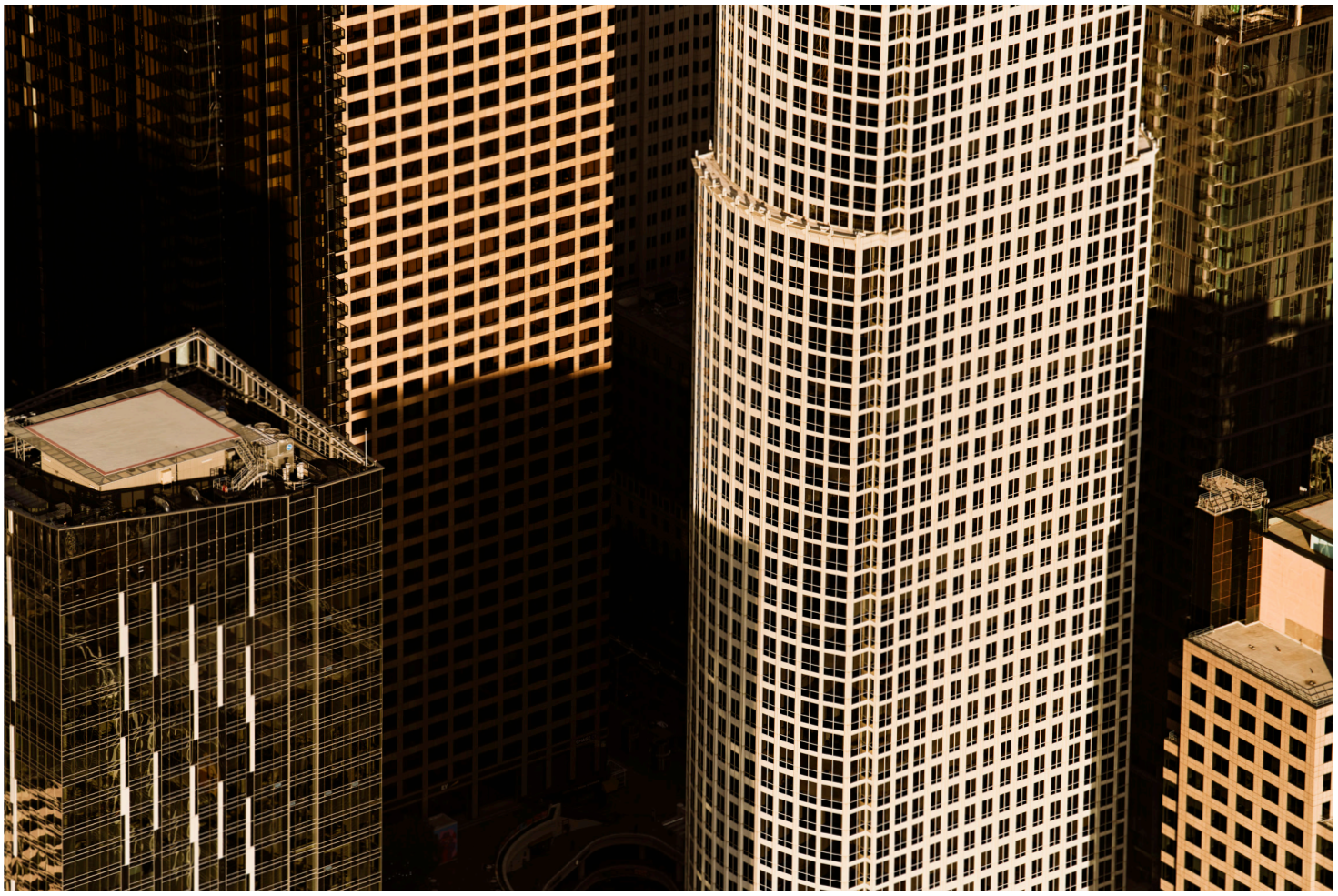
IBM Quantum Safe
→ Financial services



IBM Quantum Safe for financial services

Secure your financial services data and systems with quantum-safe cryptographic technology

FSS security in the quantum era

Financial services (FSS) organizations are responsible for large volumes of confidential customer data, as well as highly sensitive proprietary data and intellectual property. A data breach at a financial institution can result in substantial damages, reputational loss, and legal liability. Considering these risks, FSS organizations must proactively address evolving cybersecurity threats, particularly those related to quantum.

With its potential applications in portfolio optimization, fraud detection, and risk management, quantum computing presents an exciting opportunity for the FSS industry. At the same time, it creates a challenge: quantum computers will one day become powerful enough to break many of the cryptographic algorithms used across FSS systems to protect data and communications. To ensure the confidentiality, integrity, and authentication of financial transactions in the quantum future, FSS organizations must transition their systems to quantum-safe cryptography.

