AXIOM RESEARCH INSTITUTE

Publication Series: Emerging Technology Governance

Post-Quantum Cryptography and the Governance Imperative

A Foundational Framework for Organizational Readiness in the Post-NIST Era

KEY FINDINGS

01 NIST finalized FIPS 203/204/205 in Aug 2024 — the standards gap is closed; the governance gap is not

02 Harvest Now, Decrypt Later is an active collection operation, not a projected threat

03 PQC migration fails at the governance layer: no owner, no inventory, no vendor mandate

04 HIPAA, SEC, and CMMC create quantifiable financial exposure from delayed migration

05 The 2030 deprecation deadline requires organizations to begin governance decisions now

Document ARI-2026-001 | Published May 2026 | axiomresearch.institute

About the Axiom Research Institute

The Axiom Research Institute is the independent research and publications division of Axiom Sovereign LLC, a fractional vCISO and GRC consulting firm. The Institute publishes primary research on post-quantum cryptography governance, AI privacy compliance, space cybersecurity, and emerging technology risk management. All publications are grounded in primary regulatory and standards sources and are designed to support practitioners, legal counsel, and executive leadership in navigating complex governance challenges.

About Axiom Sovereign

Axiom Sovereign LLC provides fractional vCISO services, GRC program design and assessment, vendor privacy risk analysis, and AI governance advisory for mid-market organizations in regulated sectors. Principal: Cory Missimore, CISSP, CISM, CISA, CIPP/E, CIPP/US, CIPM, AIGP.

How to Use This Paper

This is a foundational publication. It establishes the Institute's analytical framework and primary source grounding for this topic. Subsequent publications in the series address specific implementation domains and can be used independently or in conjunction with this paper. Implementation guides, assessment instruments, and templates derived from this paper are published separately and reference this document.

Document Number	ARI-2026-001
Publication Series	Emerging Technology Governance
Published	May 2026
Version	1.0 — Initial Release
Suggested Citation	Axiom Research Institute. (2026). Post-Quantum Cryptography and the Governance Imperative (ARI-2026-001). A
Distribution	Public — Unrestricted
License	CC BY-NC 4.0 — Non-commercial with attribution

Disclaimer

EXECUTIVE SUMMARY

01

The standards gap is closed. The governance gap is not.

NIST published FIPS 203, 204, and 205 in August 2024 — the first federally standardized post-quantum cryptographic algorithms. That event removed the last credible rationale for organizational inaction. The gap that remains is organizational: no executive owner, no completed inventory, no vendor commitments, no board engagement.

02

Harvest Now, Decrypt Later is an active threat, not a projected one.

NSA's CNSA 2.0 advisory stated in 2022 that adversaries are "currently harvesting encrypted data." Data transmitted under RSA or ECC encryption in prior years is potentially archived. Migration protects future transmissions. It does not protect data already collected.

03

Regulatory retention requirements define the HNDL exposure window.

HIPAA's Privacy Rule requires six-year retention of policies and procedures (45 CFR 164.530(j)); state law and CMS requirements typically govern clinical record retention at six to ten years. SEC Rule 17a-4 mandates three to six years for financial records. CUI under CMMC carries indefinite sensitivity obligations. Organizations should confirm their specific retention obligations with legal counsel — but the point holds regardless of the precise timeframe: the harvest window is already open. Regulated data transmitted today will still be a viable decryption target years from now.

04

Migration fails at the governance layer, not the technical layer.

The algorithms, the guidance, and the timelines are all published. What is missing in most organizations is the accountability structure: an executive sponsor, a funded program, vendor engagement with contract authority, and board reporting that creates accountability. The decision to begin is an organizational decision, not a technical one.

05

Three decisions need to be made at the executive level before any technical work begins.

Who owns the migration program with budget authority? What is the cryptographic inventory scope? Which vendors need to be formally assessed? This paper establishes the framework for answering those questions. Organizations ready to begin may contact Axiom Sovereign at axiomsovereign.com for practitioner support.

SECTION 1

The Threat Is Not Future-Tense

1.1 The Wrong Question

Organizations approaching post-quantum cryptography for the first time almost always start with the same question: when will a cryptographically relevant quantum computer exist? The question is understandable. It is also the wrong starting point.

