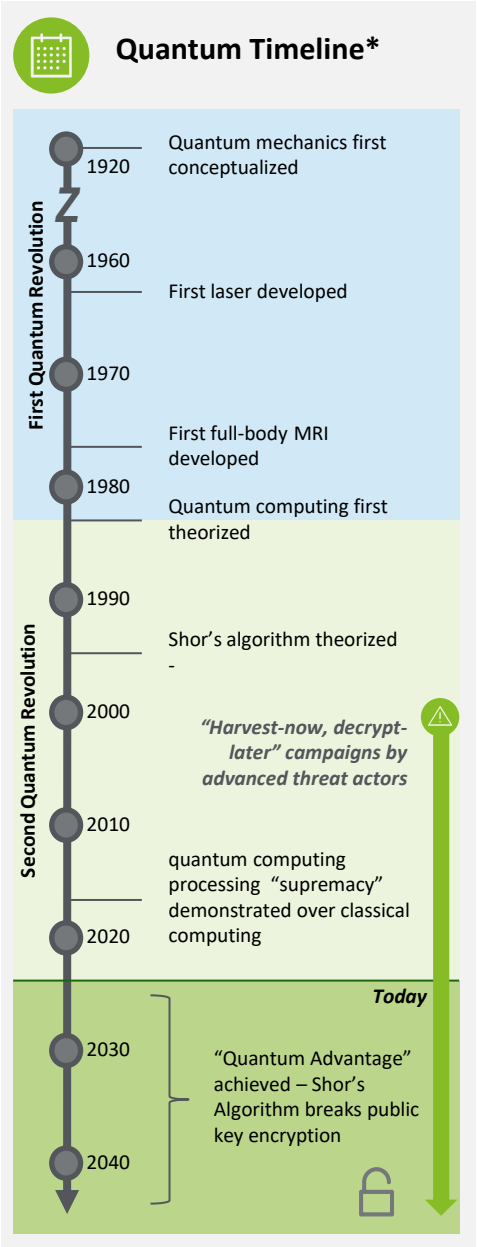
Deloitte.

Future Forward Readiness: Quantum Risk

Quantum opportunities and risks today and how to prepare for tomorrow

Emerging technologies consistently endeavor to address many pressing problems, giving many a sense of both inspiration and skepticism. Quantum technologies are no exception. For many, the word "quantum" is more likely to conjure thoughts of science-fiction than one of today's news headlines. Yet, what exactly does "quantum" really mean? When will it be mainstream? And most importantly, what are the impending risks and opportunities that quantum may bring?

The 2nd quantum revolution is upon us



Quantum mechanics explains foundational concepts of how basic matter exists, changes, and interacts over time. These concepts were first conceived in the 1920s and started the quantum revolution. Those initial discoveries fascinated scientists for the next several decades and inspired groundbreaking innovations such as lasers, semiconductors, and magnetic resonance imaging (MRI) systems.

More recently, a second quantum revolution has been underway, garnering attention for advanced applications such as quantum computing, quantum sensing, and quantum communications. Though their capacity to drive high-impact use cases is currently narrowed by the nascency of today's quantum hardware, these newer applications theoretically hold transformative potential. It is also important to note that these applications and their development timelines are uniquely evolving with prospective use cases.

Quantum Security Risks

Quantum computing's large-scale computational capabilities may also enable significant disruption to the information security frameworks widely used today. In 1994, an algorithm developed by MIT mathematician, Peter Shor, became the theoretical basis of how quantum computers could eventually break some of today's current cryptographic algorithms with large number factorization. Given its predication on the inability to achieve such factorization, public key encryption is put squarely at risk by Shor's Algorithm.

Although there are various opinions on when quantum computers will be able to break current-day cryptography standards, it is believed that data is being captured and stored today for decryption tomorrow – in so-called "harvest now, decrypt later" attacks. This situation is forcing organizations to better understand the potential impacts of quantum to their current data and assets, forcing many to begin evaluating capabilities to establish quantum-resistant cryptography to confirm sensitive data and transmissions are impervious to the looming capabilities of quantum computers.

