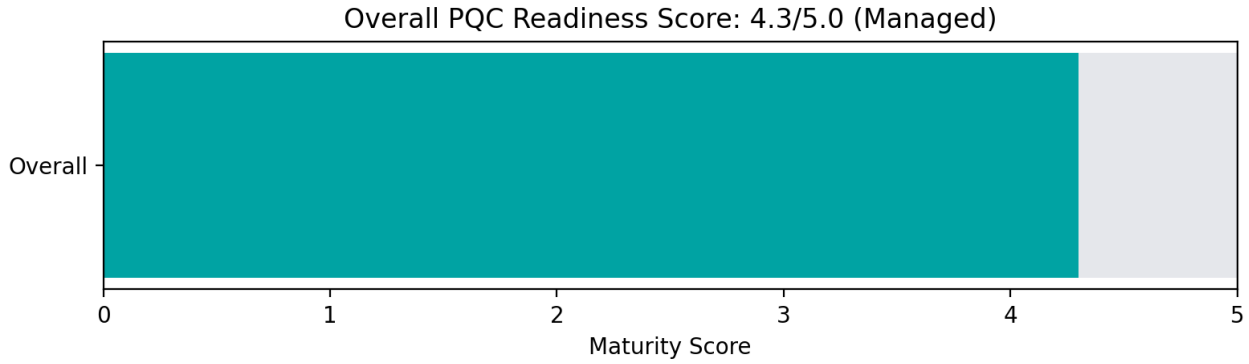
Post-Quantum Cryptography Readiness Assessment Report

Assessment Findings, Critical Issues, FIPS Mapping and Remediation Roadmap



Source Workbook	nist_pqc_readiness_assessment(2).xlsx
Source Tabs Reviewed	Tab 2: Assessment; Tab 3: Summary
Assessment Date	May 2026
Framework Basis	NIST PQC FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA

1. Executive Summary

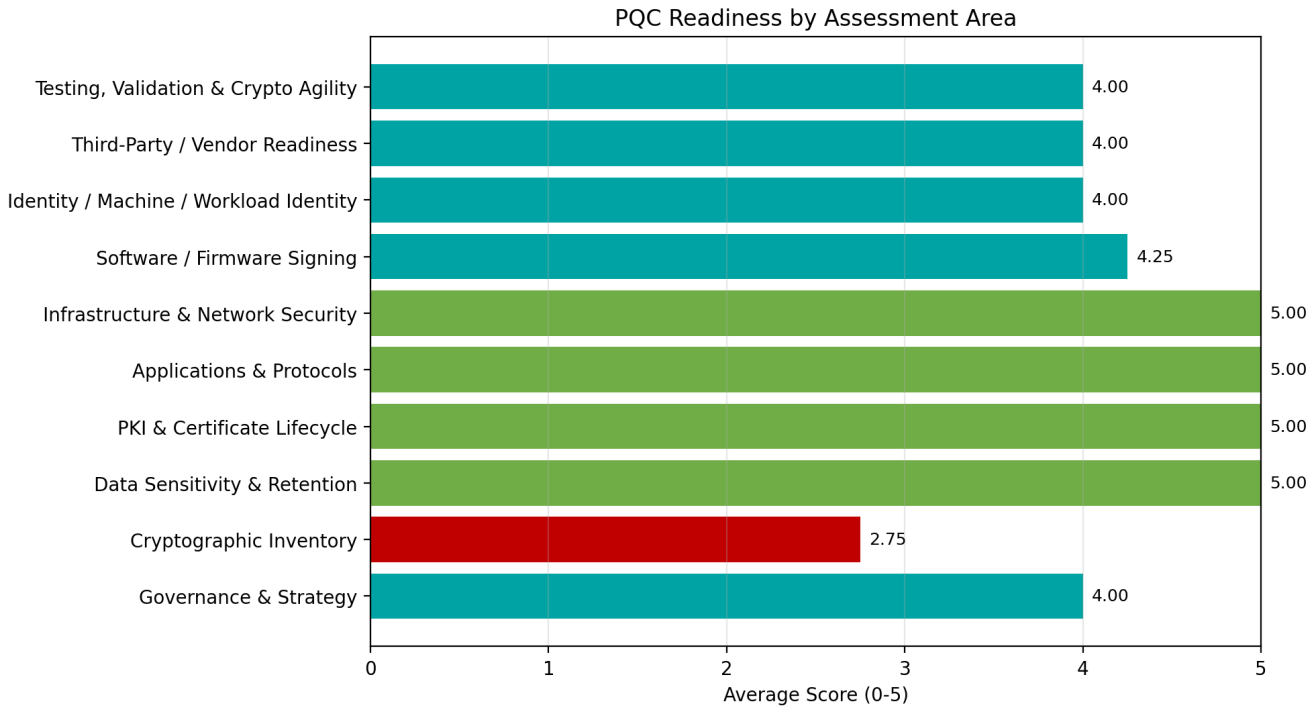
The PQC readiness assessment indicates a strong overall maturity profile with an average score of 4.3/5.0, classified as Managed. The program shows very strong self-assessed performance in Data Sensitivity & Retention, PKI & Certificate Lifecycle, Applications & Protocols, and Infrastructure & Network Security, all scoring 5.0/5.0. These results suggest the organization has a good understanding of harvest-now/decrypt-later risk, priority data classes, PKI impact, protocol transition planning, and infrastructure implications.

