Quantum-Safe Readiness Program for Enterprise

Learn how to manage quantum risk by understanding what's at stake, gaining hands-on experience with hybrid certificates and exploring quantum-safe cryptography

Quantum computers will deliver tremendous benefits, but they will also be able to break the cryptography underlying public key infrastructure (PKI).

An enterprise risk-management imperative

Because of the real risks imposed by quantum computing—and despite the uncertain arrival time—many CISOs and CIOs have tasked their IS/IT teams with investigating the threat and recommending a course of action.

In other organizations, IS/IT teams have taken it upon themselves to deeply explore the subject so that they can convince executives and boards to consider quantum risk within the existing security governance.

Separating fact from fiction

But learning about quantum computing and cryptography isn't easy—and it can be even harder to take that information and determine what actions should be taken today versus what can wait.

A Program Unlike Any Other

To help forward-thinking enterprises take steps to manage quantum risk—today—ISARA has developed a **Quantum-Safe Readiness Program** which equips your IS, IT and cryptography teams with actionable know-how and practical hands-on experience through:

- A half-day workshop, **The Path to Quantum-Safe**, which prepares your organization with quantum security domain knowledge, demonstrations and training
- A specially prepared leave-behind VM with embedded **ISARA Catalyst™ Agile Certificate Technology**, which allows your security and information teams to simulate and demonstrate crypto-migration using hybrid certificates
- An Enterprise Evaluation license and hands-on training with the **ISARA Radiate™ Quantum-Safe Toolkit**, so your team can experiment, develop and gain real experience with leading quantum-safe algorithms
- 12-month access to **ISARA's renowned quantum security experts**, to help you on your journey to a quantum-safe future

The business world is taking notice

Governments, defense contractors and a handful of enterprises take the quantum threat very seriously—but now the rest of business world is taking notice, thanks to leading analysts, consulting firms and government agencies.

Gartner

"If a sufficiently powerful quantum computer becomes available within 10 or so years, any data that has been published or intercepted is subject to cryptanalysis by a future quantum computer."

—Gartner, in The CIO's Guide to Quantum Computing

Deloitte.

"Enterprises and governments should start protecting against the threat of powerful quantum computers today, not when it happens, since by then it will be too late."

—Deloitte, in Technology, Media, and Telecommunications Predictions 2019

NATIONAL ACADEMY OF SCIENCES

"Prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

—National Academy of Sciences, in Quantum Computing Progress and Prospects

Act Today to Protect Tomorrow

This comprehensive program includes everything you need to take meaningful steps toward managing quantum risk—and it also comes with 12-month access to our renowned quantum security experts for ongoing Q&A, solution feedback and domain discussions to assist with your journey to a quantum-safe future.

Workshop: The Path to Quantum-Safe

This four-hour virtual workshop equips you with the information and training required to understand the security risks quantum computing introduces and—crucially—how you can prepare, by providing:

- An overview of quantum threats and quantum-safe cryptography
- An examination of the impacts of quantum-safe cryptography on information security systems
- An exploration of cryptographic risk, the importance of cryptographic agility, migration challenges and the migration path from the present day to a quantum-safe future
- Training on how to use the ISARA Catalyst™ Crypto-Agile Hybrid Certificate Virtual Machine

Crypto-Agile Hybrid Certificate Virtual Machine

This specially prepared VM (a Linux system image for VirtualBox) allows your security and information professionals to explore, simulate and demonstrate crypto-migration using a TLS 1.2 test environment and Certification Authority (CA) which implements hybrid certificates using ISARA Catalyst™.

ISARA Catalyst™ Agile Digital Certificate Technology

ISARA Catalyst™ enhances X.509 digital certificates by adding support for multiple cryptographic algorithms into a single certificate. This technology allows enterprises to seamlessly integrate quantum-safe security into their certificate and PKI management products today—while maintaining backward compatibility with legacy components and adhering to global standards.

Explore Cryptographic Migration

The TLS 1.2 test environment enables your team to explore two cryptographic migration scenarios:

- From RSA-ECDHE to ECDSA-ECDHE
- From RSA-ECDHE to Dilithium-Kyber*

**Dilithium and Kyber are quantum-safe cryptographic algorithms which are based on a lattice problem referred to as Learning with Errors (LWE)—they are leading candidates in the NIST's post-quantum cryptography standardization process*

Toolkit & Training: Quantum-Safe Cryptography

This component allows you to experiment, develop and gain hands-on experience with quantum-safe algorithms by providing:

- An evaluation version of the ISARA Radiate™ Quantum-Safe Toolkit, available for a number of platforms (including Linux, macOS, Windows, iOS and Android)
- A virtual training session which can be scheduled within six months of executing this readiness program

ISARA Radiate™ Quantum-Safe Toolkit

The ISARA Radiate™ is a high-performance, lightweight, standards-based quantum-safe SDK to allow developers to test and integrate—into commercial products—post-quantum cryptography.

Prepare for tomorrow with practical actions today.

Contact us at **quantumsafe@isara.com** to learn more about how the Quantum-Safe Readiness Program can help your enterprise understand and manage quantum risk.

ISARA

isara.com | quantumsafe@isara.com | +1 877 319 8576
560 Westmount Road North, Waterloo, Ontario, Canada N2L 0A9

Version 1.0 | 2020-04-20