


Post-Quantum Cryptography Assessment

How Crypto Agile Are You?

With the quantum threat approaching, organizations need to prepare now to mitigate cryptographic security risks and encrypt long-term sensitive data securely. Organizations can prepare by taking our post-quantum cryptography readiness assessment and become crypto-agile.

 <h3>How We Can Help</h3> <ul style="list-style-type: none"> ■ We take a deep dive into your critical data. ■ We explain quantum computing trends and what it means to be crypto-agile. ■ We help you adopt hybrid post-quantum cryptography solutions today and prepare for the new ciphers as they are finalized by NIST in 2024. 	 <h3>Am I Secure? Key Questions to Ask</h3>  <ul style="list-style-type: none"> ■ Where is our environment vulnerable? ■ What data is vulnerable to near exposure? ■ What is the current state of quantum computing and how soon may regulators require upgrades to cryptography?
---	---

Assess Your Crypto-Agility

We help you prepare long before a problem occurs by planning, implementing and testing cryptographic solutions. We outline four steps to migrate to Post-Quantum "Safe" Cryptography:

01 Manage Your Data

- Classify critical data at rest and in motion
- Understand your data life cycle and how long you must protect it

04 Become Crypto-Agile

- Update your development lifecycle for new cryptography standards established
- Consider current post-quantum computing solutions for critical data



02 Know Your Crypto

- Identify your existing cryptography inventory and understand how quantum computing will affect it
- Comprehend your third-party vendors' cryptography environments

03 Abstract It Out

- Determine your lead times to update your vulnerable cryptography
- Know your cryptography hardware and software and which components are hard coded

Quantum Applied to Cybersecurity Challenges



Prepare Now with Our Quantum Solutions

We help clients maximize the benefits of quantum with an end-to-end approach. The risk of ignoring quantum computing can result in several losses:



Disruption of Business



Cybersecurity Risk



Encryption Risk



Reputational Risk



Competitor Risk



What is the Quantum Threat?

The quantum threat to cryptography emerged in 1994 when Peter Shor invented a quantum algorithm to break the RSA cryptosystem— a public-key cryptosystem that is used for secure data transmission.

Although the Advanced Encryption Standard (AES) that we use today will not be broken by quantum computers, it can be weakened, and once we increase the algorithmic power of quantum technology, our current public-key cryptography will become defenseless against security threats.

Organizations must prepare now to become crypto-agile and defend against quantum security threats as this technology evolves.



Explore Our Quantum Solutions



Quantum-Inspired Use Case

Achieve ROI today while learning quantum-inspired techniques that run on today's classical hardware



Quantum Business Proof of Concept

Build the code necessary for portfolio optimization, fraud detection and vehicle routing



Post-Quantum Readiness Workshop

Assess your readiness for the arrival of quantum computing and explore potential use cases for your industry

Let's Transform Together.



Protiviti.com/TechnologyConsulting



TechnologyConsulting@Protiviti.com



TCblog.Protiviti.com