Deloitte.

Quantum Trust

The essential combination of Zero Trust and Quantum Readiness

July 2023

Quantum Trust

With recent Federal mandates to migrate to a Zero Trust (ZT) architecture[1] and Post-Quantum Cryptography (PQC),[2] the US Government is aggressively transforming how it approaches information security. However, the success of this transformation will depend on how organizations integrate these two initiatives. Specifically:

- ZT reflects a significant paradigm shift in how infrastructure, networks, and data are secured.[3]
- This paradigm shift relies on the ubiquitous use of strong encryption.[4]
- This foundation of secure encryption will likely be undermined by quantum computers, capable of breaking much of the public-key cryptography used on digital systems around the world.[5]
- While a shift to a ZT approach is essential to enable effective, modern information security, migration to PQC is critical to success.
- By both incorporating cryptographic agility—“crypto-agility”—into all ZT pillars and addressing the ZT pillars as part of quantum readiness, organizations can enhance innovation and system modernization, reducing costs and time and improving security.

The Essential Combination of Zero Trust and Quantum Readiness Efforts

Despite the fundamental threat quantum computers pose to the cryptography underlying modern information security and ZT efforts in particular, little guidance exists on how to evaluate and address this risk.

However, the challenges super-imposed on systems by ZT and quantum readiness present a unique opportunity for innovation and system modernization—and importantly—also provide a roadmap for success. Specifically...

There is zero trust in Zero Trust without quantum readiness

If organizations do not integrate PQC and crypto-agility across the pillars of their ZT roadmaps (i.e., identity, device, network, applications, and data), ZT initiatives will likely be undermined. Given the ubiquity of encryption across the ZT pillars, an organization that has knowledge gaps where they are using encryption (and inspecting and monitoring it)—and in their ability to rapidly update keys/certificates, or even switch algorithms—faces significant risk across its IT operations and business functions. For example, implementing a ZT solution to restrict access at the application layer, but failing to secure the underlying public key infrastructure (PKI) that manages identities, can further undermine security posture.

There is Quantum Uncertainty without Zero Trust

If organizations do not incorporate the ZT pillars into their PQC and crypto-migration planning, quantum readiness efforts will likely be lost in a vacuum. In particular, organizations risk misdirecting or missing PQC activities without accounting for broader system modernization initiatives. For example, it may be ineffective to procure solutions to transition device-level encryption to PQC if that hardware is planned to be decommissioned and supported workloads moved to the cloud. Similarly, it may be inefficient to prioritize cryptographic migration for an entire network infrastructure, when only a single database within that environment contains information that is particularly vulnerable to quantum threats.

The Maturity of Cryptographic Agility will determine success

Organizations should utilize a cryptographic agility maturity model across the ZT pillars to guide and assess effectiveness of combined ZT and quantum readiness efforts. It should be more manageable to identify, evaluate, and plan for cryptographic agility and migration with respect to discrete identities, devices, network infrastructure, applications, and data—especially when efforts are already underway in these areas.

Zero Trust
Quantum Readiness

The Entangled Challenges of Zero Trust and Quantum Readiness

In this context, solutions to the entangled challenges of ZT and quantum readiness should be guided by a new model for maturing cryptographic agility. It is not enough to simply aspire for crypto-agility or implementation of PQC—organizations need a framework for progress.

Building upon the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model[6] that organizations are already referencing on their ZT modernization journey, a cryptographic agility maturity model can guide efforts related to PQC and integrate crypto-agility across the ZT pillars. Such a framework provides a measured, meaningful approach that facilitates clear and actionable planning as well as cost savings and risk reduction associated with broader ZT and PQC efforts. Further, it can be used to inform:

- **Governance and standards.** Integration into existing frameworks (e.g., the CISA ZT Framework and the National Institute of Standards and Technology (NIST) Cybersecurity Framework) facilitates adoption.
- **C-Suite decision making.** Alignment to broader modernization and risk management activities accelerates innovation and impact.
- **Stakeholder engagement.** Engagement across interdependent system modernization priorities enhances momentum and efficiency.

Threats to cryptography present significant risk to the success of ZT initiatives.

If quantum risk is not accounted for as part of current ZT efforts, much of the current ZT and IT modernization efforts may be compromised.

Zero trust in ZT without Quantum Readiness

ZT is about removing legacy perimeter-based protections and applying security through a layered approach that allows organizations to continually assess their environment and adapt it to threats.