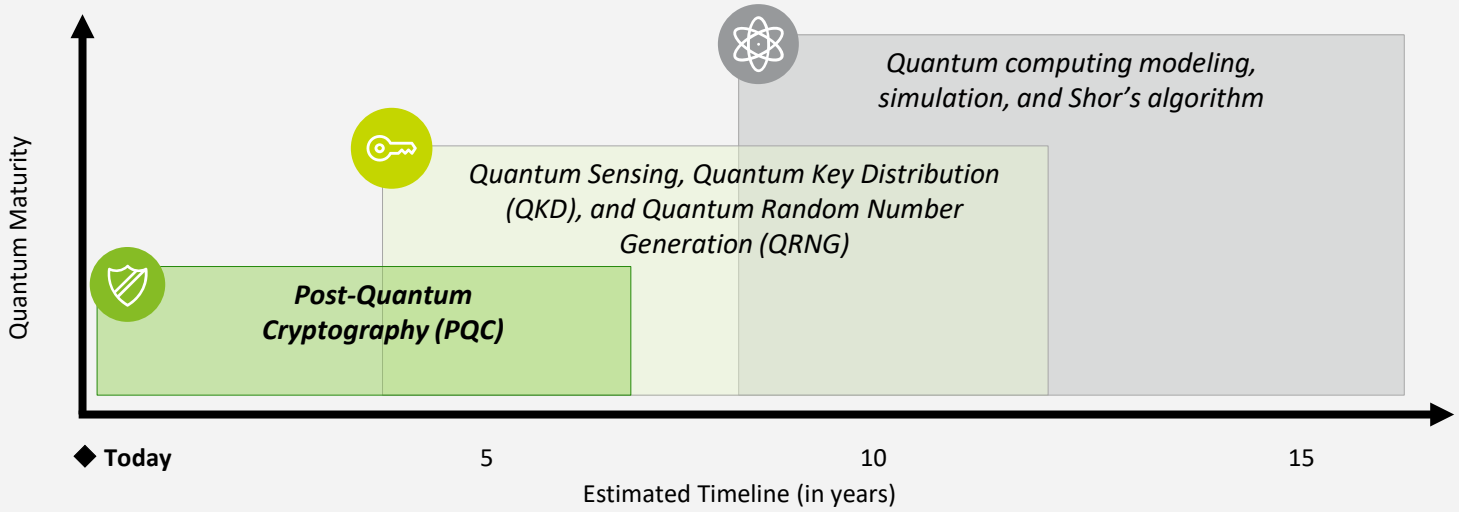
**Timeline dates and forecasts developed from the following sources:*

1) Stein, Ben P. "The History and Future of Quantum Information" www.NIST.gov. 2019, https://www.nist.gov/topics/physics/introduction-new-quantum-revolution
2) Forrester. (2021) The CISO Guide To Quantum Computing Risks;
3) Gartner. (2020) Predicts 2021: Disruptive Potential During the Next Decade of Quantum Computing;
4) Deloitte internal analysis and quantum risk industry participation

The market for quantum-resistant encryption solutions

As the market for quantum encryption technologies continues to mature on pace with the underlying quantum technologies driving their respective capabilities, three (3) distinct categories of quantum –resistant risk solutions are emerging: 1) Post Quantum Cryptography (PQC); 2) Quantum Random Number Generation (QRNG); and Quantum Key Distribution (QKD).

Quantum Cyber Risk Solutions Capability Maturity Outlook



Post Quantum Cryptography (PQC)

PQC generates cryptographic algorithms that are resistant to quantum computing algorithms such as Shor's algorithm and has been under development by the National Institute of Standards and Technology (NIST) and others for several years. Unlike public-key encryption algorithms, PQC algorithms do not use integer factorization, discrete logarithm, or elliptic-curve discrete logarithm problems, which could be broken by quantum computers running Shor's Algorithm. Notably, PQC algorithms can run on today's traditional computers rather than quantum machines. PQC will likely be the dominant market solution for quantum resistance and is likely to be the solution of choice for the US Government. NIST is set to release a first draft of PQC standards as early as this year and 2024 for standardized release.