The threat that requires action today does not require a quantum computer today. It requires only that adversaries collect encrypted traffic now and decrypt it later — when quantum processing reaches the required threshold. This attack model, documented by NSA and CISA under the name Harvest Now, Decrypt Later (HNDL), describes a collection operation that is technically simple and strategically rational. Encrypted traffic is captured. It is stored. It waits.

> NSA's 2022 CNSA 2.0 advisory stated plainly: "NSA is concerned that adversaries are currently harvesting encrypted data with the expectation that they will eventually be able to decrypt it with a quantum computer." That language — "currently harvesting" — is present tense and intentional. It describes an active operation, not a projected one.

The practical consequence is asymmetric. An organization that completes PQC migration in 2029 has protected all data transmitted after that date. It has not protected data transmitted in 2021, 2022, 2023, 2024, 2025, 2026, 2027, or 2028. The harvest window has been open for years. Migration closes it going forward. It does not close it retroactively.

1.2 Which Data Is Actually at Risk

HNDL risk is not uniform. It is calibrated by the length of time data remains sensitive. Routine operational data, short-lived commercial communications, and time-bounded transactional records carry limited exposure. Data that remains sensitive for years is directly in scope.

Regulatory retention requirements define that exposure with reasonable precision. HIPAA's Privacy Rule requires covered entities to retain documentation of their policies and procedures for six years (45 CFR 164.530(j)); state law and CMS Conditions of Participation govern clinical medical record retention, with most states requiring six to ten years. Organizations should work with qualified legal counsel to determine the specific retention obligations applicable to their record categories and jurisdictions. Health data transmitted under RSA-2048 in 2022 will remain a regulated record — and a viable intelligence target — for years beyond transmission under virtually any applicable framework.

SEC Rule 17a-4 requires broker-dealers to retain transaction records for three to six years. CUI handled by CMMC-regulated contractors carries sensitivity that does not expire on a fixed schedule, because defense-related technical data and acquisition-sensitive information retain operational value for as long as the programs they support remain active.

> These are not abstractions. They are the actual data categories that state-sponsored actors with quantum-decryption capability would prioritize. The retention requirements that create compliance obligations also define the HNDL exposure window.

1.3 The Technical Vulnerability Is Specific

RSA and Elliptic Curve Cryptography underpin TLS key exchange, PKI certificate infrastructure, VPN authentication, code signing, email encryption, and document signing. Both families derive their security from mathematical problems — integer factorization and discrete logarithm — that classical computers cannot solve efficiently but that Shor's algorithm, running on a sufficiently powerful quantum computer, can solve in polynomial time.

Symmetric cryptography — AES-256 and SHA-384 — is not equivalently vulnerable. Grover's algorithm provides a quadratic speedup against symmetric key search, effectively halving key strength. AES-256 retains approximately 128 bits of effective security against a quantum attacker, which is sufficient under current standards. AES-128's effective security drops to approximately 64 bits, approaching the boundary of acceptability; NIST guidance recommends migrating AES-128 deployments to AES-256.

The practical inventory of quantum-vulnerable components concentrates in three places: key exchange mechanisms in TLS and VPN infrastructure; digital signature implementations in PKI, code signing, and email security; and certificate infrastructure where CA signing keys using RSA or ECC propagate quantum vulnerability through the entire trust chain.

SECTION 2

What the Standards Actually Require

2.1 FIPS 203, 204, and 205

The three August 2024 publications each address a different cryptographic function and are not interchangeable.

FIPS 203 standardizes ML-KEM (derived from CRYSTALS-Kyber) for key encapsulation, replacing RSA and ECDH in key exchange contexts including TLS and VPNs. Three parameter sets apply: ML-KEM-512, ML-KEM-768, and ML-KEM-1024, corresponding to NIST security levels 1, 3, and 5.

FIPS 204 standardizes ML-DSA (derived from CRYSTALS-Dilithium) for digital signatures, replacing RSA and ECDSA in PKI certificate issuance, code signing, and document authentication. Three parameter sets: ML-DSA-44, ML-DSA-65, ML-DSA-87.

FIPS 205 standardizes SLH-DSA (derived from SPHINCS+) as a hash-based backup signature algorithm for contexts where lattice-based security assumptions are considered insufficient.

FIPS 206, standardizing FN-DSA (derived from FALCON), followed in subsequent months and provides a lattice-based signature option with smaller signature sizes than ML-DSA, relevant for bandwidth-constrained deployments.