However, the assessment also identifies a major readiness gap: Cryptographic Inventory scored 2.75/5.0, with one underlying control scored 0 and another scored 1. This is the most critical finding because cryptographic discovery and dependency mapping are the foundation for any migration to NIST standardized post-quantum cryptography. Without a complete inventory of where RSA, ECC, DH, ECDH, ECDSA, certificates, signing workflows, and key exchange mechanisms exist, the organization cannot reliably prioritize, test, or migrate.

Executive conclusion

The organization appears strategically aware and broadly mature, but the current assessment is not yet audit-ready. The immediate priority is to convert high-level readiness into evidence-backed execution by completing the cryptographic inventory, mapping dependencies by application and owner, validating critical-system prioritization, and assigning remediation owners and dates.

Overall Score	Overall Maturity	Questions Answered	Lowest Area	Evidence Completion
4.3/5.0	Managed	40/40	**Cryptographic Inventory: 2.75/5.0**	0% populated in assessment fields



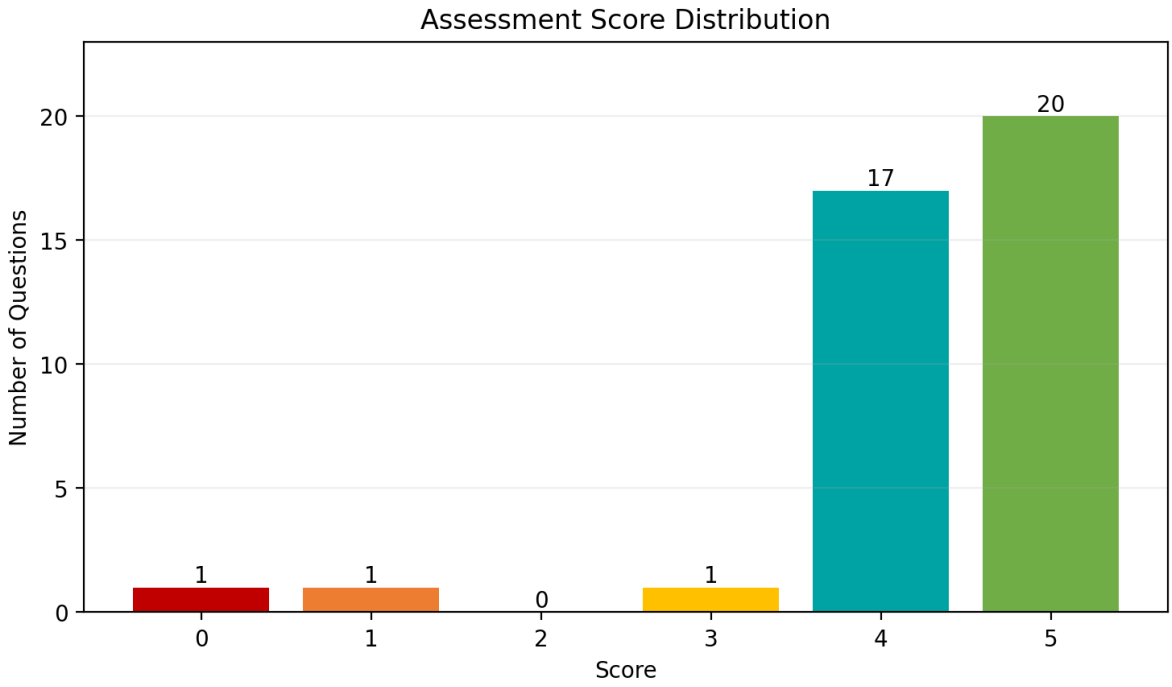
2. NIST PQC FIPS Framework Used for Mapping

