digicert®

Your Quantum Readiness Playbook

What you need to do now to protect against the quantum computing threats of the near future

Quantum computers capable of breaking today's encryption are coming. Nobody knows the exact date, but the main players in the industry target 2029 or 2030 as the point when organizations need to have core systems ready. This means IT teams need to start planning immediately. These changes are non-negotiable, because they'll become the prevailing encryption methods. No matter the date or long-term implications of quantum, starting now makes adoption of Post-Quantum Cryptography easier and less expensive.

Here are the steps to take as you start.

Get executive buy-in

This project requires executive support to succeed. The sections below are the rough outline of your proposed plan. Why is it necessary and why start soon?

Here are some points worth making with your leadership team:

- The changes are mandatory. As the industry shifts, we'll need to implement PQC just to function.
- Customers are already asking us about our quantum security plans, and governments will eventually demand it.
- Moving now saves money, because it allows us time to plan properly and spread costs over a longer period of time.
- This project will expose many problems in our systems and processes that are already costing us money. Such things always happen with comprehensive programs like PQC migration.
- If there's no formal risk management process, this program can form the nucleus of a mature risk management process for our company.
- The threat of "Harvest Now, Decrypt Later" is a reality and has been for years. Implementing the proposed plan can arrest its progress.

Form a task force

This will be a long-term project that will need people to focus on it. Create a team to connect security operations, architecture, PKI, infrastructure, application owners, vendor management, and risk stakeholders. They should build the strategic foundation—visibility, cryptographic agility, governance, and supplier engagement—but also select practical, low-regret technical steps that generate evidence. Therefore, the members of the team will need a variety of skillsets from across IT.

When it comes to leading the team, someone technical enough to understand the PQC issues and the company's operations should be in charge and responsible for tracking progress. Consequently, they should have authority and sufficient access to senior management.



When it comes to leading the team, someone technical enough to understand the PQC issues and the company's operations should be in charge and responsible for tracking progress. Consequently, they should have authority and sufficient access to senior management.

Inventory your cryptographic infrastructure

The standard approach to these migrations begins with an inventory, and you need one for PQC migration. That can mean a lot of work for a large organization, but keep in mind, you don't need a comprehensive inventory to start. The team should agree on one important, representative application and create an inventory for it. The inventory needs to include client and server network connections (TLS), keys, certificates, cryptographic libraries, vendors, hardware, firmware, and software.

All public key (asymmetric) cryptography will be using vulnerable algorithms. If you don't yet have full buy-in from leadership, use the inventory to show the scale and complexity of the work ahead.

That said, don't wait for a comprehensive inventory that spans your entire enterprise since doing so will block progress. Begin by communicating a broadly defined plan to stakeholders, by working on the migration for one key application, and by following the next two steps (in sequence).

Migrate to TLS 1.3

The first technical change you need to make to start building towards PQC is to migrate all networking to TLS 1.3. This has been the current and preferred standard for many years, but there's still a lot of TLS 1.2 out there, and none of it will support PQC algorithms.

This task has the benefit of being possible today, and many companies have achieved it. You can use tools like DigiCert Quantum Central to inventory assets and identify those that need upgrading. You'll need to work closely with your vendors to address the problems you will probably find.

> *"PQC exposes technical debt that already exists. That's not a reason to wait. It is precisely why starting early matters."*
>
> **Christian Pfister**
> Lead, Quantum Safe Competence Center, LGT Financial Services

Enable hybrid key exchange

The first thing two systems must do before establishing a TLS connection is to exchange cryptographic keys. Our networks have been using Elliptic-curve Diffie Hellman (ECDH) as the key exchange for a long time, but that protocol is vulnerable to quantum attacks. The agreed quantum-safe protocol for replacing it is ML-KEM. This new protocol has been in widespread real-world use by major players like Google and Cloudflare since 2024, and it's already considered a proven technology.

Because you'll need to support ECDH for now, there is a hybrid mechanism called ML-KEM-25519 (formally X25519MLKEM768) that prefers ML-KEM but also supports ECDH to maintain interoperability with current systems. You'll need to work with your networking vendors to plan for implementing it. Like TLS 1.3, this is possible today, and many companies have accomplished it.

There is the added benefit that ML-KEM and ML-KEM-25519 traffic isn't vulnerable to "harvest now, decrypt later" attacks. With hybrid implementations, you can achieve this relatively quickly for internal systems and be ready as other parties add their support.

Create test environments

The preferred PQC algorithm standards are set, but other PQC standards and implementation details are still being finalized. The preferred digital signature algorithms have reached a stage where you can begin testing them for your environment. You should create test instances separate from your production systems for this. DigiCert Labs created an ML-DSA Web Server that you can use as a foundation at no cost. There are potentially significant performance implications to ML-DSA owing to its much larger key and signature sizes. To address this, a new certificate scheme called Merkle Tree Certificates is under development for public web servers.

It may be tempting to test performance, but this can't be your first priority. Make sure you can get your applications working with the new PQC standards, starting with conventional ML-DSA certificates. Then you can worry about performance.

Build a plan for PKI

The PKI side of quantum readiness will be the larger and more complex part of the migration. While the core PQC algorithms are set, standards for PQC certificates are still evolving and will likely differ across public TLS, digital signature use cases, and constrained environments like embedded devices. Your organizations should expect to operate multiple PKIs during the transition, and potentially long afterward. This will make PKI governance and certificate lifecycle management exponentially more complex. Now is the time to modernize.



PKI is the larger and more complex part of the migration. The solution to complexity is automation.

The TLS and ML-KEM transitions are easier because the affected systems are easier to identify, and responsibility falls to a relatively small number of IT staff.

Implementing ML-DSA in place of RSA will affect large numbers of applications, and certificates may be distributed across the enterprise. This is why a complete inventory is necessary.

Lower the cost of management by starting earlier

Because the date of quantum supremacy is unknown, the sooner you start, the longer you have to work, which helps you avoid disruptive and expensive acceleration to full migration. Adopting TLS 1.3 and hybrid key exchange are worthwhile measures on their own and the right place to start. Developing a test lab for your application migrations will make them happen more smoothly as vendor support expands. ML-KEM and TLS 1.3 are table stakes for this lab, but the important testing will be for ML-DSA with your applications.

Finally, as you plan, consider the prospect of such a widespread and complex transition in a compressed timeframe where an attack from a quantum computer isn't necessarily the pressure point. All it takes is regulators or important customers demanding evidence that you are making progress to compel sudden acceleration in your quantum readiness. While you're considering your own state and plan, consider asking your own vendors the same questions in turn.

Summary

You still have time to plan and execute a migration to quantum-resistant cryptography. There are changes you can and should make right now that will represent real progress in that project. But your time to do all this at a reasonable cost and pace is running out.

This work is not optional. The indications from governments and key vendors are that actual requirements to support PQC are coming within a few years.

If you start soon, you can plan to execute it over several years, making the transition to a secure quantum era easier, less expensive, and more manageable.



Quantum Central unifies cryptographic inventory and helps turn it into action for quantum readiness and overall cryptographic posture management. Request a free 60-day trial to start executing your playbook.

Get started today >

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.