Quantum Random Number Generation (QRNG)

QRNG is a quantum technology that harnesses the laws of quantum physics to produce truly random numbers as opposed to pseudo-random number generators which use computer programs to generate probabilistic random numbers. QRNG is not only being considered in cryptography solutions but also in simulation, optimization and other machine learning (ML) applications as the source for high-entropy randomness generators.

Quantum Key Distribution (QKD)

QKD is a quantum hardware-enabled secure communications method that enables shared parties to encrypt and decrypt messages by producing a key only known and accessible between them. This method uses properties derived from quantum physics to exchange cryptographic keys in a significantly more secure way against quantum-era decryption than conventional secured communications. Though QKD may be used to augment the secure transmission of crypto algorithms, PQC algorithms are still required to do so. In addition, the establishment of QKD keys generally requires a separate trusted channel to be established.

Quantum technologies will likely require significant revisions to the bedrock of informational security. While QKD and QRNG solutions will likely evolve with advancements in quantum technology, PQC's compatibility with classical systems offers an immediate and effective alternative to begin safeguarding against emerging quantum threats today.

Build Crypto-Agility as the market continues to take shape

NOW: *Take proactive steps to identify and prepare for quantum-era threats*

- ✓ **ASSESS FOR IMMEDIATE IMPACTS FROM POTENTIAL DATA HARVESTING EVENTS**
  - Discover assets and reinforce their security stature against current threats
- ✓ **EVALUATE AND UNDERSTAND YOUR QUANTUM-RISK PROFILE AND POTENTIAL VULNERABILITIES**
  - Conduct organizational quantum-risk assessment to understand potential direct impacts of quantum
  - Create an inventory of cryptographic assets aligned with prioritized list of high value assets
- ✓ **ROADMAP ORGANIZATIONAL STRATEGY & GOVERNANCE PRIORITIES FOR THE QUANTUM-ERA**
  - Align and appropriate frameworks for quantum spend against other budget priorities
  - Identify an implementation timeline and the required resources
  - Anticipate looming compliance and regulatory standards for the quantum-era
  - Build agile and broad strategic principles to withstand major market and technology developments

NEXT: *Evaluate, pilot and scale quantum security solutions against quantum risk use cases*

- ✓ **PILOT POST-QUANTUM SOLUTIONING**
  - Keep valuable assets protected from quantum-era decryption threats with quantum resistant technology
  - Evaluate and document use cases and potential solutions including Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG)
- ✓ **FOSTER ORGANIZATIONAL QUANTUM AWARENESS**
  - Quantum workshops and labs help build organizational awareness from the ground up
  - Establish communications plan to be used within the organization and with external customers and partners
- ✓ **INVESTIGATE WAYS TO ENABLE CYBER SECURITY FRAMEWORK WITH QUANTUM OPTIMIZATIONS**
  - Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), and Quantum Random Number Generators (QRNGs) have potential to integrate within existing cyber operations
  - Identify cases where interim implementations are required to maintain interoperability during migration

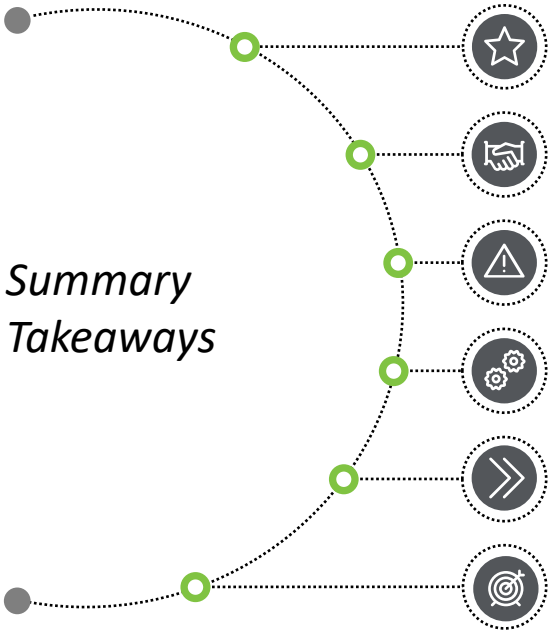
LATER: *Operationalize crypto-agility capabilities to respond to evolving advancements and guidance*