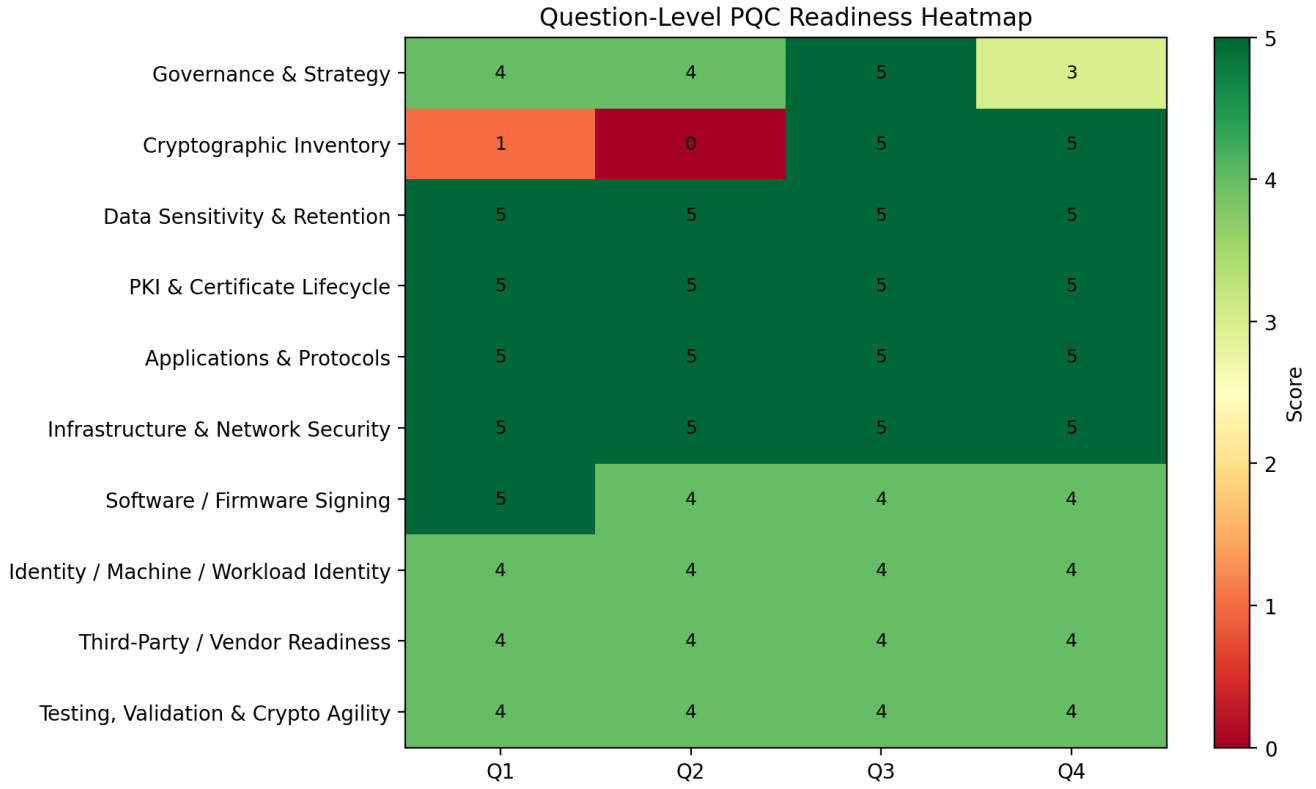
The report maps each finding to the finalized NIST post-quantum cryptography standards published on August 13, 2024. FIPS 203 defines ML-KEM for quantum-resistant key establishment; FIPS 204 defines ML-DSA for quantum-resistant digital signatures; and FIPS 205 defines SLH-DSA for stateless hash-based digital signatures.

