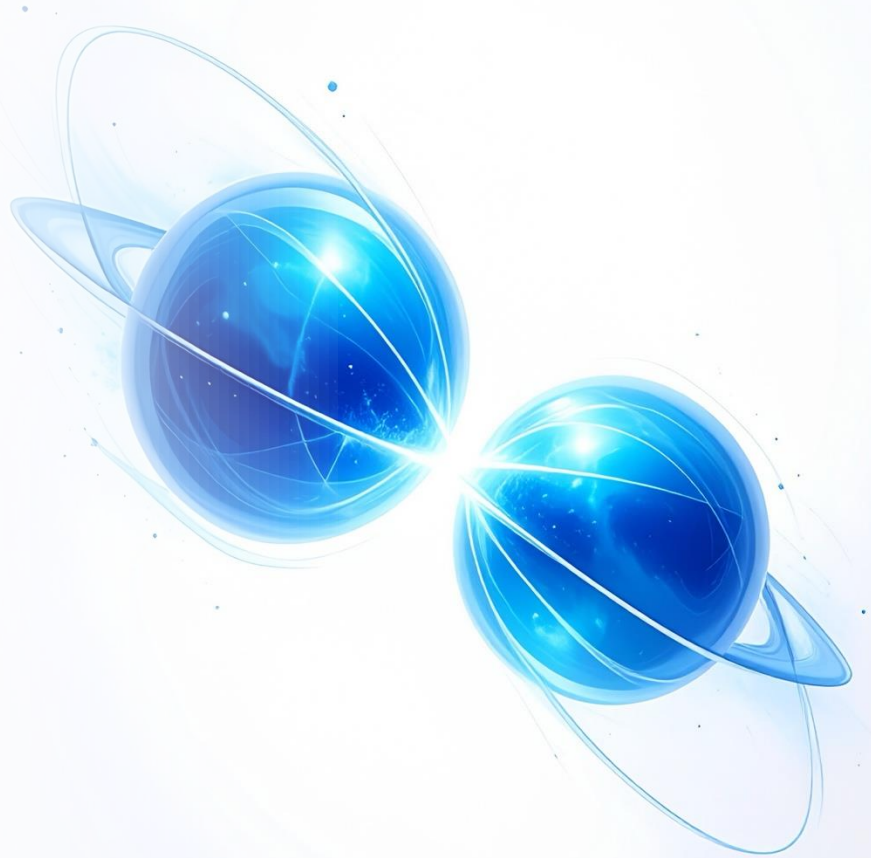
KPMG: FS & Quantum Computing



October 2025

With You Today:

