

IBM Quantum Safe Roadmap

Legend: ■ First generation available | □ On target | □ Planned

Regulatory milestones	2022	2023	2024	2025	2026+
IBM services	█ NIST selects algorithms for standardization	█ Federal agencies plan for adoption of PQ4 █ NIST publishes PQ4 standards	█ NSA 2.0: preference to PQ4-compliant vendors	█ Vendors complete transition to PQ4	
IBM Quantum Safe technology	Empowering clients to discover, observe, and transform their cryptography Helping clients throughout their journey to quantum safe █ Scale beyond crypto-agility □ IBM multi-cloud services, cybersecurity transformation services █ Modernize applications and data security □ IBM application modernization, data modernization services █ Establish foundation □ IBM Quantum Safe technical services				
IBM infrastructure	Accelerating the client journey to quantum safe IBM Quantum Safe Roadmap █ IBM Quantum Safe Assistant □ IBM Quantum Safe Assistant □ Compliance checks □ Quantum-resistant algorithms █ IBM Quantum Safe Explorer □ Inventory (dependencies) □ Inventory (data information) IBM Cloud, IBM Hyper Protect Crypto Services, IBM Cloud Security, Red Hat Security Services, IBM Security				
	Algorithms & protocols █ New encryption – CRYSTALS-Dilithium █ Digital signatures – CRYSTALS-Dilithium, FALCON				
	Interoperability standards █ COSE				
	Libraries □ OpenSSL				

Recognizing this risk, IBM has leveraged its extensive expertise across cryptography, quantum computing, and critical infrastructure to develop IBM Quantum Safe technology.

This set of capabilities is designed to help clients prepare for the post-quantum era via:

- **IBM Quantum Safe Explorer** to enable organizations to scan source and object code to locate cryptographic assets, dependencies, vulnerabilities and to build a Cryptography Bill of Materials ([CBOM](#)). This allows teams to view and aggregate potential risks into one central location.
- **IBM Quantum Safe Advisor** allows the creation of a dynamic or operational view of cryptographic inventory to guide remediation and analyzes cryptographic posture and compliance to prioritize risks.
- **IBM Quantum Safe Remediator** enables organizations to deploy and test best practice-based quantum-safe remediation patterns to understand the potential impacts on systems and assets as they prepare to deploy quantum-safe solutions.

IBM is also unveiling its IBM Quantum Safe Roadmap to help clients understand and support them through this security transition. This is IBM's first blueprint that charts the technology milestones towards increasingly advanced quantum-safe technology, which is engineered to help organizations address anticipated cryptographic standards and requirements through crypto-agility and protect systems against emerging vulnerabilities.

This journey is comprised of three key actions:

- **Discover:** Identify cryptography usage, analyze dependencies, and generate a CBOM.
- **Observe:** Analyze cryptography posture of vulnerabilities and prioritize remediation based on risks.
- **Transform:** Remediate and mitigate with crypto-agility and built-in automation.

"As a leader in quantum computing, IBM recognizes the importance of comprehensively addressing the critical needs of our clients as they also consider transforming their cryptography for the quantum era," said Ray Harishankar, IBM Fellow and lead for IBM Quantum Safe technology. "Our new suite of quantum-safe technologies and milestones laid out on our roadmap is designed for the continuous evolution of post-quantum security in tandem with useful quantum computing, including solutions to help industries navigate this shift effectively and easily."

Last year, the United States government released new requirements and guidelines calling upon federal agencies to start the quantum-safe transition. The National Institute of Standards and Technology (NIST) selected four quantum-resistant algorithms for standardization — three of which were [developed by IBM](#), alongside academic and industry collaborators.

Then, the National Security Agency (NSA) announced new requirements for national security systems to transition to quantum-safe algorithms by 2025, and the White House released requirements for federal agencies to submit a cryptographic inventory of systems that could be vulnerable to cryptographically relevant quantum computers.

"As the era of quantum computing quickly approaches reality, it is imperative that quantum-safe technologies are also deployed to protect today's classical systems and data," said Patrick Moorhead, CEO and founder of Moor Insights & Strategy. "What the world needs to secure data for the quantum age is expertise in world-class quantum technology and advanced cryptography, alongside decades of product development experience for critical infrastructure. These pillars are where I believe IBM excels, and now with a quantum-safe roadmap to

lead the industry and new technologies to simplify migration, I look forward to seeing the advancement of quantum-safe journeys globally."

The IBM Quantum Safe Roadmap and technology will expose organizations to their existing cryptographic landscape so they can begin to address changes that may be necessary to thrive in the post-quantum era.

For more information about IBM Quantum Safe technology or to request a demo, visit:

<https://www.ibm.com/quantum/quantum-safe>.

Media Contacts:

Chris Nay

cnay@us.ibm.com

Willa Hahn

willa.hahn@ibm.com

SOURCE IBM

Additional assets available online:



<https://newsroom.ibm.com/2023-05-10-IBM-Unveils-End-to-End-Quantum-Safe-Technology-to-Safeguard-Governments-and-Businesses-Most-Valuable-Data>