THALES

Building a future we can all trust

Post-Quantum Mitigation Plan

Many organizations are now faced with getting ready for compliance with PQC regulations. It's no small task

to overhaul your cryptography. How does one begin to make sense of such a large undertaking? Here's a handy set of steps to help you get started.



Vulnerable Crypto

1

- Documented CBOM that includes key lengths, location, etc.
- Partner Integrations

Set up a test environment

Ecosystems that are standards dependent

• Today, time for PoCs, experiments, announcements

Test on priority applications

Take a hybrid approach by using classic & quantum-safe crypto solutions

Algorithms - Support for alternate modes with classical algorithms and QRA

Changing algorithms, protocols, key formats is **not easy**, can be **costly**, and **takes time**

RNGs - Combine QRNGs with NIST-certified RNGs Integrate with QKD per ETSI As Standards are approved, implement and re-certify

Remain flexible with Crypto Agility

Testing your priority applications and use cases to determine how the changes will impact your organization is critical. Learn more about Thales PQC Starter Kits today.

1 1



Network Encryption Starter Kit



HSM Starter Kit

cpl.thalesgroup.com

