Quantum Readiness Executive Brief

Preparing Your Organization for the Post-Quantum Era

Executive Summary

Cryptographically Relevant Quantum Computers (CRQCs) are projected to break current encryption within 5-10 years. Organizations must begin migration now to protect sensitive data from 'Harvest Now, Decrypt Later' attacks. NIST has finalized post-quantum cryptography standards (August 2024), and federal mandates require agencies to be quantum-ready by 2035.

The Quantum Threat

Current public-key cryptography (RSA, ECC, DH) protects virtually all digital systems:

- TLS/HTTPS web communications
- VPN and secure network tunnels
- Digital signatures and certificates
- Email encryption (S/MIME, PGP)
- Financial transaction security

Quantum computers running Shor's algorithm will break these in polynomial time.

Critical Timeline

2024 NIST finalizes FIPS 203, 204, 205
2025 Federal guidance implementation
2027 Early CRQC demonstrations expected
2030-35 CRQC likely operational
2035 Federal mandate deadline

Harvest Now, Decrypt Later

Adversaries are collecting encrypted data today to decrypt with future CRQCs.

NIST Post-Quantum Cryptography Standards (August 2024)

Standard	Algorithm	Purpose	Notes
FIPS 203	**ML-KEM**	Key Encapsulation	Primary standard for key exchange
FIPS 204	**ML-DSA**	Digital Signatures	Primary standard for signatures
FIPS 205	**SLH-DSA**	Digital Signatures	Backup signature standard

Why Organizations Must Act Now

1. Migration Complexity: Enterprise cryptographic transitions typically take 5-10 years
2. Data at Risk Today: Sensitive data encrypted now will be vulnerable when CRQCs arrive
3. Compliance Requirements: NIST, federal, and industry mandates are being established
4. Vendor Dependencies: Third-party software and services require coordinated updates
5. Competitive Advantage: Early adopters demonstrate security leadership to customers

QRAMM Framework: Structured Approach to Quantum Readiness

The Quantum Readiness Assurance Maturity Model provides 120 assessment questions across 4 dimensions:

Governance & Strategy
Leadership
policy

Technical Readiness
Cryptographic inventory
architecture

Operational Capability
Processes
monitoring

Supply Chain Security
Vendor assessment
third-party risk

Recommended Actions for Leadership

Immediate (0-90 Days)

- Designate quantum readiness executive sponsor
- Conduct initial QRAMM self-assessment
- Inventory high-value data requiring protection
- Brief board on quantum risk exposure

Near-Term (90-180 Days)

- Complete cryptographic asset inventory
- Assess vendor PQC migration timelines
- Develop quantum readiness roadmap
- Allocate budget for migration program

Medium-Term (6-18 Months)

- Pilot PQC implementations in test environment
- Update procurement requirements for PQC
- Train technical staff on new algorithms
- Establish hybrid cryptography approach

Long-Term (18+ Months)

- Execute phased production migration
- Achieve compliance with regulations
- Implement continuous monitoring
- Maintain crypto-agility for future updates

Key Questions for Your Next Board Meeting

1. Do we have a complete inventory of cryptographic assets and their quantum vulnerability?
2. What is our exposure to 'harvest now, decrypt later' attacks on sensitive data?
3. What are our key vendors' PQC migration timelines?
4. What budget and resources are required for our migration program?
5. Who is accountable for our quantum readiness program?

Resources

QRAMM Assessment Toolkit: qramm.org/toolkit
NIST PQC Standards: csrc.nist.gov/pqcrypto
CISA Quantum Readiness: cisa.gov/quantum
NSM-10 Federal Requirements: whitehouse.gov/nsm-10