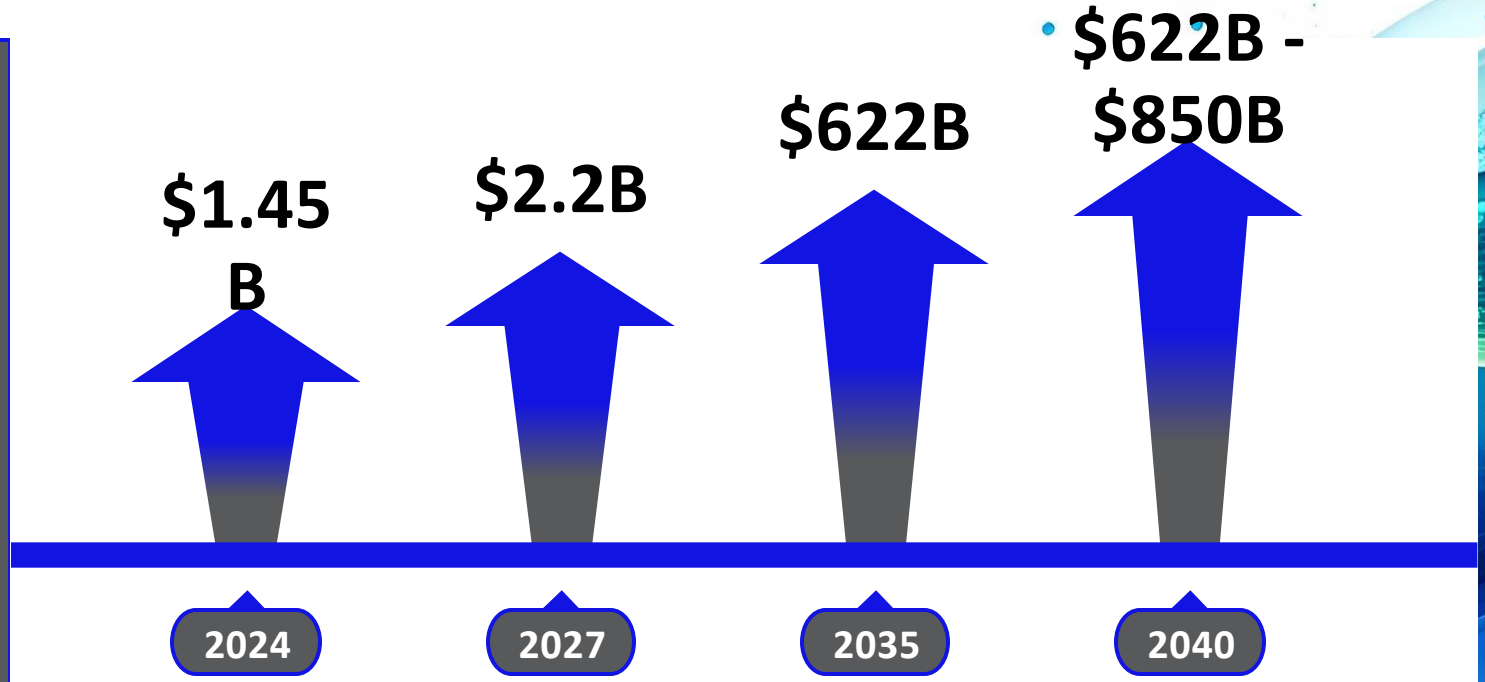
Dr. Aaron Kemp
US Quantum Lead
Enterprise Innovation

Quantum Opportunities

Quantum is Growing

Quantum computing is set to revolutionize financial services over the next 15 years by enabling faster and more accurate solutions for complex tasks such as Enhanced Security, portfolio optimization, trading, and data analysis potentially generating up to $622 billion in value by 2035.

However, this transformative potential also presents challenges, including the need for significant investment in quantum-ready infrastructure and addressing cybersecurity risks posed by the ability of quantum computers to break traditional encryption methods.



North America:
$1.1B+ investments in quantum startups (e.g., quantum sensor R&D

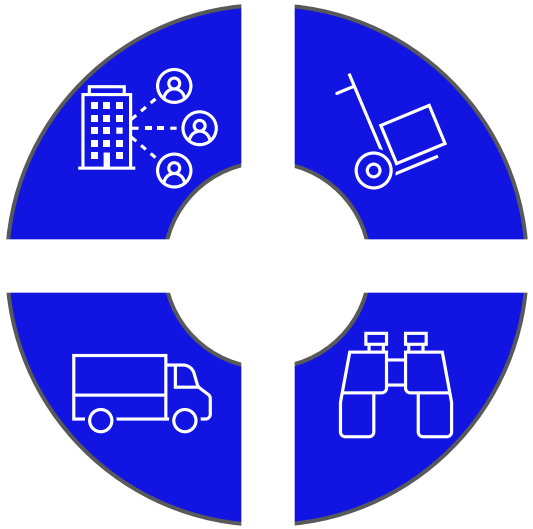
Asia-Pacific:
China $500M+ government funding for satellite QKD networks

Europe:
Germany mobile quantum computer initiative, EU Quantum Flagship

Use Cases in Practice

Quantum Approximate Optimization Algorithms (QAOA) and Quantum Monte Carlo methods are being explored for complex problems. These algorithms can solve optimization problems more efficiently than classical methods.

Fraud Detection: Quantum algorithms can identify complex fraudulent patterns across massive transaction networks in real-time by analyzing multiple variables and correlations that would be computationally prohibitive for classical systems.



Portfolio Optimization: Quantum computing can evaluate exponentially more asset combinations and market scenarios simultaneously, enabling optimal portfolio allocation across thousands of assets with complex constraints.

Risk Analysis and Monte Carlo Simulations: Quantum systems can accelerate risk modeling by running millions of market scenarios in parallel, dramatically reducing the time needed for stress testing and value-at-risk calculations.

