KEYFACTOR

# The 10-Step Checklist for Tech Leaders

## Simplify Your Transition to New NIST Algorithms

You may have heard that the National Institute for Standards and Technology (NIST) recently standardized three new post-quantum algorithms to counter the threat quantum computers pose to traditional cryptography.

Quantum computers will eventually be able to break current cryptographic methods, and the new NIST standards are here to address this risk. But how do you implement these standards? Where do you start?

The key is crypto-agility.

Prepare NOW by following this 10-step checklist to ensure your systems and data are protected.

## Explore the PQC Lab

**Ready to quickly test quantum-ready certificates?**

As part of our mission to support your post-quantum efforts, we invite you to check out PQC Lab.

This first-of-its-kind offering was designed for you to get hands-on with post-quantum cryptography in a safe sandbox environment, without the effort or expense of setting it up yourself.

Enter the PQC Lab ↗

### Understand the new standards.

Familiarize yourself with the new NIST algorithms and their implications for your organization.

### Establish visibility.

Most businesses are unaware of the scope of the problem. To start the path to quantum readiness, it's on IT and security teams to build an inventory of all the systems and applications that rely on cryptography, including certificates and algorithms.

### Plan your transition strategy.

Develop a detailed plan for transitioning to the new standards, including timelines and milestones. As part of this, be sure to allocate necessary resources (e.g., personnel, budget, tools).

### Engage stakeholders and educate staff.

Communicate the transition plan and its importance to all relevant stakeholders, including security teams and executives. Work to identify potential risks associated with the transition and develop mitigation strategies.

### Test algorithms.

Set up a testing environment for the new algorithms and identify potential issues. Establish performance benchmarks to compare your new vs. existing algorithms.

### Update crypto libraries.

Ensure all cryptographic libraries are updated to support the new NIST algorithms. Remember to regularly validate the integrity and security of cryptographic libraries to prevent tampering.

### Identify risks and priorities.

Prioritize systems and applications based on their criticality to start swapping out encryption algorithms. The place to start is with critical data that can be harvested now and later decrypted by a future quantum computer, or digital signatures that are trusted for a long time, such as firmware on long-lived IoT devices, roots of trust, and so on.

### Upgrade, upskill, and test again.

Software vendors, hardware providers, and enterprise IT organizations should start exploring how to incorporate these new algorithms into their products and systems now, as it will take serious effort, upgrades, and new skills to implement them.

### Enable automation and migrations.

Being ready to make swift changes to cryptography is the new norm; the key is to make the transition as smooth as possible. That's where automation can help. By automating processes, such as replacing a certificate with one issued from a PKI that supports quantum-resistant algorithms, it's possible to swap encryption at scale and without disruption. That's crypto-agility.

### Monitor and adjust.

Continuously monitor the transition process and make adjustments as necessary to address any challenges that arise.