At its core, ZT provides a framework focused on the following pillars:

- Identity—Knowing who and what is accessing your data
- Device—Verifying devices are trust-worthy, healthy, and secure
- Networks—Monitoring and protecting traffic
- Applications—Understanding application workflows and restricting traffic through microsegmentation
- Data—Protecting data and controlling access to it granularly.

Each pillar has its own relationship with a single security concept: encryption. Encryption is essential to each of the pillars and touches many of an organization's security solutions across each pillar—whether PKI for authentication, encryption, and signing, as well as protection of data at rest and in transit. Indeed, in CISA's newly released ZT Maturity model,[6] encryption is emphasized in its promotion of crypto-agility within certain pillars. Crypto-agility is an approach for organizations to adapt to future cryptographic algorithms and standards without modifying or replacing surrounding infrastructure.

An organization that has gaps in knowing where they are using encryption (and inspecting and monitoring it)—and in their ability to rapidly update keys/certificates, or even switch algorithms—faces significant risk across its IT operations and business functions.

In this context, incorporating agile encryption solutions across pillars should be core to organizations' ZT strategies.

What about an organization that can't trust its cryptography at all, or that has no mechanism to migrate to new forms of secure cryptography? This is one challenge that has emerged in the face of Quantum computers.

Quantum computers will be able to break many common forms of cryptography exponentially faster than classical computers, rendering certain cryptographic algorithms used to protect data obsolete. Moreover, given the embedded nature of cryptography throughout the enterprise—including in-flight modernization efforts across ZT pillars—the time to fully migrate to PQC would potentially take decades to complete, and be highly disruptive. One report from the World Economic Forum estimates that 20 billion digital devices will need to be upgraded or replaced with PQC in the next 20 years.[7]

In short, if quantum risk is not accounted for as part of current ZT efforts, much of current ZT and IT modernization efforts may be compromised. Organizations will likely have to undo and rework substantial investments in ZT to enable crypto-agile architectures and implement PQC. However, by integrating PQC and crypto-agility across the pillars of their ZT roadmaps, organizations can be better positioned to mitigate these risks while also saving time and effort.

Quantum Uncertainty without Zero Trust

Uncertainty is essential to quantum computing's promises of technological advancement and innovation. It underlies the fundamental principles of quantum theory that will allow quantum computers to push computational boundaries, ultimately enabling solutions to problems that have been nearly impossible with classical computers. Uncertainty is likewise an essential component of quantum risk.

As quantum computing advances, the threat that adversaries use quantum computers to crack today's encryption accelerates—yet scientists are not sure when quantum computers will be sufficiently powerful, stable, and available to pose such a threat. Moreover, attackers are already harvesting data today with the aim of decrypting it at a later date when quantum computers are sufficiently mature (in so-called "Harvest-now, Decrypt-later" attacks). This increases the need to take steps to mitigate quantum risk more important today, despite the uncertainty of the availability of quantum computers tomorrow.

Facing this uncertainty, the federal government has prioritized and accelerated its leadership regarding the migration of information technology systems to PQC—encouraging federal agencies to conduct a prioritized inventory of cryptographic systems, and an assessment of funding required for systems to migrate to PQC.

To adequately build their inventories, and effectively plan for crypto-migration, organizations should both understand the sensitivity of their data over time and track how various cryptographic algorithms are used—something they have never had to do before.

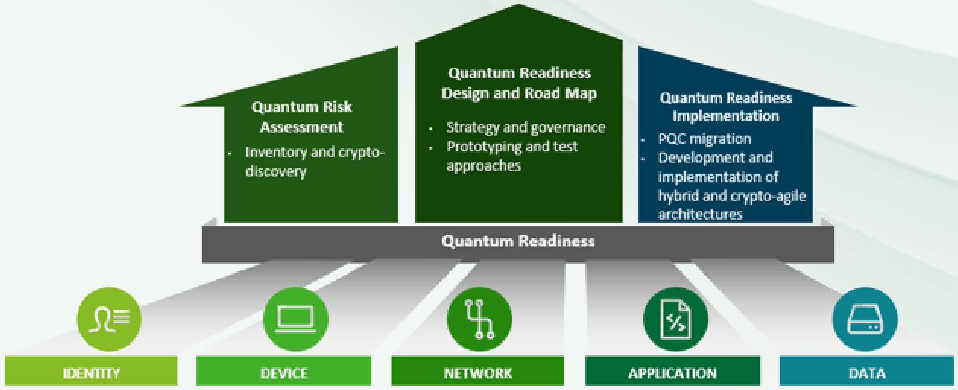
If there is one thing certain about this uncertainty, it is that there cannot be a one size fits all approach to crypto-agility and PQC migration. Unlike quantum computers, quantum readiness cannot exist in a vacuum.