Derivatives Pricing: Quantum algorithms can more accurately price complex derivatives with multiple underlying variables and path dependencies, particularly exotic options that require intensive computational modeling.

Quantum Risk

Why Is PQC Important?

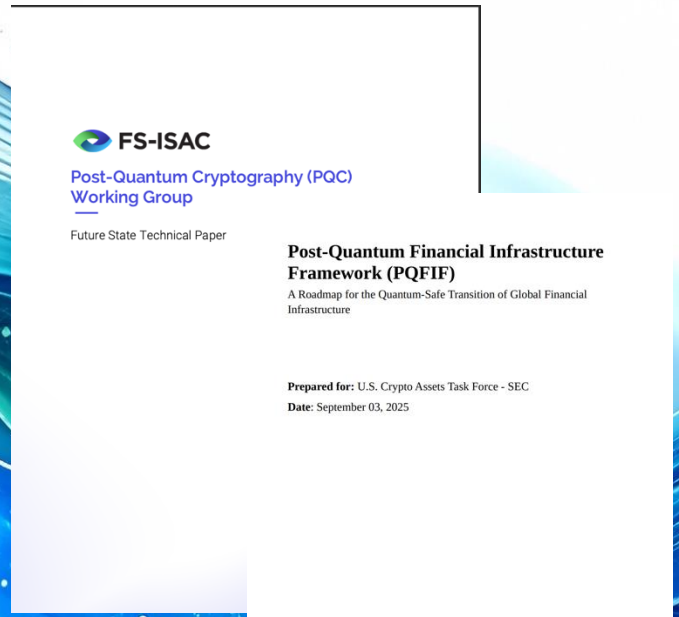
NIST's release of the first PQC standards allows organizations to begin planning for their migrations. During the 2025 OCC examination period, the first questions began being asked about quantum readiness.

Governance

While the timeline for quantum computers with enough qubits and fidelity to crack current encryption protocols is years away, the time needed for organizations to migrate is also going to take years.

- Is management actively monitoring developments in quantum computing, quantum-resistant encryption algorithms and related technologies, and external sources of guidance and standards on PQC such as the National Institute of standards and Technologies PQC Project? If yes, please describe current monitoring processes.
- Has management evaluated PQC risks through the institution's risk framework processes? If yes, how has management assigned risk ownership and aligned with technology strategies to mitigate the risks?
- Has management inventoried the cryptographic technologies (such as encryption algorithms, protocols, and hardware) used (e.g., Production, Non-production, Sandbox environments)? Please provide an overview of management's approach to performing this inventory
- Has management identified the components of those cryptographic technologies that may be quantum-vulnerable, and which may need to upgraded or replaced as part of a migration to PQC? If yes, is the organization managing, or establishing plans to management, through existing enterprise processes (e.g., change management, lifecycle/end-of-life management)?
- With respect to data assets replated to the services provided by a third-party to your financial institution, has management identified those data assets that:
  - Might be vulnerable to decryption by a quantum computer,
  - Bear the highest probability of being targeted in a quantum-based attack, or
  - Must be secured for an extended period.

FS Governance & Guidance for PQC + KPMG Q-PREP



1. **Preparation & Scope:** Define project objectives and align with business goals to establish a clear foundation for the PQC transition
2. **Cryptographic Asset Inventory:** Catalog all cryptographic assets, including algorithms, keys, and certificates, to identify quantum-vulnerable systems and prioritize PQC transition efforts
3. **Risk & Data Governance:** Establish policies and frameworks to manage cryptographic data lifecycle, ensuring compliance, security, and alignment with quantum-resistant standards
4. **PQC Solutions Exploration:** Evaluate and test quantum-resistant algorithms and protocols to identify scalable, compatible solutions for organizational needs
5. **Transition Plan Development:** Create a strategic plan outlining timelines, resources, and milestones for migrating to PQC solutions with minimal operational disruption
6. **Implementation & Remediation:** Deploy quantum-resistant cryptography across systems, validate effectiveness, and address vulnerabilities through targeted remediation actions
7. **Continuous Monitoring:** Maintain long-term resilience by monitoring emerging quantum threats, updating algorithms, and adapting to evolving standards

Questions?

Thank you

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

- The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.