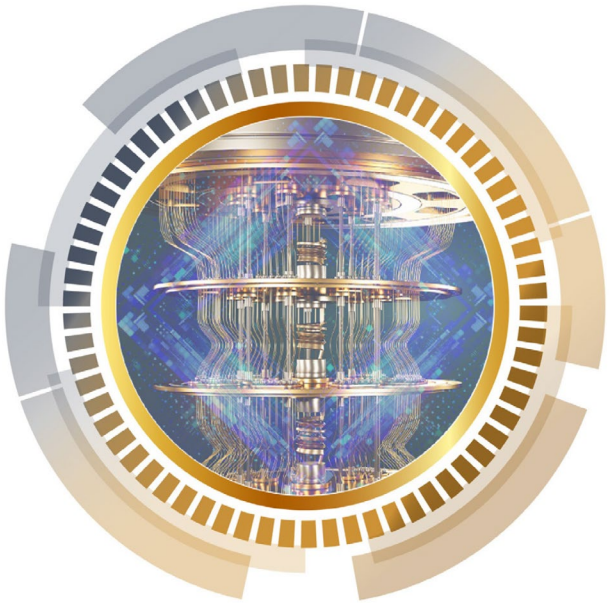
Deloitte.



Future forward readiness

Quantum cyber readiness

Navigating uncertainty and achieving resilience in the quantum era

While quantum technologies have the incredible potential to accelerate your organization's ability to reach its ambitions, it can also be a threat, with attackers leveraging the powers of quantum computers to steal and decrypt valuable data. One thing is for sure: the best time to start preparing for a quantum-safe 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 and implement quantum-resistant cryptographic algorithms to protect your organization and data, now.

Current trends

New applications and use cases for quantum technologies are being explored every day, yielding an unprecedented opportunity to create new business value. And while quantum computers are unlikely to be a general replacement for today's machines, their new processing power will enable organizations to solve tough problems, from the simulation of complex scenarios to solving optimization problems and training AI models.

A lot of encrypted data is protected using cryptography that could take today's computers thousands of years to break. However, Shor's algorithm, developed in the 1990s, proved how powerful quantum computers could break that cryptography in just seconds.

The exact date that sufficiently powerful quantum computers will emerge is uncertain, yet adversaries may already be targeting organizations in Harvest Now, Decrypt Later (HNDL) attacks, wherein they steal data today with the intent to decrypt it with quantum computers in the future.

While organizations may feel like they have time to prepare, previous cryptographic migrations (e.g., 3DES to AES or MD5 to SHA1) have taken a decade or more to complete.[1]

Desired outcomes

Becoming quantum cyber ready can yield several benefits, including:

Reduced risk of security incidents that can lead to loss of data (e.g., personal data and intellectual property), which can result in damage to your organization, as well as regulatory and legal penalties.

Improved compliance with anticipated regulations and security standards requiring that organizations have quantum risk measures and mitigation plans in place.

Increased perception as a market leader through early adoption and preparedness against emerging quantum threats, with competitors likely to follow suit.

Increased crypto-agility, enabling your organization to promptly respond to evolving security threats in an efficient manner, with the flexibility to update algorithms and comply with new standards quickly.

Deloitte can help your organization achieve an enhanced security posture as threats and disruptions grow. With services across the advise, implement, and operate spectrum, Deloitte can help you forge a better balance between intel-driven prevention and battle-tested response to reach greater operational efficiency.

Quantum cyber readiness in action

Data integrity in financial institutions
Trust in the integrity of financial data is essential to provide financial services. Financial institutions must become quantum-secure to prevent hackers from reading or changing financial data, which can result in public security incidents and plummeting consumer trust.

Device security in health care
Patient data can remain sensitive for decades, and health care providers process this data on large amounts of connected devices, such as insulin monitors. Health care providers should make these devices quantum-secure to ensure the safety of their patients.

Regulatory compliance
Compliance with pending regulations is essential. Organizations should understand quantum risk and work toward the National Security Memoranda[2] and developing laws such as the Quantum Cybersecurity Preparedness Act.[3]

Business continuity in the energy sector
Recent ransomware attacks have demonstrated how seriously advanced threat actors can disrupt business continuity. Energy providers should act to understand their quantum risk and be in control of advanced, emerging threats.