Prior cryptographic transitions have taken years, and in some cases decades, in large part because of the impact of cryptography on broader information technology ecosystems. This has included systems needing to be upgraded to be able to process the new algorithms and support interoperability with external systems. For PQC in particular, system migration to new crypto-agile environments, may be more feasible and cost effective than individual migration of system components (in many cases, this may mean migration from legacy infrastructure to cloud).

Importantly, organizations do not approach cryptography from the perspective of high-level systems inventories; they do so—as we have seen through ZT—across and throughout the pillars of identity, devices, networks, applications, and data. Existing ZT efforts can provide a meaningful and actionable framework for quantum readiness. Specifically, ZT pillars can be leveraged for identifying and planning quantum readiness activities, in alignment with ZT efforts.

It is more manageable to identify, evaluate, and plan for cryptographic agility and migration with respect to discrete identities, devices, network infrastructure, applications, and data—especially when efforts are already underway in these areas.

As highlighted in the figure below, by incorporating the ZT pillars into their PQC and crypto-migration planning (from assessment through implementation), organizations can gain confidence that PQC efforts should adequately account for broader system modernization, saving cost and time, and improving security.


Quantum Risk Assessment
Inventory and crypto-discovery
Quantum Readiness Design and Road Map
Strategy and governance
Prototyping and test approaches
Quantum Readiness Implementation
PQC migration
Development and implementation of hybrid and crypto-agile architectures
Quantum Readiness
IDENTITY
DEVICE
NETWORK
APPLICATION
DATA

Maturity of Cryptographic Agility will determine success

A Quantum Trust framework for maturing cryptographic agility provides organizations an understanding of the current state of their cryptographic agility and how to prioritize improvements within ZT and quantum readiness efforts. It measures both how an organization integrates crypto-agility and how it advances quantum readiness, across the ZT pillars.

As organizations mature, they progress along the following dimensions:

- Basic—Visibility and governance related to crypto-agility is limited and ad hoc
- Traditional—Visibility and governance related to crypto-agility is formalized, but not implemented within, or incorporated across, ZT pillars
- Initial—Crypto-agility is implemented within at least one ZT pillar, but not across pillars as part of broad quantum readiness and ZT strategies
- Advanced—Crypto-agility is implemented across pillars as part of broad quantum readiness and ZT strategies. Organization has complete cryptographic awareness and has developed and centralized management solution across the environment to enforce policies and standards; however, processes are mostly manual for issuance and lifecycle activities and monitoring of risk.
- Optimal—Processes are mostly automated and provide ongoing feedback on risk as well as orchestration of cryptographic agility.

This model recognizes that—given the scope and scale of ZT and quantum readiness efforts required to fully implement crypto-agility across identities, devices, network infrastructure, applications, and data—progress will not instantly materialize. Rather, organizations can take incremental steps, that build maturity over time, so long as they maintain awareness and oversight of their cryptographic risk.

Quantum Trust is a function of how an organization matures crypto-agility and integrates Quantum Readiness across the ZT pillars.

Getting started

Review the Deloitte Quantum Trust Maturity Model.

Establish a foundation for progress by inventorying cryptographic risk across ZT pillars.

Reduce inefficiencies and promote innovation by establishing cross-pillar strategies and roadmaps for cryptographic migration.

Conduct pilots and implement proofs of concept that facilitate cryptographic agility across ZT pillars (solutions that cannot scale or be implemented across pillars will have limited impact and may even undermine long-term success).

Endnote

1. Executive Order (EO) 14028, Improving the Nation’s Cybersecurity (2021); OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
2. National Security Memorandum (NSM)-10, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (May 01, 2022); OMB Memorandum M-23-02, Migrating to Post-Quantum Cryptography (November 18, 2022)
3. Department of Defense Zero Trust Reference Architecture (July 2022)
4. OMB M-23-02, ibid.
5. NSM-10, ibid.
6. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA), Zero Trust Maturity Model (April 2023)
7. Catherine P. Foley et al., “Is your cybersecurity ready to take the quantum leap?”, World Economic Forum, May 7, 2021.

Contacts

To learn more, please contact:

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

Robert Hankinson
Specialist Leader
Cyber & Strategic Risk
Deloitte & Touche LLP
rohankinson@deloitte.com

Benjamin Shapiro
Senior Manager
Cyber & Strategic Risk
Deloitte & Touche LLP
beshapiro@deloitte.com

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document 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 document.

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.