SafeCipher's 2026 Post-Quantum Cryptography (PQC) Readiness Checklist

Your Essential Guide to Quantum-Safe PKI and Crypto Agility

safecipher.com | Leading Post-Quantum & PKI Experts

Introduction to the Quantum Threat in 2026

As we enter 2026, quantum computing advances make "harvest now, decrypt later" attacks a real risk. NIST has finalized core standards:

- ML-KEM (key encapsulation – primary for encryption)
- ML-DSA (primary digital signatures)
- SLH-DSA (hash-based signatures for conservatism)

Upcoming standards to watch in 2026:

- FN-DSA (compact signatures)
- HQC (diverse backup KEM; draft expected 2026)

2026 is pivotal. Expect:

- First quantum-safe certificates
- Hybrid deployments in protocols (e.g., TLS)
- Regulatory pushes (e.g., CISA, NSA CNSA 2.0)

Vulnerable algorithms (RSA, ECC) remain usable but should be inventoried and prioritized for migration. Aim for crypto agility to handle hybrids and future updates.

Phase 1: Build Awareness and Governance

☐ Form a cross-functional PQC task force (IT, security, compliance, procurement, executives).

☐ Assign clear ownership for cryptographic decisions and migration oversight.

☐ Secure executive sponsorship and allocate budget for 2026 pilots (e.g., hybrid testing).

☐ Educate stakeholders on risks and 2026 milestones (use NIST/CISA guidance as a baseline).

☐ Update policies: mandate crypto inventory and vendor PQC roadmaps in procurements.

☐ Define success metrics (e.g., percentage of vulnerable crypto identified by mid-2026).

Phase 2: Cryptographic Inventory and Discovery

☐ Map all cryptographic uses: algorithms (RSA, ECC, etc.), locations (code, cloud, devices, HSMs, PKI certificates), and data flows.

☐ Prioritize high-risk assets: long-lived sensitive data, critical systems, supply chain dependencies.

☐ Use automated tools for discovery to uncover hidden crypto implementations.

☐ Document dependencies: libraries, protocols (TLS, SSH), vendors, and certificate lifecycles.

☐ Identify a Crypto Bill of Materials (CBOM) for compliance reporting.

☐ Flag quick wins: systems ready for immediate hybrid upgrades.

Phase 3: Risk Assessment and Prioritization

☐ Score risks based on data sensitivity, system lifespan, and quantum threat horizon (e.g., prioritize data needing protection beyond 2030).

☐ Evaluate alternatives: hybrid (classical + PQC) vs. pure PQC; consider diversity (e.g., HQC as backup to ML-KEM).

☐ Assess supply chain readiness: request vendor PQC roadmaps and timelines.

☐ Perform impact analysis: downtime, cost, and interoperability implications during migration.

☐ Create a prioritized roadmap: high-risk items for 2026 pilots; full migration targets by 2030–2035 (per applicable guidance).

☐ Plan for agility: favor vendor-neutral HSMs and automated key management where practical.

Phase 4: Migration Planning

☐ Test NIST algorithms in labs/non-production (start with ML-KEM/ML-DSA hybrids).

☐ Update PKI policies and certificate profiles to prepare for quantum-safe certificates (expected availability in 2026).

☐ Implement crypto agility: modular systems for easy algorithm swaps.

☐ Pilot deployments in 2026 (e.g., quantum-safe TLS, VPNs, or code signing).

☐ Set timeline goals: inventory complete by mid-2026; pilots underway; monitor for FN-DSA/HQC standards progress.

☐ Address known challenges: performance impacts, larger keys/signatures, and interoperability constraints.

Bonus: Quick Wins and Next Steps

Immediate actions for 2026:

- Enable crypto agility in new procurements.
- Encrypt new sensitive data with hybrids where possible (“harvest-no-more”).
- Monitor updates from NIST PQC and the CISA quantum initiative.

Partner with SafeCipher: schedule a free readiness scan or consultation to accelerate your journey. Our vendor-neutral expertise supports seamless PKI transitions.

Resources

- NIST PQC: csrc.nist.gov/projects/post-quantum-cryptography
- CISA Quantum Initiative: cisa.gov/quantum