Deloitte.

5x5 series: Insights and Actions

# Quantum Cyber Readiness: Achieve resiliency in the Quantum Era

Quantum technologies have the incredible potential to accelerate your organization's ability to reach its ambitions. For example, they enable advanced simulations and modeling or provide sensing capabilities that yield advanced analytics. Nevertheless, it can also be a risk, with attackers leveraging the powers of future, sufficiently powerful quantum computers to decrypt your most valuable data. One thing is for sure: the best time to start preparing for a quantum-secure tomorrow is today. Deloitte is here to guide you every step of the way, with an experienced team ready to help you understand the risks, preparefor your transition, and assist you in transforming your organization to confidently enter the Quantum Era.

## 5 things you should know

1 **Quantum computers threaten the security of your data.** A lot of today's digital data traffic is protected using cryptography that takes today's computers thousands of years to break. However, Shor's algorithm, developed in the 1990s, demonstrated how future quantum computers will be able to break that cryptography in just seconds.

2 **The threat is now.** Although it is uncertain when sufficiently powerful quantum computers will emerge, adversaries may already be targeting organizations in Harvest Now, Decrypt Later (HNDL) attacks, wherein they steal your data today with the intent to decrypt it with quantum computers in the future.

3 **Becoming quantum-secure will take a long time.** While organizations may feel like they have time to prepare, previous large cryptographic migrations (e.g., 3DES to AES) have taken a decade or more to complete. Starting too late can mean a quantum computer maybe able to break the vulnerable cryptography you have yet to replace.

4 **Regulators will act.** It is likely that quantum-secure cryptography in the future will be required by regulators, which are still waiting for the standardization of quantum-secure cryptographic algorithms. US federal organizations are already being required to prepare to become quantum-secure.

5 **Being an early adopter can accelerate your business.** Starting now with your quantum-security journey can increase trust amongst your customers who want their valuable (personal) data to be in good hands and can strengthen your name as an industry leader with your competitors likely to follow suit.

## 5 actions you can take

1 **Educate your teams and build awareness** around the risk that quantum computers may pose to your cybersecurity and why it is relevant to act. This awareness should extend from the operational level to leadership to ensure broad support for the investments required for a quantum-security transition.

2 **Take inventory of which data in your organization is at risk.** Identify valuable and long-lived data in your organization and assess whether it is protected with cryptography that will likely be rendered obsolete once sufficiently powerful quantum computers arise.

3 **Review the governance mechanisms in place and catalog gaps** to effectively change cryptography in your organization, such as cryptographic policies and responsibilities. These are essential to be in continuous control and be 'crypto agile' in implementing new cryptographic algorithms as they become available.

4 **Experiment with implementing quantum-secure algorithms in a pilot.** This gives you an idea of what to expect when the time comes to implement them throughout your organization, such as unexpected challenges, dependencies, and success factors you might currently be unaware of.

5 **Reach out to our Quantum Cyber Readiness team** to take the first step toward resiliency. Learn how a Quantum Risk Assessment can help you understand your quantum risk and provide you with a practical way forward.

### Learn more from these additional resources

Quantum Cyber Readiness | Deloitte US

### Connect with us


**Colin Soutar**
Managing Director, US Quantum Cyber Readiness Leader
Deloitte & Touche LLP
csoutar@deloitte.com

**Chris Knackstedt**
Senior Manager, US Quantum Cyber Readiness
Deloitte & Touche LLP
cknackstedt@deloitte.com

**Benjamin Shapiro**
Senior Manager, US Quantum Cyber Readiness
Deloitte & Touche LLP
beshapiro@deloitte.com



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2024 Deloitte Development LLC. All rights reserved.