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.