- ✓ **CONFIRM ONGOING MANAGEMENT OF NEW AND EXISTING QUANTUM-ENABLED SOFTWARE APPLICATIONS**
  - Routinely scan for, update, test, and assess cryptography to maintain quantum security posture against evolving guidance and technology
  - Update and manage the processes and procedures of developers, implementers, and users
- ✓ **QUANTUM APPLICATIONS FOR CYBER-AI AND ML**
  - Begin experimenting with quantum computing to find opportunities to leverage computing capacities for detection and response use cases
- ✓ **PRIORITIZE FINDING, ATTRACTING, AND SUPPORTING QUANTUM TALENT RESOURCES**
  - Facilitating talent pipelines with leading academic & research bodies can be critical to finding quantum professionals
  - Investing in in-house quantum programs to educate and support existing personnel on quantum subject matter

Taking proactive measures to address the immediate and eventual threats produced by quantum computing can help confirm that your organization is "crypto –agile"

Summary

Organizations should prepare for a future in which quantum technologies substantially impact security and operational frameworks. While today's quantum computing capabilities may be constrained, significant progress is anticipated over the next few years. While many organizations may wait to take action, their data may already be under threat today due to harvest now and decrypt later attacks. Forward-looking stakeholders now have the opportunity to use today to prepare for tomorrow's quantum impacts.



Quantum computing is imminent: while timing is still unclear, a quantum computer will likely be able to break current public-key cryptography

The threat may be more immediate: Sophisticated threat actors are harvesting data now to decrypt later when quantum is more mature

Build crypto-agility: Redefining how you manage cryptography capabilities can help protect against an evolving threat landscape

Understand your quantum risk NOW: Discover and classify specific data and cryptographic assets and evaluate potential risk to the organization

NEXT Plan, pilot and implement quantum risk solutions: identify use cases and risk solutions, evaluate tools and operationalize

Establish a repeatable process LATER: stay up to speed with evolving guidance and standards, monitor your environment and update as needed

Engage with Deloitte

How Deloitte can help

Deloitte helps clients design build, and operate dynamic, business-aligned security programs for each stage in their cyber journey. Services that aligned to quantum preparedness include, but are not limited to, the following:

- **Quantum Risk Assessments & Vulnerability Scanning (organizational and 3rd party)**
- **Cryptographic Asset Scanning & Inventory**
- **Quantum Risk Solution Evaluation and Selection Support**
- **Post Quantum Cryptography Software Implementation and Operations Management**

Along with a catalog of over 30 adjacent cyber risk services including zero trust, data governance and attack surface management.

The Deloitte difference

- **Global leadership:** Deloitte is a leader in the quantum risk space – we were selected to support the World Economic Forum's global Quantum Security Initiative.
- **Ecosystems & alliances:** Strong alliances with leading technology vendors, industry organizations, government, and research entities to provide leading insights, intelligence, information-sharing and collaboration
- **Outcomes Driven:** In the face of growing complexity, our breadth and depth allows us to provide the outcomes and value you need
- **Quantum computing experience :** leading consulting practice actively working to commercialize quantum applications

Contact us

Deborah Golden
Principal, US Cyber & Strategic Risk Leader
Deloitte & Touche LLP
Tel: + 1 571 882 5106
Email: debgolden@deloitte.com

Colin Soutar
Managing Director, US Quantum Cyber Readiness Leader
Deloitte & Touche LLP
Tel: + 1 571 447 3817
Email: csoutar@deloitte.com