Understanding current and future risks

There is particular urgency for FSS institutions to migrate to quantum-safe cryptography. Not only do many FSS companies have technological debt from legacy systems, but they also have complex IT landscapes comprising internally developed and third-party applications, cloud and SaaS capabilities, and more, whose security depends on quantum-vulnerable cryptography. It will take a quantum-literate workforce for enterprises to address these risks. However, as a white paper by UK Finance notes, the FSS sector contends with a skills gap in post-quantum cryptographic algorithms and their real-world applications.[1]

Recognizing the need for FSS enterprises to start their quantum-safe transition, standards bodies have begun to issue new guidance for cryptography compliance in the post-quantum era. For example, the National Institute of Standards and Technology (NIST) has selected four quantum-resistant encryption algorithms for standardization, three of which were developed by IBM researchers. In line with this, financial standards organizations such as the Accredited Standards Committee (ANSI) X9 are developing best practices for the implementation of these standards, which are expected to be published in 2024.

The complexity of these new standards, coupled with an evolving regulatory landscape and rigorous compliance requirements, means that FSS organizations need to plan for, and incrementally execute, their quantum-safe transition. According to Project Leap,[2] a joint effort by the BIS Innovation Hub Eurosystem Centre, the Bank of France, and Deutsche Bundesbank to build quantum cyber resilience in the FSS sector, this journey involves addressing three main risks to the global financial system:

“Harvest now, decrypt later” attacks – stealing confidential data now in order to decrypt it with a future cryptographically relevant quantum computer.

Fraudulent authentication – falsifying code signing certificates and digital signatures to tamper with software updates and weaken online account security.

Digital signature forgery – manipulating mobile banking transactions and payment processes by forging digital signatures.

Benefits of forward planning

While there is no exact date for when quantum computers will challenge existing cryptography, quantum technology is evolving at a rapid pace. Governments and regulatory bodies around the world are already establishing guidelines for the transition to quantum-safe cryptography. The US Government has issued National Security Memoranda (NSM-8, NSM-10), Executive Orders (EO 14028), and legislation (HR 7535) that outline the steps for migrating systems to post-quantum cryptography.

Recognizing the complexity of this migration for FSS firms, the World Economic Forum published a joint white paper with the Financial Conduct Authority outlining principles for industry and regulators to collectively build a quantum-secure global economy.[3] To this end, IBM has been leading FSS consortia efforts to engage stakeholders and accelerate the adoption of quantum-safe cryptography. For example, as a founding member of the EPAA Post-Quantum Work Group, IBM is collaborating with the APAC/global payments service community to drive awareness of, promote regulatory alignment on, and develop use cases for quantum-safe cryptography in the FSS ecosystem.

FSS organizations that form a quantum-safe strategy now can stay ahead of potential privacy breaches, operational disruption, and reputational damage. For FSS firms, beginning the quantum-safe transition now offers several possible advantages, such as:

Optimize investment

- Opportunity to leverage technology refresh cycle activities and investments; improved budgeting and purchasing decisions
- Ability to establish a data strategy that includes protection and analytics tools
- Phasing to amortize costs over a longer period of time

Mitigate risk

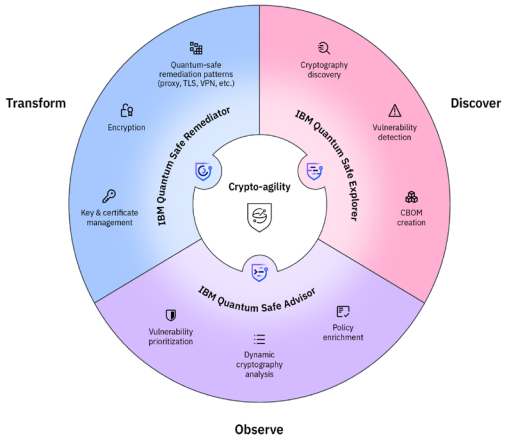
- Ability to develop an agile remediation strategy that maximizes efficiency and minimizes disruption
- Increased opportunities for phasing of testing and implementation cycles
- Greater ability to protect customer/shareholder data and transactions and to secure the financial markets

Target incremental revenues

- Competitive advantage from quantum-safe practices
- Decreased volatility of cryptocurrencies

Building a robust quantum risk posture with IBM Quantum Safe technology

IBM is ready to help enterprises plan and execute an end-to-end transition to post-quantum cryptography with IBM Quantum Safe. Discover, observe, and transform your cryptography for the quantum era with IBM Quantum Safe technology and services.



IBM has already begun integrating quantum-safe cryptography into technologies such as IBM z16® and IBM Cloud® and has developed a tried and tested transition approach. IBM Quantum Safe equips financial organizations to accomplish the steps required for a successful quantum-safe migration, including:

Identify applications and systems that depend on at-risk cryptography.

Perform a cryptography risk assessment to prioritize vulnerable data and systems.

Upskill teams in the capabilities needed to support the quantum-safe transition.

Collaborate with regulators and vendors to advance quantum-safe mandates.

Develop cross-industry governance for the transition to quantum-safe cryptography.

Learn more about IBM Quantum Safe and start your journey to post-quantum resilience today: https://ibm.biz/BdM8DD

1. Minimising the risks: Quantum technology and financial services, UK Finance, November 2023.
2. Quantum-proofing the financial system, Project Leap, June 2023.
3. Quantum security for the financial sector: Informing global regulatory approaches, World Economic Forum, January 2024.