Standard	Algorithm	Primary Use	Enterprise Migration Relevance
FIPS 203	ML-KEM	Key establishment / key encapsulation	TLS, VPN, mTLS, workload-to-workload communication, secure sessions, hybrid key exchange.
FIPS 204	ML-DSA	Digital signatures	Code signing, certificate signing, transaction signing, software supply-chain integrity, API/message signing.
FIPS 205	SLH-DSA	Stateless hash-based digital signatures	High-assurance signing, long-lived trust anchors, firmware/root signing, conservative backup signature approach.

3. Assessment Scoring Overview

The scoring profile is heavily weighted toward Managed and Optimized maturity. Twenty questions scored 5, seventeen scored 4, one scored 3, one scored 1, and one scored 0. This creates a strong average score but also masks a critical foundational weakness in cryptographic discovery and dependency mapping.





4. Area-by-Area Findings

Assessment Area	Avg Score	Maturity	FIPS Mapping	Primary Finding
Governance & Strategy	4.00	Managed	FIPS 203/204/205 cross-cutting governance	Strong sponsorship/roadmap; critical-system prioritization needs stronger evidence and business-impact validation.
Cryptographic Inventory	2.75	Developing	FIPS 203 key exchange + FIPS 204/205 signatures	Highest-priority gap; dependency mapping by application, protocol, infrastructure component, and owner is not started.
Data Sensitivity & Retention	5.00	Optimized	FIPS 203 ML-KEM for confidentiality/key establishment	Optimized self-score; validate evidence for 10+ year confidentiality and harvest-now/decrypt-later prioritization.
PKI & Certificate Lifecycle	5.00	Optimized	FIPS 204 ML-DSA + FIPS 205 SLH-DSA signatures; FIPS 203 TLS impact	Optimized self-score; validate certificate toolchain support for PQC/hybrid sizes and algorithms.
Applications & Protocols	5.00	Optimized	FIPS 203 for TLS/IPsec/SSH/mTLS; FIPS 204/205 for S/MIME/code signing	Optimized self-score; maintain testing for TLS, IPsec, SSH, S/MIME, code signing, middlebox impact.
Infrastructure & Network Security	5.00	Optimized	FIPS 203 for VPN/TLS/remote access; FIPS 204/205 for device identity/signatures	Optimized self-score; confirm network devices, VPN, HSMs, and secure access platforms are upgradeable.
Software / Firmware Signing	4.25	Managed	FIPS 204 ML-DSA and FIPS 205 SLH-DSA	Managed; needs deeper PQC signature readiness

				validation for larger signatures and verification paths.
Identity / Machine / Workload Identity	4.00	Managed	FIPS 203 for mTLS/key establishment; FIPS 204/205 for identity/token/cert signatures	Managed; require mapping of machine identity, mTLS, federation, tokens, service mesh, and embedded identities.
Third-Party / Vendor Readiness	4.00	Managed	FIPS 203/204/205 vendor readiness and interoperability	Managed; turn vendor roadmap tracking into contractual requirements and evidence-based risk decisions.
Testing, Validation & Crypto Agility	4.00	Managed	FIPS 203/204/205 lab validation and crypto-agile rollout	Managed; formalize interoperability test cases, rollback/downgrade protections, and performance acceptance criteria.