2.2 NIST IR 8547: The Deprecation Timeline

NIST IR 8547 (2024) is the primary migration roadmap. RSA and ECC key exchange and signature algorithms are designated for deprecation by 2030 for federal use. "Legacy use allowed" through 2030 means continued use with approved key lengths is currently permissible but not indefinitely. For organizations outside the federal sector, IR 8547 increasingly functions as the professional standard against which auditors and regulators will measure compliance.

2.3 NSA CNSA 2.0

The NSA's CNSA 2.0 advisory establishes algorithm requirements for National Security Systems and publishes the timeline that defense industrial base contractors should treat as authoritative: CNSA 2.0 adoption for software and firmware to begin no later than 2025, with full adoption targeted by 2030. For CMMC-regulated contractors, CNSA 2.0 is not a background reference — it is the standard against which DoD evaluates cryptographic posture.

2.4 The 2023 Joint Advisory

The August 2023 joint advisory from CISA, NSA, and NIST — "Quantum-Readiness: Migration to Post-Quantum Cryptography" — establishes that organizations should begin immediately, independent of quantum computing timeline projections. It identifies cryptographic discovery as the foundational prerequisite and explicitly addresses supply chain risk: organizations cannot assume vendor readiness.

> The advisory is public. Its recommendations are specific. Organizations that have not acted on them are not unaware. They are ungoverned.

2.5 The International Regulatory Dimension: ASD and the LATICE Framework

NIST and NSA are not the only authoritative sources establishing migration timelines. Australia's Signals Directorate (ASD), through the Australian Cyber Security Centre (ACSC), published updated PQC guidance in September 2025 that establishes three hard milestones: a refined PQC transition plan by end of 2026, commencement of migration for critical systems by end of 2028, and full transition completion by end of 2030. ASD recommends organizations cease using traditional asymmetric cryptography by 2030 and mandates ML-KEM-1024 as the replacement encryption standard.

The ASD guidance introduces the LATICE framework — a structured five-phase approach to PQC migration: **L**ocate (build a CBOM identifying all uses of traditional asymmetric cryptography), **A**ssess (evaluate the sensitivity and value of systems and data protected by vulnerable algorithms), **T**riage (prioritize systems for transition based on risk and data longevity), **I**mplement (deploy post-quantum algorithms following updated ISM guidelines), and **C**ommunicate (coordinate vendors, internal teams, and stakeholders). LATICE is significant not merely as Australian guidance but as an international governance framework that operationalizes the same principles as NIST's approach in a structured, auditable form.

MAS, Singapore's Monetary Authority, issued a quantum advisory to financial institutions in February 2024 encouraging awareness of quantum threats and vendor engagement on quantum-safe roadmaps. MAS subsequently completed a cross-border PQC experiment with Banque de France in November 2024 and a QKD sandbox with major Singapore banks in September 2025. These developments signal that quantum readiness is becoming a regulatory expectation in major financial centers beyond the US — reinforcing the position that organizations with international operations or international data flows face quantum governance obligations from multiple regulatory directions simultaneously.

SECTION 3

Why Migration Fails Before It Starts

3.1 The Accountability Problem

In 2026, most mid-market organizations outside the defense industrial base have not completed a cryptographic inventory. They have not asked their vendors about PQC timelines. Their boards have not seen a quantum risk briefing. The standards, the advisory, and the threat documentation have been available for years.

This is a governance failure with a specific anatomy. Technical awareness concentrated in a security team does not become an organizational program without accountability structures: an executive owner with budget authority, a board line item, a vendor engagement mandate with contract authority, and a reporting cadence that creates accountability. None of these structures is created by publishing a NIST standard.

> The pattern is consistent. The security team circulates the joint advisory. It gets read by security staff and filed. A CISO briefing note reaches the CTO. The CTO agrees it's important. Nothing is funded. Nobody is assigned. The migration does not start. This is not a failure of technical capacity. It is a failure of governance.

3.2 The Inventory Deficit and the CBOM

Without a cryptographic inventory, migration has no starting point, no scope, and no vendor engagement target list. Most organizations lack a complete inventory for structural reasons. Cryptographic dependencies are not co-located: TLS configurations exist at the network perimeter, in application middleware, in internal service-to-service communications, and in API integrations. PKI dependencies reach every system that validates certificates. Key management infrastructure may be distributed across on-premises HSMs, cloud KMS services, and vendor-managed systems.

