POST-QUANTUM CRYPTOGRAPHY
READINESS CHECKLIST

Enterprise Framework for Quantum-Safe Migration

January 2026 Edition

1,095	**100%**	**3-5 Years**
Days to Q-Day 2028	Enterprises with PQC Gaps	Typical Migration Time

Aligned with NIST FIPS 203/204/205 | NSA CNSA 2.0 | CISA Quantum Readiness

Sector guidance for Financial Services | Healthcare | Government | Critical Infrastructure

QRYPTONIC

SECURING TOMORROW, TODAY

Executive Summary

Quantum computers capable of breaking RSA, ECC, and Diffie-Hellman encryption are projected to emerge between 2028 and 2035. The threat is not theoretical. Adversaries are executing Harvest Now, Decrypt Later (HNDL) attacks today, capturing encrypted data for future quantum decryption.

This creates an urgent calculus. If your data must remain confidential for 10 years and migration takes 5 years, you needed to start in 2018. Most organizations have not.

NIST finalized the first three post-quantum cryptography standards in August 2024: FIPS 203 (ML-KEM for key encapsulation), FIPS 204 (ML-DSA for digital signatures), and FIPS 205 (SLH-DSA for stateless hash-based signatures). The standards are done. Implementation must begin now.

This checklist synthesizes guidance from NIST, NSA, CISA, and sector-specific regulators into an actionable framework. It goes beyond generic advice to provide the timeline pressure, algorithm decision criteria, and maturity measurement that enterprise security teams require.

The Mosca Inequality: Why 2026 Is Already Late

If X + Y > Z, you must act now. X = shelf life of your data. Y = time to migrate. Z = time until quantum threat.

Example: Healthcare records (X = 50 years) + typical migration (Y = 5 years) = 55 years. If Z = 10 years, you are 45 years behind.

Financial transaction archives, M&A due diligence, government classified material, and long-term contracts all face immediate HNDL exposure.

Regulatory Timeline and Compliance Mandates

Multiple regulators have issued or are developing quantum cryptography requirements. These hard dates should anchor your roadmap.

Date	Authority	Requirement
Aug 2024	NIST	FIPS 203, 204, 205 finalized. PQC standards official.
2025	OCC / FFIEC	Banks must inventory quantum-vulnerable cryptography.
2025	PCI DSS 4.0	Crypto-agility requirements for payment card data.
2027	OMB M-23-02	Federal agencies must complete crypto inventory.
2030	NSA CNSA 2.0	NSS software must use PQC algorithms.
2033	NSA CNSA 2.0	NSS firmware/hardware must use PQC algorithms.
2035	NSA CNSA 2.0	Full quantum resistance required for all NSS.

Sector-Specific Compliance Hooks

- Financial Services: OCC Bulletin 2024-18 requires banks to inventory quantum-vulnerable cryptography. FFIEC guidance emphasizes crypto-agility. SOX audit committees should receive quantum risk briefings.
- Healthcare: HIPAA Security Rule requires encryption of PHI. Patient records have lifetime retention requirements, creating immediate HNDL exposure. OCR enforcement will follow NIST standards.
- Government/Defense: FedRAMP is tracking PQC readiness. CMMC 2.0 will incorporate quantum requirements. Defense contractors should align with CNSA 2.0 timelines.
- Critical Infrastructure: NERC CIP standards will evolve to include PQC. Energy sector ICS/SCADA systems have long upgrade cycles requiring early planning.

Algorithm Selection Guide

NIST has standardized three algorithms. Each serves different use cases with distinct tradeoffs. This table provides decision criteria.

Algorithm	Standard	Use Case	When to Choose
ML-KEM (Kyber)	FIPS 203	Key encapsulation	Default for TLS, VPN, encrypted communications. Smaller ciphertext than alternatives. Best general-purpose choice.
ML-DSA (Dilithium)	FIPS 204	Digital signatures	Default for code signing, certificates, authentication. Fast signing/verification. Larger keys than classical.
SLH-DSA (SPHINCS+)	FIPS 205	Digital signatures	Conservative choice when lattice assumptions concern you. Hash-based security well understood. Large signatures but proven foundation.
FN-DSA (Falcon)	Draft 2025	Digital signatures	Smallest signatures of lattice schemes. Requires careful implementation to avoid side-channel attacks. Wait for NIST finalization.

Implementation Note: Most organizations should start with ML-KEM for key exchange and ML-DSA for signatures. SLH-DSA serves as a fallback if future cryptanalysis weakens lattice-based schemes. Hybrid deployments (classical + PQC in parallel) provide defense-in-depth during transition.