Quantum-secure networks in telecommunications
The confidentiality, availability and integrity of communications are essential for consumers and businesses. Telecommunications providers should innovate and explore quantum-secure networks to ensure these networks maintain their fidelity.

Crypto-agility with consumer goods
Speed and efficiency in delivering goods can yield a vital edge over competitors. Consumer goods providers should consider implementing crypto-agility so they can spend less time responding to evolving security threats and focus on the consumer.

1. Computing Community Consortium (2019) *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*.
2. Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility - CCC (cra.org)
3. Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems - The White House National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems - The White House

Turn complex challenges into opportunities

Our industry-tailored approach enables us to apply the right solutions to your precise business challenges.

When you're looking for global leadership

Deloitte is recognized as a global leader in the quantum risk space. With our strong expertise, we support the World Economic Forum's global Quantum Security Initiative.

When you need a strong ecosystem of partners and alliances

We have strong alliances with leading technology vendors, and work with industry sectors, research organizations, and government agencies to provide leading insights, share intelligence, and collaborate.

When you need a one-stop quantum shop

While navigating the uncertainty of the quantum era, the breadth of our services allows us to provide you with an expansive solution to help you move forward and achieve the outcomes most critical to your organization, wherever you are in your quantum cyber journey.

We're well positioned to help you achieve your objectives

Wherever you are in your journey, we have the experience, knowledge, and tools to help move your organization forward.

Outcomes-driven

In the face of growing complexity, we make finding a Cyber & Strategic Risk provider easy. Our breadth and depth allow us to provide the outcomes (and value) you seek as a trusted advisor, a technology-savvy pioneer, a visionary integrator, and a dependable operator. We connect the dots, so you don't have to—helping you to improve security, trust, and resilience.

Quality-oriented

We bring together a powerful combination of proprietary technology, domain experience, leading alliances, and industry knowledge to deliver better. Our obsession with quality means we consistently work to help realize your vision, because Cyber & Strategic Risks are mission critical.

Value-focused

We act as a leader in times of crisis, a teammate to help you navigate change, and a force to have your back when you are on the front lines. We create value for our clients beyond the deal, pioneering cutting edge resources and innovation, paving the way for forward leaning collaboration, and leading bold thinking on tomorrow's emerging technologies so you can turn risks into opportunities.

Future forward readiness

Quantum cyber readiness in action

Quantum risk assessment

Our expansive risk assessment is designed to help you understand your organization's risk exposure to quantum computer attacks and identify which data, applications, and networks may be most vulnerable.

Quantum readiness design and roadmap

Our experienced specialists will help you prepare for your quantum readiness transition by defining ambitions, designing a future state operating model, and planning an actionable path forward.

Quantum training

We organize trainings and workshops to help you ensure that your team is equipped to understand and act on quantum risk in ways tailored to their role.

Quantum readiness implementation

We will help you to successfully implement quantum-resistant cryptography across your network, as well as the required governance to ensure that you maintain continuous control of cryptographic risks and become quantum cyber ready.

Engineered for

Chief Information Security Officers

Ensure your most critical data and systems are secure and ready for the quantum era.

Chief Risk Officers

Be in control of the complete picture of risks to your organization, which includes quantum risk.

Chief Technology Officers

Create more efficiency in the development and management of your IT assets through crypto-agility.

Start the conversation

Deborah Golden
Principal, US Cyber & Strategic Risk Leader
Deloitte and Touch LLP
debgolden@deloitte.com

Chris Knackstedt
Senior Manager, US Quantum Cyber Readiness team
Deloitte and Touch LLP
cknackstedt@deloitte.com

Colin Soutar
Managing Director, US Quantum Cyber Readiness Leader
Deloitte and Touch LLP
csoutar@deloitte.com

Ryan Kaiser
Senior Manager, US Quantum Cyber Readiness team
Deloitte and Touch LLP
rykaiser@deloitte.com