The industry has developed a structured answer to the inventory problem: the Cryptographic Bill of Materials (CBOM). Developed by IBM Research and standardized in CycloneDX 1.6 (released April 2024, formalized as ECMA-424 in July 2024), a CBOM is a machine-readable inventory of all cryptographic assets in a system — algorithms, key types, key lengths, certificates, protocols, and their dependencies. NIST's National Cybersecurity Center of Excellence references CBOM creation in its PQC migration drafts (NIST SP 1800-38B). Australia's ASD explicitly identifies CBOM creation as the first deliverable of the LATICE framework's Locate phase.

> Just as SBOMs (Software Bills of Materials) became the standard for software supply chain security following Executive Order 14028, CBOMs are becoming the compliance baseline for cryptographic supply chain visibility. Organizations that cannot produce a CBOM cannot demonstrate cryptographic inventory to auditors, regulators, or enterprise procurement teams asking about PQC readiness.

Discovery methodology varies by category: automated scanning for perimeter and application-layer components, manual review for key management and code signing, vendor documentation for embedded and third-party components. An inventory that covers some categories and not others provides a false sense of completion. The CBOM format provides the standardized output structure that makes the inventory actionable rather than merely descriptive.

3.3 The Vendor Dependency Gap

An internal cryptographic inventory that stops at the organizational boundary is incomplete. Cloud KMS implementations, identity platform vendors, PKI certificate authorities, and VPN vendors each have their own PQC migration timelines — timelines that may or may not align with the organization's requirements.

> An organization that completes its internal migration on schedule but has not engaged its identity platform vendor, which is still running ECDSA-signed certificates with an undocumented PQC roadmap, is not migrated. Its migration timeline is bounded by its slowest critical-path vendor.

3.4 The Board Engagement Gap

Boards that have not been briefed on quantum risk cannot authorize migration programs. Migration programs without authorization are not funded. The financial exposure is quantifiable: HIPAA civil monetary penalties for willful neglect reach $2 million per violation category per year; SEC cybersecurity disclosure rules require public companies to disclose material cybersecurity risks; CMMC disqualification removes organizations from DoD contracting. These numbers belong in board briefing materials, not only in technical security documentation.

SECTION 4

The Governance-First Migration Framework

4.1 Accountability Assignment

PQC migration is not an IT project and should not be owned exclusively by the CISO or IT organization. The migration touches procurement, legal, finance, and operations. A single-function owner is a single point of failure. Effective accountability structures define three roles: an executive sponsor with budget authority, a program owner who manages execution and vendor engagement, and a board reporting owner who prepares quarterly progress briefings. Quantum risk reporting should be a standing board agenda item, not a one-time briefing.

4.2 Two-Phase Cryptographic Inventory

Phase One maps the full scope of quantum-vulnerable algorithm use. Inventory categories: network perimeter (TLS, VPN, certificate validation), application layer (inter-service authentication, API cryptography, application PKI), key management (HSMs, cloud KMS, on-premises key stores), code and firmware (signing pipelines, embedded cryptography), and data at rest (encrypted storage and key management dependencies). Discovery methodology varies: automated scanning for perimeter and application-layer components, manual review for key management and code signing, vendor documentation for embedded and third-party components.

Phase Two converts the technical ledger into a risk-prioritized migration queue using three variables: data sensitivity and retention horizon, regulatory obligation and enforcement consequence, and vendor dependency timeline. Output: a sequenced work order with each target carrying a risk score, regulatory mapping, and vendor dependency flag.

4.3 Vendor Engagement Program

Initial assessment deploys the PQC readiness questionnaire covering algorithm inventory, migration roadmap documentation, crypto-agility posture, and contractual representations. Ongoing monitoring tracks critical-path vendors — identity providers, cloud KMS, PKI certificate authorities — at quarterly intervals minimum. Contract integration embeds FIPS 203/204/205 support milestones, notification requirements for roadmap changes, and algorithm implementation representations into new and renewing agreements.

4.4 Board Briefing Structure

Board briefings follow the structure of any material risk disclosure: the risk, the financial exposure, the current organizational state, and the decision required. The risk is stated plainly. Financial exposure is quantified by data category and regulatory framework. Current state is reported against the migration

roadmap with specific metrics: percentage of inventory completed, vendors assessed, milestones achieved versus planned. The decision required is resource authorization.

SECTION 5

Implementation Sequencing

Governance decisions precede technical execution. The following sequencing assumes a mid-market organization beginning the program in 2026.