5. Critical Issues and Improvement Priorities

Severity	Question / Scope	Finding	FIPS Mapping	Corrective Recommendation
Critical	Q006	Cryptographic dependencies are not mapped by application, protocol, infrastructure component, and owner.	FIPS 203/204/205	Launch a cryptographic bill of materials (CBOM) and dependency mapping workstream covering RSA, ECC, DH/ECDH, ECDSA, certificates, keys, libraries, APIs, HSMs, TLS, IPsec, SSH, S/MIME, code signing, container signing, firmware signing, and workload identity.
High	Q005	Inventory of quantum-vulnerable public-key algorithms is only at Initial maturity.	FIPS 203 for key exchange; FIPS 204/205 for signatures	Implement cryptographic discovery tooling plus application owner attestations to identify where RSA, ECC, DH, ECDH, ECDSA, and certificate-based trust are used.
High	All tabs	Assessment evidence fields, action fields, owners, and target dates are blank, creating audit-readiness risk despite high scores.	FIPS 203/204/205 governance evidence	Require evidence artifacts for every score above 3, assign owners and due dates, and create an evidence repository with policy, architecture, test results, vendor confirmations, and remediation tickets.
Medium/High	Q004	Critical systems prioritization is Defined but not yet Managed or Optimized.	FIPS 203 confidentiality planning; FIPS 204/205 trust-anchor planning	Prioritize systems using business criticality, data retention horizon, exposure, regulatory obligations, cryptographic concentration, and vendor upgrade complexity.
Medium	Q026-Q028	Software and firmware signing is Managed, but future support for PQC signatures requires validation.	FIPS 204/205	Test ML-DSA and SLH-DSA signing/verification paths, certificate chain sizes, firmware bootloader constraints, signing appliance support, and build-pipeline readiness.

6. Recommended Remediation Roadmap

The remediation roadmap should focus first on evidence-backed cryptographic discovery and dependency mapping, then move into PQC design, lab validation, vendor alignment, and phased migration.

Phase	Timeline	Objective	Key Activities	FIPS Alignment
1. Mobilize	0-30 days	Establish governance and evidence model	Confirm executive sponsor, establish PQC steering group, define evidence requirements, assign owners for every assessment item.	FIPS 203/204/205 cross-cutting
2. Discover	30-90 days	Build cryptographic inventory and CBOM	Run discovery tools, collect application-owner attestations, map RSA/ECC/DH/ECDH/ECDSA usage, identify certificates, signing workflows, HSMs, protocols, vendors, and hidden crypto.	FIPS 203 for KEM/key exchange; FIPS 204/205 for signatures
3. Prioritize	60-120 days	Rank migration targets by risk and business impact	Classify assets by confidentiality duration, external exposure, criticality, vendor dependency, crypto concentration, and operational complexity.	FIPS 203 for long-lived confidentiality; FIPS 204/205 for trust anchors and signatures
4. Validate	90-180 days	Create PQC lab and test plans	Test hybrid key exchange, larger certificates, ML-KEM parameters, ML-DSA/SLH-DSA signing paths, protocol interoperability, latency, rollback, monitoring, and downgrade protection.	FIPS 203/204/205
5. Migrate	180+ days	Execute phased PQC transition	Pilot non-production systems, update PKI/signing policies, align vendors, migrate priority channels and signing workflows, measure adoption, and continually update inventory.	FIPS 203/204/205

