QUADRANT LAW GROUP

BULLETIN
Technology & Security

Post-Quantum Cryptography (PQC) Readiness Planning
A Practical Roadmap

Jake Vollebregt, Partner

Executive Summary

Quantum computing is expected to weaken widely used encryption methods in the next few years. Financial institutions, cloud providers, and other regulated entities are planning for migration to NIST-approved post-quantum cryptography (PQC) standards to protect long-lived sensitive data from "harvest now, decrypt later" attacks and other risks. This bulletin provides a practical roadmap for contractual readiness and vendor management.

"After 2030, these encryption methods will no longer be approved for new systems or applications requiring NIST-compliant security. By 2035, NIST will classify these algorithms as non-compliant in regulated environments."

The Quantum Threat

Quantum computing is a cutting-edge field of computer science and engineering research that seeks to harness quantum mechanics to perform calculations exponentially faster than even the most powerful traditional computers. If successful, quantum computing will pose a fundamental challenge to customary encryption practices.

It could undermine the reliability of current digital signature methods, and even the theoretical possibility of quantum computing creates a "harvest now, decrypt later" scenario (HNDL), in which bad actors capture or retain encrypted data today for future decryption once quantum capabilities mature. This risk is acute for long-lived sensitive data such as financial records, trade secrets, health information, or personal data that may remain valuable and confidential for decades. Financial institutions, cloud providers, and other enterprises handling regulated data face heightened exposure due to long retention periods and dependencies across interconnected information systems.

Additional Reading

NIST Internal Report (IR) 8547: Transition to Post-Quantum Cryptography Standards [https://csrc.nist.gov/pubs/ir/8547/ipd]

Mastercard Whitepaper: Migration to Post-Quantum Cryptography [https://www.mastercard.com/us/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html]

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/205/final]

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

ISACA: Passwordless Authentication: Risk, Reward, and Readiness (January 2026) [https://www.isaca.org/resources/news-and-trends/industry-news/2026/passwordless-authentication-risk-reward-and-readiness]

NIST Timeline and Deprecation Schedule

As of early 2026, common public-key algorithms like RSA-2048 and ECC-256 remain secure against attacks from classical computers. However, organizations have begun planning migrations as quantum-vulnerable algorithms (e.g., RSA and ECC) face deprecation over time. The National Institute of Standards and Technology (NIST) has proposed timelines for phasing out these classical algorithms:

• By 2030, NIST plans to deprecate RSA-2048, ECC-256, and related algorithms like ECDSA, EdDSA, DH, ECDH.

• By 2035, NIST will classify these algorithms as non-compliant in regulated environments.

After 2030, these algorithms may no longer be approved for certain new systems or applications requiring NIST-aligned security.

NIST Post-Quantum Cryptography Standards

In August 2024, NIST published the first post-quantum cryptography (PQC) standards. These Federal Information Processing Standards (FIPS) are derived from quantum-resistant algorithms:

- **FIPS 203** (ML-KEM): Module-Lattice-Based Key-Encapsulation Mechanism, derived from CRYSTALS-Kyber—used for secure key exchange
- **FIPS 204** (ML-DSA): Module-Lattice-Based Digital Signature Algorithm, derived from CRYSTALS-Dilithium—used for digital signatures
- **FIPS 205** (SLH-DSA): Stateless Hash-Based Digital Signature Algorithm, derived from SPHINCS+—used for hash-based signatures

Key Implementation Factors

Risk Horizon: Quantum threats are forward-looking but accelerating. Accounting for NIST's target dates, many implementation roadmaps target full migration of critical systems by the early-to-mid 2030s.

Enforcement Drivers: Beyond data protection authorities, enterprises operating in regulated industries can expect scrutiny from financial regulators (e.g., SEC, OCC, CISA, BIS frameworks) and corresponding contractual obligations in vendor ecosystems.

Technical Focus: Emphasis shifts to cryptographic agility (seamless algorithm swaps), hybrid implementations (combining classical and PQC during transition), and inventorying quantum-vulnerable assets.

Practical Roadmap to PQC Readiness

Remediation Planning: Data controllers can develop an internal migration roadmap aligned with NIST guidance, incorporating hybrid modes initially and full PQC adoption on a risk-based timeline (e.g., targeting core systems by 2028–2030 where feasible). For critical services, flag PQC requirements during contract renewals or negotiate mid-term amendments for critical, high-volume, or long-term arrangements.

Checklist: Enterprise data offices can improve readiness by adopting best practices and engaging in proactive governance. Specifically, they can incorporate evolving NIST FIPS into their cryptographic inventories, vendor due diligence, audit trails, and incident response plans.

- ☐ Conduct cryptographic discovery to identify systems using quantum-vulnerable algorithms
- ☐ Classify data by sensitivity and retention period to prioritize migration
- ☐ Review existing vendor contracts for cryptographic obligations
- ☐ Develop internal PQC migration roadmap with target dates
- ☐ Flag PQC requirements in upcoming contract renewals
- ☐ Request PQC roadmaps from critical vendors
- ☐ Establish audit protocols for ongoing PQC compliance monitoring
- ☐ Assess authentication policies and prioritize passwordless solutions

Data Categorization: A cryptographic discovery exercise can identify and prioritize systems using quantum-vulnerable algorithms. Focus on data-intensive functions such as:

- Cloud platforms
- Encrypted hosting services
- Identity and access management systems
- Endpoint protection solutions

Data or security offices can catalog third-party services, map data lineage, and classify data by sensitivity (e.g., personal, highly confidential, trade secrets, export controls, and other regulated data). This inventory informs risk-based prioritization and highlights risk exposure from long-term retention.

Contractual Clauses: Data controllers should incorporate forward-looking provisions to ensure vendors, affiliates, and other third-party partners can upgrade cryptographic functions without disruption or added cost.

Harmonize Retention Policies and Data Destruction Triggers: HNDL risk can be reduced (likelihood and impact) by enforcing strict retention limits, requiring vendors to return data for secure internal archival (where long-term retention is required), and deleting vendor-held copies thereafter. Policies can be tailored based on these factors:

- Data confidentiality level (e.g., trade secrets vs. personal data)
- Storage medium (e.g., cloud vs. air-gapped archives)
- Data volume and time-value processing requirements

Passwordless Credential Policies: While HNDL primarily targets the long-term vulnerability of encrypted data to future quantum decryption, it also intersects with authentication risks like password reuse. If a bad actor harvests encrypted credentials today (e.g., hashed passwords or protected credential stores from legacy systems), quantum capabilities could decrypt them and expose reusable passwords that persist after PQC migration. This enables credential stuffing attacks, where compromised credentials from one breach are tested against other accounts. To mitigate, enterprises can incorporate modern authentication standards into their PQC roadmaps, prioritizing passwordless solutions such as single sign-on (SSO), biometrics, or hardware-based private keys (e.g., FIDO2-compliant security keys).