Phase	Timeframe	Key Actions
Foundation	**Months 1–3**	Governance accountability assignment. Executive sponsor designation. Board briefing — initial risk
Inventory & Prioritizatio	**Months 4–6**	Phase One completion. Phase Two risk prioritization. Vendor questionnaire deployment to all ident
Initial Execution	**Months 7–12**	Migration of highest-priority systems. Vendor contract integration for new and renewing agreement
Systematic Migration	**2027–2028**	Phased migration through prioritized inventory. Crypto-agility requirements in all new deployments.
Completion	**2029–2030**	Full migration aligned to NIST IR 8547 deprecation timelines and NSA CNSA 2.0 targets. Legacy a

SECTION 6

Sector-Specific Observations

6.1 Healthcare and HIPAA-Covered Entities

The HIPAA intersection with HNDL risk is acute for covered entities and business associates. HIPAA's Security Rule (45 CFR Part 164) requires technical safeguards protecting ePHI in transit. OCR enforcement has consistently referenced NIST cryptographic guidance as the standard of care. An assertion that RSA-2048 satisfies the Security Rule's encryption requirement — made after NIST has published post-quantum alternatives and after agencies have publicly documented HNDL collection operations targeting healthcare — is defensible in 2026. It becomes progressively less defensible as the 2030 deprecation deadline approaches. Healthcare organizations should treat HNDL exposure of ePHI transmission systems as a current compliance question.

6.2 Defense Industrial Base

DIB contractors face the clearest regulatory pressure. NSA CNSA 2.0 is mandatory for National Security Systems, and DoD acquisition policy is moving toward CNSA 2.0 requirements in contractor systems handling CUI. CMMC 2.0 Level 2 contractors should note that SC.L2-3.13.8 (cryptographic mechanisms for transmission) and SC.L2-3.13.10 (key establishment and management) are the controls through which PQC migration requirements will be evaluated during C3PAO assessments. DIB contractors who have not incorporated PQC migration into their System Security Plans are carrying compliance risk that will appear in assessments.

6.3 Financial Services

SEC cybersecurity disclosure rules (2023) require public companies to disclose material cybersecurity risks. Quantum risk — specifically HNDL exposure of historically transmitted financial records and the migration status of critical infrastructure — is a material cybersecurity risk for financial institutions with long-retention data obligations. Disclosure counsel should assess whether current 10-K risk factor disclosures adequately characterize quantum risk. The combination of documented HNDL collection operations and published NIST migration timelines makes the "not yet material" position increasingly difficult to sustain.

CONCLUSION

The NIST standards are published. The NSA timeline is set. The CISA/NSA/NIST joint advisory states that organizations should begin now. The harvest collection operations are, by NSA's own assessment, current.

What is missing in most organizations is not awareness. It is the governance structure that converts awareness into action: an executive owner with budget authority, a completed inventory that defines scope, vendor commitments that establish the dependency timeline, and board engagement that provides the authorization and accountability the program requires.

> The organizations that will complete PQC migration before the timeline forces it are not distinguished by technical sophistication. They are distinguished by governance discipline. The technical work is executable. The governance decisions must come first.

For executives reading this paper: three decisions are required before any technical work can proceed. Someone must be assigned ownership with budget authority. The scope of the cryptographic inventory must be defined. The vendors in the critical path must be formally engaged. None of these decisions requires a technical background. All of them require executive authority.

Axiom Research Institute's subsequent publications in this series address cryptographic inventory methodology, vendor PQC assessment questionnaire design, and board reporting templates aligned to NIST IR 8547 milestones. Organizations seeking practitioner support for PQC migration governance may request an initial consultation at axiomsovereign.com.

REFERENCES

National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce. csrc.nist.gov

National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). NIST IR 8547: Transition to Post-Quantum Cryptography Standards. U.S. Department of Commerce.

National Security Agency. (2022, updated 2024). Commercial National Security Algorithm Suite 2.0. NSA Cybersecurity Advisory.

Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography. Joint Advisory.

Department of Defense. (2023). Cybersecurity Maturity Model Certification (CMMC) 2.0 Program. 32 CFR Part 170.

National Institute of Standards and Technology. (2021). SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

U.S. Department of Health and Human Services, Office for Civil Rights. (2013). HIPAA Security Rule. 45 CFR Parts 160 and 164.

U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Final Rule.