KPMG

KPMG Perspectives Quantum

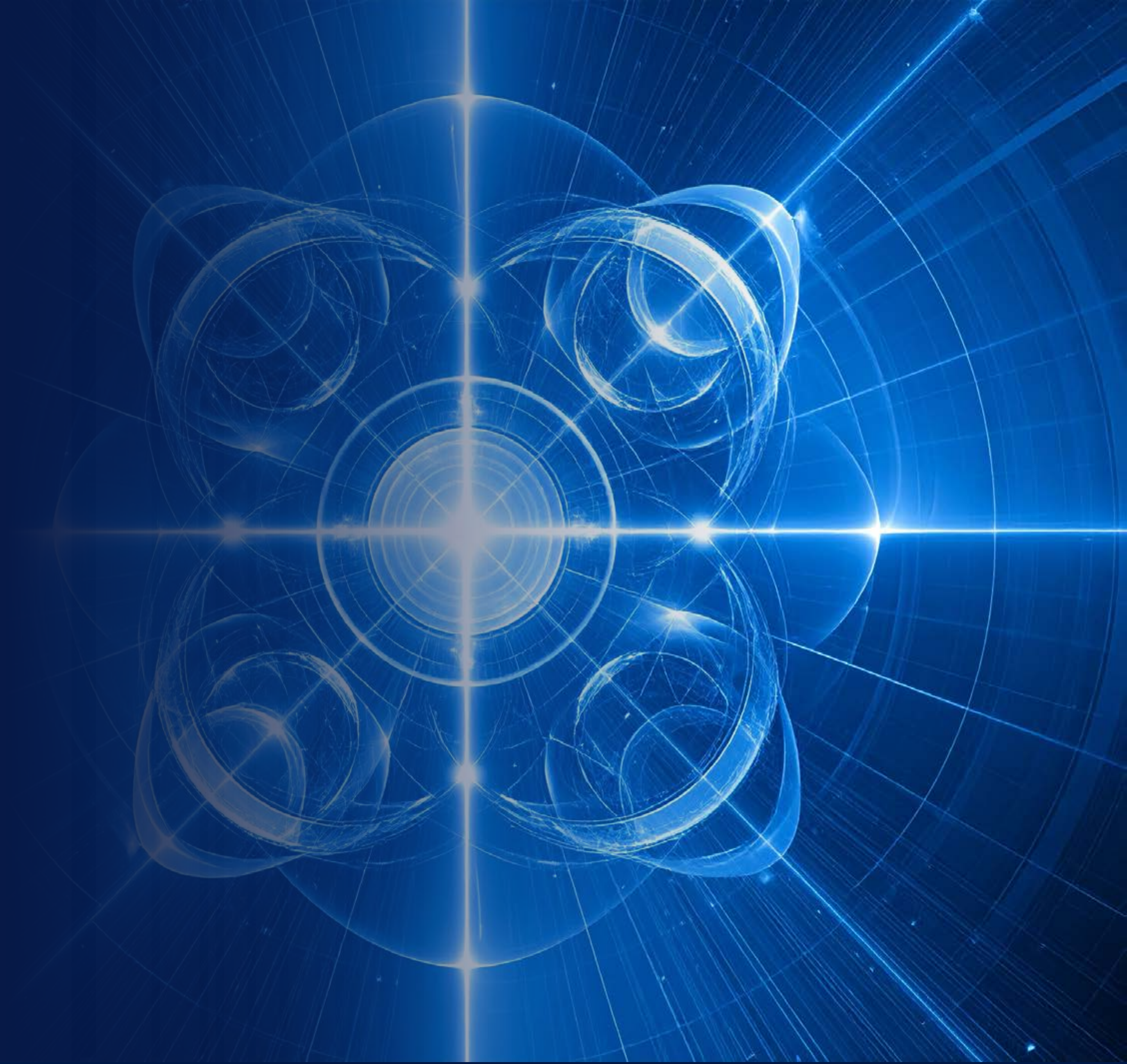
A Brief for BoardProspects

May 2025

With you today

Dr. Aaron Kemp

US Quantum Lead – Enterprise Innovation, Emerging Technologies



Introduction

Quantum computing is poised to revolutionize the financial services and insurance industry by offering unprecedented capabilities in data analysis, risk management, and optimization. This emerging technology has the potential to solve complex problems more efficiently and accurately than classical computers.