7. Detailed FIPS Mapping of Assessment Findings

Assessment Area	FIPS 203 ML-KEM	FIPS 204 ML-DSA	FIPS 205 SLH-DSA
Governance & Strategy	Governance must define how key-establishment migrations will be planned, prioritized, funded, tested, and measured.	Governance must define signature migration policy for code, certificates, documents, APIs, and identity assertions.	Governance should identify where conservative hash-based signatures are preferred for long-lived/high-assurance trust.
Cryptographic Inventory	Inventory TLS, IPsec, SSH, mTLS, VPN, ECDH/ECDHE, DH, and RSA key transport usage.	Inventory RSA/ECDSA signing, certificate chains, code signing, token signing, and document signing.	Inventory high-assurance signing, root-signing, firmware, and long-lived signature use cases.
Data Sensitivity & Retention	Prioritize ML-KEM transition for data requiring confidentiality beyond quantum-risk horizon.	Identify signed data records and transaction evidence requiring future verifiability.	Use SLH-DSA for long-lived signatures where conservative hash-based assurance is required.
PKI & Certificate Lifecycle	Test certificate and TLS handshake impact in hybrid/PQC environments.	Assess CA, issuance, certificate profile, CRL/OCSP, and chain validation readiness for ML-DSA.	Assess root/intermediate trust-anchor use cases that may need SLH-DSA.
Applications & Protocols	Validate ML-KEM/hybrid support for TLS, IPsec, SSH, S/MIME, and application transports.	Validate ML-DSA support for signed messages, S/MIME, app packages, containers, and code artifacts.	Use SLH-DSA for high-assurance or backup signature migration paths.
Infrastructure & Network Security	Prioritize VPN, secure access, firewalls, load balancers, proxies, and remote access cryptography.	Validate device certificate, management-plane, firmware and signature verification readiness.	Use for high-assurance infrastructure signing where support and performance are acceptable.

Software / Firmware Signing	Limited direct use except where update transport/session keys are involved.	Primary standard for PQC software, package, container, and firmware signatures.	Alternative/backup signature option for high-trust firmware and long-term validation.
Identity / Machine / Workload Identity	Relevant to mTLS and service-to-service key establishment.	Relevant to certificate, token, workload identity, and federation signing workflows.	Relevant for long-lived identity trust anchors and high-assurance device/workload signatures.
Third-Party / Vendor Readiness	Vendors must demonstrate ML-KEM support, hybrid options, and protocol interoperability.	Vendors must disclose ML-DSA roadmap and signing/certificate support.	Vendors should provide SLH-DSA roadmap where high-assurance signing is relevant.
Testing, Validation & Crypto Agility	Lab must test ML-KEM parameters, hybrid negotiation, latency, packet/handshake sizes, and downgrade protection.	Lab must test ML-DSA key/signature sizes, validation paths, signing performance, and certificate implications.	Lab must test SLH-DSA performance, signature sizes, verification impact, and appropriate use cases.

8. Evidence Required to Make the Assessment Audit-Ready

Because the notes, evidence/actions, owner, and target-date fields in the assessment are blank, the next step is to turn maturity scores into verifiable evidence. For each high-scoring area, the assessment should be supported by documented proof.

Evidence Category	Examples of Required Evidence	Related FIPS Area
Governance evidence	PQC strategy, steering committee charter, roadmap, budget, risk acceptance criteria, board reporting.	FIPS 203/204/205
Cryptographic inventory evidence	CBOM, discovery tool outputs, application-owner attestations, protocol scans, certificate inventories, signing workflow inventory.	FIPS 203/204/205
Data-retention evidence	Data classification, retention schedules, crown-jewel inventory, HNDL risk assessment, sensitive data flow diagrams.	FIPS 203
PKI evidence	PKI hierarchy diagrams, CA profiles, certificate templates, issuance workflows, HSM compatibility notes, hybrid certificate test results.	FIPS 203/204/205
Application/protocol evidence	TLS/IPsec/SSH/S/MIME/code-signing inventory, compatibility test outputs, middlebox testing, performance benchmarks.	FIPS 203/204/205
Vendor evidence	Vendor roadmap letters, contract clauses, support matrices, product crypto disclosures, exception records.	FIPS 203/204/205
Testing evidence	Lab architecture, test cases, success criteria, regression results, rollback plans, downgrade protection tests.	FIPS 203/204/205

9. Priority Action Plan

- Start a 30-day Cryptographic Inventory Recovery Sprint focused on Q005 and Q006.
- Create a CBOM for critical applications, infrastructure, identity platforms, PKI, software-signing systems, and third-party services.
- Assign owners and target dates for every assessment row; no score above 3 should remain without evidence.
- Validate all Optimized scores through artifact review, architecture review, and stakeholder interviews.
- Build a PQC test lab to validate FIPS 203 ML-KEM key establishment and FIPS 204/205 signature migration scenarios.
- Prioritize migration using business criticality, data-retention horizon, external exposure, cryptographic concentration, and vendor dependency.