The 12-Step PQC Readiness Checklist

Phase 1: Foundation (Months 1-3)

1. Establish Governance and Executive Sponsorship

Form a cross-functional quantum readiness team with C-suite sponsorship. Assign board-level or CISO ownership. Integrate quantum risk into existing enterprise risk management frameworks. Set budget allocation and success metrics.

- ○ *Deliverable: Quantum Risk Governance Charter with named accountable executive*
- ○ *Maturity indicator: Executive receives quarterly quantum risk briefings*

2. Conduct Cryptographic Discovery and Inventory

Deploy automated scanning tools to identify all cryptographic implementations across applications, infrastructure, and third-party dependencies. Build a Cryptographic Bill of Materials (CBOM) documenting algorithms, key lengths, protocols, libraries, and the data each protects.

- ○ *Deliverable: Complete CBOM with quantum vulnerability classification*
- ○ *Maturity indicator: 95%+ coverage of enterprise systems in inventory*

3. Assess HNDL Exposure and Data Classification

Calculate your Mosca Inequality for each data category. Identify data with secrecy requirements exceeding the quantum threat timeline. Prioritize: M&A records, litigation holds, healthcare PHI, financial archives, government classified material, and any data subject to long regulatory retention.

- ○ *Deliverable: HNDL exposure matrix with risk-ranked data categories*
- ○ *Maturity indicator: Board-approved prioritization of crown jewel data*

Phase 2: Planning (Months 4-9)

4. Develop Migration Roadmap with Regulatory Alignment

Create a phased migration plan working backward from regulatory deadlines. Map CNSA 2.0 dates for government work. Align with sector-specific requirements (OCC, PCI, HIPAA). Define milestones, resource requirements, and dependencies. Plan for 3-5 year execution timeline.

- ○ *Deliverable: Board-approved PQC migration roadmap with budget*
- ○ *Maturity indicator: Roadmap milestones incorporated into IT strategic plan*

5. Evaluate and Select PQC Algorithms

Assess NIST-standardized algorithms against your use cases. Test ML-KEM for key exchange, ML-DSA for signatures. Evaluate performance impact on latency-sensitive applications. Consider hybrid approaches for defense-in-depth. Document algorithm selection rationale.

- ○ *Deliverable: Algorithm selection matrix with performance benchmarks*
- ○ *Maturity indicator: Lab testing completed on candidate algorithms*

6. Design Crypto-Agility Architecture

Architect systems for algorithm flexibility. Implement abstraction layers that allow cryptographic modules to be swapped without application changes. Design for negotiable cipher suites. Plan key management systems that support both classical and post-quantum algorithms during transition.

- ○ *Deliverable: Crypto-agility architecture specification*
- ○ *Maturity indicator: Reference implementation in development environment*

7. Engage Vendors and Supply Chain

Survey all vendors on their PQC roadmaps. Obtain written timelines for when products will support NIST standards. Update procurement requirements to mandate PQC readiness or upgrade paths. Identify vendors without plans and develop mitigation strategies or alternatives.

- ○ *Deliverable: Vendor PQC readiness assessment with risk ratings*
- ○ *Maturity indicator: PQC requirements in new contract language*

Phase 3: Implementation (Months 10-36)

8. Execute Pilot Deployments

Deploy PQC in non-production environments first. Test hybrid TLS configurations. Validate certificate chain handling with PQC signatures. Measure performance overhead. Conduct security testing of implementations. Document lessons learned for production rollout.

- ○ *Deliverable: Pilot deployment report with performance metrics*
- ○ *Maturity indicator: Successful hybrid TLS handshakes in test environment*

9. Migrate Data-in-Transit

Upgrade TLS implementations to support ML-KEM key exchange. Deploy hybrid cipher suites that combine classical and post-quantum algorithms. Prioritize external-facing endpoints and VPN infrastructure. Coordinate with partners on interoperability.

- ○ *Deliverable: Production TLS upgrade completion report*
- ○ *Maturity indicator: 100% of external endpoints support PQC cipher suites*

10. Migrate Data-at-Rest and Re-encrypt Archives

Address the HNDL backlog. Re-encrypt high-value archived data with quantum-resistant algorithms. Update key management systems. Rotate certificates to PQC-signed versions. Document data that cannot be re-encrypted and implement compensating controls.

- ○ *Deliverable: Data-at-rest migration completion with exceptions documented*
- ○ *Maturity indicator: Crown jewel data protected with PQC algorithms*

Phase 4: Sustainment (Ongoing)

11. Validate and Audit Completion

Conduct post-migration audit to verify all identified vulnerabilities addressed. Update documentation. Perform penetration testing against PQC implementations. Validate compliance with applicable regulations. Obtain third-party attestation where required.

