)	MEDIUM (Within 12 months)	Long retention requirements (7+ years) create HNDL exposure for financial data.	Begin Phase 1. Include PQC readiness in next technology refresh cycle.
Financial services organizations	MEDIUM (Within 12 months)	SEC, FFIEC, and NY DFS anticipated to issue PQC guidance. SWIFT is evaluating PQC.	Begin Phase 1. Monitor regulatory developments. Update vendor procurement criteria.
NGOs with sensitive international programs	MEDIUM (Within 12 months)	Geopolitical sensitivity of program data makes NGO records HNDL targets for state actors.	Conduct Phase 1. Assess cloud provider PQC roadmaps. Engage donors on requirements.
General SMB without government contracts or long-lived sensitive data	LOW (Monitor and Plan)	Limited HNDL exposure. Supply chain requirements from clients will emerge.	Monitor developments. Include PQC in 5-year technology roadmap. Track vendor readiness.

PQC Readiness Assessment

Axiom Sovereign conducts post-quantum cryptography readiness assessments for professional services firms and government contractors. Our engagement begins with a complete cryptographic asset inventory (Phase 1) and delivers a prioritized migration roadmap, vendor assessment scorecard, and procurement language for PQC requirements. We work with your existing IT team or managed service provider to implement PQC controls.

Schedule a PQC readiness consultation: calendly.com/cmissimore-6zkc/30min

Email: info@axiomsovereign.com · **Web:** axiomsovereign.com