10. References

NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM): https://csrc.nist.gov/pubs/fips/203/final

NIST FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA): https://csrc.nist.gov/pubs/fips/204/final

NIST FIPS 205, Stateless Hash-Based Digital Signature Standard (SLH-DSA): https://csrc.nist.gov/pubs/fips/205/final

NIST announcement: first finalized post-quantum encryption standards: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST NCCoE Migration to Post-Quantum Cryptography: https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

MODERN AI
smart. secure. transformative

Post-Quantum Cryptography 120-Day Posture Improvement Roadmap

Executive one-page summary | Prioritized from most critical to least critical |
Mapped to NIST PQC FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)

Overall Maturity	Lowest Domain	Critical Gap
4.3/5 Managed	2.75/5 Cryptographic Inventory	Q006 = 0

Priority sequence: close cryptographic visibility gaps first, then enable crypto-agility, signature modernization, and sustainable governance.

1 Cryptographic Inventory & Dependency Mapping

Identify all RSA, ECC, DH, ECDH, ECDSA, certificates, TLS/VPN use, libraries, HSM/KMS dependencies, appliances, and hidden vendor cryptography. Most critical starting point.

Foundation for FIPS 203 / 204 / 205 adoption

2 Quantum Risk Classification

Classify systems and data by confidentiality horizon, business criticality, internet exposure, regulatory sensitivity, and harvest-now-decrypt-later risk.

Prioritization for FIPS 203 confidentiality migration

3 Crypto-Agility & Migration Architecture

Define hybrid migration patterns for TLS, VPN, APIs, PKI, KMS/HSM, cloud workloads, and key establishment. Establish future-state architecture.

FIPS 203 ML-KEM

4 Digital Signature Modernization

Modernize code signing, firmware signing, certificate chains, document signing, software supply chain trust, and AI artifact signing.

FIPS 204 ML-DSA / FIPS 205 SLH-DSA

5 Vendor & Third-Party Readiness

Obtain supplier PQC roadmaps, SBOM/CBOM evidence, crypto library plans, appliance readiness, firmware commitments, and contractual assurances.

Cross-cutting across all PQC FIPS standards

6 Testing, Validation & Continuous Governance

Run pilots, compatibility tests, performance validation, change control, metrics, exception management, detection updates, and audit reporting.

Sustain FIPS-aligned adoption

Business Value, Risk Mitigation & Cybersecurity Improvement

Business Value

- Protect long-lived sensitive data
- Enable controlled migration instead of emergency rip-and-replace
- Strengthen trust with clients, regulators, and partners

Risk Mitigation

- Reduce harvest-now-decrypt-later exposure
- Eliminate blind cryptographic dependencies
- Lower third-party and supply-chain risk

Cybersecurity Improvements

- Improve crypto visibility and governance
- Modernize key exchange and digital signature strategy
- Improve resilience of software, identities, and certificates

Overall Business Impact

- Highee roaidance and audit readiness
- Clearer investment prioritization
- Reduced disruption during future PQC migration

120-Day Plan

Phase 1: Days 1–30 | Discover & Mobilize

- Appoint PQC owner and governance team
- Launch crypto inventory sprint
- Prioritize Q006 dependency gap

Business Impact: Immediate visibility and executive alignment

Phase 2: Days 31–60 | Prioritize & Design

- Complete quantum risk classification
- Identify high-risk data and systems
- Design hybrid migration architecture

Business Impact: Clear prioritization and migration blueprint

Phase 3: Days 61–90 | Pilot & Validate

- Pilot ML-KEM use cases
- Assess ML-DSA / SLH-DSA signature opportunities
- Validate vendor readiness and compatibility

Business Impact: Reduced technology uncertainty and stronger cyber controls

Phase 4: Days 91–120 | Govern & Scale

- Finalize roadmap and remediation plan
- Define metrics, reporting, and audit evidence
- Launch phased rollout and governance cadence

Business Impact: Sustainable transformation and measurable risk reduction

Assessment-informed executive roadmap. Values shown reflect the current readiness assessment.