- ○ *Deliverable: Independent audit report confirming PQC implementation*
- ○ *Maturity indicator: Clean audit findings on cryptographic controls*

12. Establish Continuous Monitoring and Evolution

Quantum threats and cryptographic standards will continue evolving. Institute continuous monitoring of NIST announcements, cryptanalysis research, and quantum computing progress. Keep CBOM current as systems change. Drill crypto-agility procedures annually. Treat PQC readiness as permanent posture, not a project endpoint.

- ○ *Deliverable: Crypto monitoring program with defined triggers for action*
- ○ *Maturity indicator: Annual crypto-agility drill completed successfully*

PQC Readiness Maturity Model

Use this framework to assess current state and track progress. Score each dimension 1-5 and calculate overall readiness.

Dimension	1 - Initial	2 - Aware	3 - Planned	4 - Active	5 - Optimized
Governance	No ownership	CISO aware	Charter approved	Board reporting	Integrated ERM
Inventory	None	Partial manual	Automated scan	Full CBOM	Continuous update
Risk Assessment	Not started	Ad hoc review	HNDL mapped	Prioritized plan	Quantified risk
Crypto-Agility	Hardcoded	Some flexibility	Architecture spec	Implemented	Tested annually
Vendor Mgmt	Not addressed	Some inquiries	All surveyed	Contract terms	Ongoing validation
Implementation	No PQC	Lab testing	Pilot deployed	Production live	Full migration

Scoring: Sum all dimensions (max 30). Score 6-12 = Critical gaps requiring immediate action. Score 13-18 = Developing program, accelerate planning. Score 19-24 = Active migration, maintain momentum. Score 25-30 = Mature posture, focus on optimization.

About This Checklist

This framework synthesizes guidance from authoritative sources including NIST SP 800-208, NSA CNSA 2.0, CISA Quantum Readiness guidance, OMB M-23-02, and sector-specific regulations. It reflects the consensus of industry practitioners while adding the practical specificity that generic frameworks lack.

Qryptonic prepared this checklist as part of our mission: Post-Quantum Ready, Permanently. We are an independent, vendor-neutral advisory firm specializing in cryptographic risk assessment and PQC migration. Our assessments have identified 300+ critical vulnerabilities across Fortune 500 enterprises.

What Makes Qryptonic Different

- **Real Quantum Hardware Testing:** We validate findings across IBM Quantum, AWS Braket, Azure Quantum, Google, IonQ, D-Wave, Quantinuum, and Rigetti. Not simulation. Actual quantum hardware.
- **$2M Quantum Challenge:** 90-120 day white-box assessment. Zero critical vulnerabilities found = $2,000,000 wire transfer. To date: $0 paid out. Every assessment has discovered critical vulnerabilities.
- **Vendor Independence:** No product sales. No vendor partnerships that create conflicts. Fee-only advisory with recommendations in your interest alone.
- **Intelligence-Grade Standards:** Advisory board includes former CISA Executive Assistant Director, CIA Deputy Director for Cyber, DIA Senior Executive, and Fortune 500 CISOs. We apply national security rigor to enterprise problems.

Next Steps

Ready to assess your cryptographic posture? Qscout26 delivers first findings in 7 days with board-ready reporting. Qstrike26 provides comprehensive 4-month testing with proof-of-concept demonstrations.

- Request Assessment: qryptonic.com/contact
- Take the $2M Challenge: qryptonic.com/quantum-challenge
- Email: info@qryptonic.com
- Phone: +1 (888) 2-QRYPTONIC

References

1. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.

2. NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard. August 2024.

3. NIST. FIPS 205: Stateless Hash-Based Digital Signature Standard. August 2024.

4. NSA. Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Cybersecurity Advisory. September 2022.

5. CISA, NSA, NIST. Quantum-Readiness: Migration to Post-Quantum Cryptography. August 2023.

6. OMB. M-23-02: Migrating to Post-Quantum Cryptography. November 2022.

7. OCC. Bulletin 2024-18: Cryptographic Risk Management. 2024.

8. PCI Security Standards Council. PCI DSS v4.0. March 2022.

9. IBM. The CISO's Guide to Quantum-Safe Readiness. 2024.

10. Deloitte, World Economic Forum. Quantum Readiness Toolkit. 2023.

11. CyberArk. A CISO's Guide to Post-Quantum Readiness. 2024.

12. Mosca, M. Cybersecurity in an Era with Quantum Computers. Global Risk Institute. 2015.