Step-by-step PQC migration journey

A simple guide

The urgency of PQC migration

Regulatory bodies mandating PQC migration to start within next 12 months

e.g.
EU by end of 2026
UK NCSC by 2028
US to complete by 2035

Only 8Hrs

to crack 2048-bit RSA key

Current estimates suggest that a fault-tolerant quantum computer with around 20 million qubits could factor a 2048-bit RSA key in about eight hours, a task that would take classical computers roughly one billion years.

67% of people are worried that **quantum computing**

will break existing encryption before platforms fully implement **post-quantum cryptography**, according to a survey for the IT sector association, ISACA.

CTOs perspective

Where do I start the migration journey?

Jonathan Nguyen-Duy

Chief Technology Officer at Arqit

Brings over 25 years of cybersecurity leadership across Intel, Fortinet and Verizon.

He shares his perspective on the most critical steps to successfully begin your PQC migration journey.

Where to start?

Complexity has always been the enemy of security and will be a significant challenge as most enterprises have widespread cryptographic deployments, spanning network and security devices, servers, applications and clouds.

As with the start of all cybersecurity initiatives, we should begin by inventorying and assessing the current cryptographic state, classifying assets, criticality, and then prioritizing migration.

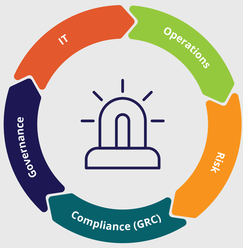
We should approach **PQC migration** like another **Y2K enterprise-wide IT initiative.**

With less clarity as there's no definitive end date when quantum computers will emerge with the ability to crack current encryption.

But that shouldn't lull us into complacency, as malicious actors have for years been stealing and storing data for future decryption.

These Store Now Decrypt Later (SNDL) attacks have been with us for some time, as evidenced by the targeting of submarine cables and global networks.

CISOs and security teams should consider building specific cross-functional migration teams spanning:



Step-by-step PQC migration journey

1 Inventory and Assess the Current State

Identify and inventory all the places cryptography is used in your organization, including public key infrastructure, algorithms, protocols, email/messaging, network services, applications, etc.

Teams should be mindful of the cryptography deployed, as well as other crypto tools provided by vendors in the form of cloud services, networking and security devices.

2 Prioritizing the Migration

With inventory completed, the next step is to assess the criticality of cryptographic assets that need to be migrated to quantum safe solutions. Considerations include regulatory requirements, potential impact of compromised data, business loss, and reputational loss. Start with less critical assets and progressively migrate the more important systems.

3 Develop an Agile Crypto Strategy

Determine an appropriate migration strategy that is designed to accommodate developments in algorithms and other forms of cryptography. While quantum resistant solutions based on NIST approved Post Quantum Algorithms (PQAs) are currently popular, your strategy should allow use of hybrid solutions using classical encryption, symmetric keys and PQAs. There's no singular solution for every organization, as migrations will vary depending on each organization's unique requirements and legacy cryptographic infrastructure.

Pay particular attention to whether you'll implement the PQC solution, rely upon vendor-provided products with cryptography, or some combination of both - ensuring the solution consistently meets the myriad of local, national, and global regulatory and standards requirements. Be especially mindful of existing cryptographic deployments, compatibility, and vendor reliance during and after the migration. This is where an agile crypto strategy comes into play – ensuring that you can switch algorithms and strategies with changes in technology.

4 Implementation and Testing

Continuously test and validate processes and performance throughout the implementation to ensure the migration is happening as planned and unforeseen issues are identified, such as compatibility, form factor flexibility and vendor lock-in.

5 Crypto Life Cycle Management

Security teams should also consider a PQC Posture Management solution to ensure continuous monitoring of cryptographic infrastructure for anomalous behavior, indicators of compromise, and vulnerabilities. Be mindful of vendor integrations and in-house systems to ensure robust protection for data at rest, in transit, and in process. A crypto posture management platform with threat detection and incident response capabilities will be valuable in managing the complexity of legacy and future crypto assets.

These are just a few ways to frame your PQC migration planning. Please feel free to contact Arqit for a deeper discussion.