Post-Quantum Cryptography Migration Checklist

A Step-by-Step Guide for Your PQC Transition

Use this checklist to track your organization's progress through the post-quantum cryptography migration. Check off items as completed and note responsible parties and target dates.

Phase 1: Discovery & Assessment

	Task	Owner	Target	Status
☐	Identify executive sponsor for quantum readiness initiative			
☐	Establish quantum readiness working group with cross-functional repres...			
☐	Conduct initial awareness training for leadership and key stakeholders			
☐	Define scope of cryptographic inventory (systems, applications, data s...			
☐	Select and deploy cryptographic discovery tools			
☐	Complete automated scan of infrastructure for cryptographic assets			
☐	Manual review of custom applications for hardcoded cryptography			
☐	Document all certificates, keys, and key management systems			
☐	Identify third-party and vendor cryptographic dependencies			
☐	Catalog cryptographic libraries and their versions across systems			

Phase 2: Risk Analysis & Planning

	Task	Owner	Target	Status
☐	Classify data by sensitivity and retention requirements			
☐	Identify systems vulnerable to harvest now, decrypt later attacks			
☐	Assess quantum risk for each cryptographic asset			
☐	Prioritize assets based on risk score and business criticality			
☐	Develop preliminary migration timeline and resource requirements			
☐	Create budget proposal for quantum readiness initiative			
☐	Establish governance framework for migration decisions			
☐	Define success metrics and KPIs for migration program			
☐	Identify regulatory and compliance requirements (NIST, FedRAMP, etc.)			
☐	Document risk acceptance criteria and escalation procedures			

Phase 3: Architecture & Planning

	Task	Owner	Target	Status
☐	Evaluate NIST PQC algorithms for organizational fit			
☐	Design crypto-agile architecture patterns			
☐	Plan certificate and key management system upgrades			
☐	Define hybrid cryptography approach for transition period			
☐	Create detailed migration runbooks for each system category			
☐	Establish rollback procedures and contingency plans			
☐	Plan performance testing methodology			
☐	Design monitoring and alerting for cryptographic operations			
☐	Coordinate with vendors on PQC support timelines			
☐	Develop staff training and certification program			

Phase 4: Pilot Implementation

	Task	Owner	Target	Status
☐	Select pilot systems representing diverse use cases			
☐	Configure test environment with PQC algorithms			
☐	Implement ML-KEM for key encapsulation in pilot			
☐	Implement ML-DSA for digital signatures in pilot			
☐	Conduct performance benchmarking vs. classical crypto			
☐	Test interoperability with external systems and partners			
☐	Validate backup and recovery procedures with new algorithms			
☐	Document lessons learned and update migration playbooks			
☐	Obtain stakeholder sign-off on pilot results			
☐	Refine timeline and resource estimates based on pilot			

Phase 5: Production Deployment

	Task	Owner	Target	Status
☐	Execute phased rollout per migration schedule			
☐	Update certificate infrastructure to support PQC			
☐	Migrate key management systems to quantum-safe algorithms			
☐	Update TLS configurations across web infrastructure			
☐	Migrate VPN and network security to PQC algorithms			
☐	Update code signing and software distribution systems			
☐	Migrate database encryption to quantum-safe algorithms			
☐	Update identity and access management systems			
☐	Coordinate third-party and vendor migrations			
☐	Maintain hybrid mode during transition period			

Phase 6: Validation & Compliance

	Task	Owner	Target	Status
☐	Verify all critical systems are using PQC algorithms			
☐	Conduct security assessment of migrated systems			
☐	Perform penetration testing on PQC implementations			
☐	Validate compliance with regulatory requirements			
☐	Update security policies and procedures documentation			
☐	Complete third-party security audit if required			
☐	Obtain formal compliance attestation			
☐	Document evidence for audit trail			
☐	Update incident response procedures for PQC environment			
☐	Conduct tabletop exercise for quantum-related scenarios			

Phase 7: Continuous Improvement

Task	Owner	Target	Status
☐ Establish ongoing cryptographic monitoring program			
☐ Schedule regular cryptographic inventory reviews			
☐ Monitor NIST and industry for algorithm updates			
☐ Plan for SLH-DSA adoption for stateless signatures			
☐ Maintain vendor engagement for updates and patches			
☐ Conduct periodic staff training refreshers			
☐ Review and update migration documentation			
☐ Share lessons learned with industry peers			
☐ Plan for next-generation algorithm adoption			
☐ Establish metrics dashboard for quantum readiness			

Notes & Key Contacts

Additional Resources

NIST Post-Quantum Cryptography: csrc.nist.gov/pqcrypto
QRAMM Assessment Toolkit: qramm.org/toolkit
CISA Quantum Readiness: cisa.gov/quantum
NSA Cybersecurity Advisory: media.defense.gov