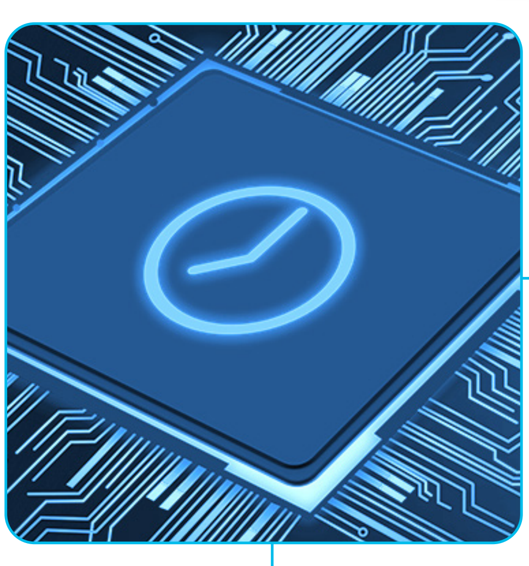
Getting Started on Your Post-Quantum Cryptography Journey

2024
Release of NIST Post-Quantum Cryptography Standard

2030-2035
Emergence of Cryptographically Significant Quantum Computers

2024-2030
Migration to NIST Post-Quantum Cryptography Standard

With the recent release of the NIST post-quantum cryptography standard, the clock has officially started for organizations to ensure the continued security of their essential data against the post-quantum threats. These tips are designed for organizations to prepare for their transition to post-quantum cryptography.



Strengthen Engagement with Standards Bodies

Actively engage with standards-developing organizations. Stay updated on the latest developments related to necessary algorithm and protocol changes.

Catalog Critical Data Assets

Identify and catalog critical data that may be at risk now and could be decrypted once a cryptographically relevant quantum computer becomes available. This will inform future risk assessments.

Audit Cryptographic Technologies

Conduct a comprehensive inventory of all systems using cryptographic technologies. This will facilitate a smooth transition to post-quantum cryptography.

Identify Quantum-Vulnerable Public Key Systems

From the inventory list, pinpoint where and for what purpose public key cryptography is being used. Mark these systems as quantum-vulnerable.

Update Internal Standards

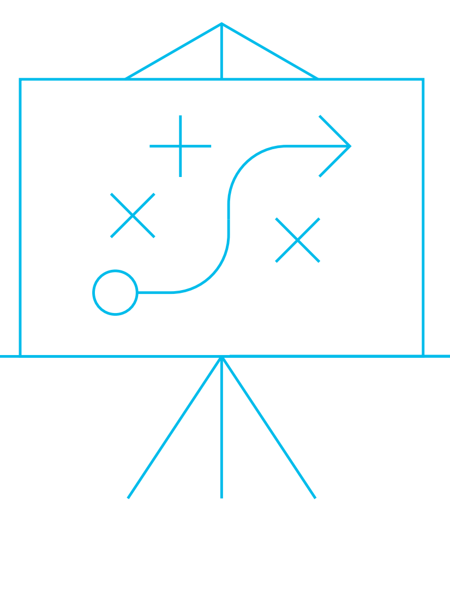
Identify and update acquisition, cybersecurity, and data security standards to reflect post-quantum requirements.

- Acquisition
- Cybersecurity
- Data Security

Evaluate Risk and Prioritize System Upgrades

Prioritize systems for cryptographic transition based on organizational functions, goals, and needs. Consider the following factors when assessing risk of a quantum-vulnerable system:

- Does the system qualify as a high-value asset according to the organization's risk assessment criteria?
- What types of data is the system safeguarding (e.g., key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
- What is the required duration for data protection?
- Which other systems does it interact with and what is the exposure if information is leaked to another party?
  - How much information does it share with federal agencies?
  - How much information does it share with external organizations?
  - Is it integral to any critical infrastructure sector?



Develop a Transition Strategy

Develop a transition plan for systems based on your inventory and prioritization information. Ensure the plan includes creating cryptographic agility to accommodate future adjustments and enable flexibility for unexpected changes.

Get Started Today!

- Now is the time to define your quantum-safe transition.
- Organizations need to assign clear ownership for PQC implementation.
- Investing in cryptographic technology is essential to protect your data.

For more information, visit www.cisco.com/go/pqc