KPMG recognizes the transformative potential of quantum computing in the financial services and insurance space. As a leader in audit, tax, and advisory services, KPMG is actively exploring the applications of quantum technology to drive business value for clients. Through collaborations with companies like IBM, PSIQuantum, Q-CTRL, QuERA and the Chicago Quantum Exchange, KPMG is developing innovative quantum solutions to address complex challenges, such as fraud detection, portfolio optimization, and improving data analytics. Quantum can significantly improve financial forecasting, trading optimization, and risk profiling by processing vast datasets quickly and accurately.

The future of quantum comes with risk. Classical encryption methods are insecure against future quantum computers necessitating the adoption of quantum-resistant cryptography to secure financial transactions. As the telecommunications sector continues to evolve, embracing quantum computing will be crucial for maintaining a competitive edge and ensuring long-term resilience against emerging technological threats.

Agenda

Introductions and Objectives

Pragmatic Perspectives

Why Now?

What we're seeing and why it matters

- Cryptographic Change
- Vendor Migration

Q&A and Wrap Up

Why Quantum Now?

Quantum Imperative in Industry

- $622B market potential by 2035 in via quantum optimization, risk modeling, and AI acceleration.
- Critical risk: Current encryption (RSA, ECC) is quantum-vulnerable; attackers harvest data now for future decryption.

Tech Refresh = Quantum Readiness

- Seamless integration: Embed post-quantum cryptography (PQC) standards (NIST-approved) into ongoing infrastructure upgrades.
- Future-proofing: Hybrid systems (quantum + classical) enable incremental adoption while maintaining legacy operations.

Competitive Differentiation

- Portfolio optimization: Quantum Monte Carlo methods reduce risk calc time from hours to seconds (JPMorgan case). Example: 75% accuracy in ATM cashflow optimization (Huaxia/SpinQ collab).
- AI/ML supercharge: Quantum-enhanced fraud detection improves accuracy by 30-50% vs classical models.

Things to Consider

1 Prioritize PQC migration for core systems (NIST 2035 deadline)

2 Pilot quantum optimization through Portfolio management (QAOA algorithms) and Liquidity forecasting (quantum neural networks)

3 Build talent ecosystem: organizations already have quantum teams; partnering with IBM / PsiQuantum / QuERA and others to accelerate R&D

4 Timeline Impact

View of Quantum

What is Quantum Computing

Quantum computing has the potential to revolutionize fields such as cryptography, material science, and complex system simulation by solving problems that are currently intractable for classical computers.

Quantum Computing

Leverages the principles of quantum mechanics to perform complex calculations more efficiently than classical computing.

Basics

Uses qubits for complex data processing; can represent multiple states simultaneously

Principles

Leverages superposition and entanglement for enhanced processing and secure communication

Speedup

Offers faster problem-solving for specific tasks via unique algorithms

Status

In the age of "Quantum Utility" where systems provide practical value and advantages in solving real-world problems

Challenges

Faces operational and accuracy issues; still in experimental phase

Quantum Power

Random Circuit Sampling (RCS)

Google AI Willow Processor

- 105 Qubits
- Exponential Error Reduction
- Improved Machine Learning
- Improved Calibration Protocols

← 5 Minute Run Time

10,000,000,000,000,
000,000,000,000
Years Run Time →

10 Septillion Years!

Opportunity & Risk

El Capitan

- Location: Lawrence Livermore National Laboratory — California, U.S.
- Performance: 1,742 petaFLOPS (1.742 exaFLOPS)
- Components: AMD 4th-Gen EPYC 24-core CPUs in AMD Instinct MI300A APUs
- First online: November 2024

So What is a Qubit?

= 0 or 1

Classical Bit

= 0 and 1

Quantum Bit or Qubit

Superposition:

- A light switch that can be on or off
- In quantum, the switch can be both *on* and *off* at the same time
- This is a superposition: being in two states at once

Entanglement:

- Two qubits affecting each other
- If you observe one qubit as a 1, the other qubit *instantly* changes to a 1 too, even if it's far away
- This is entanglement: two qubits being connected so that what happens to one happens to the other, no matter how far apart they are

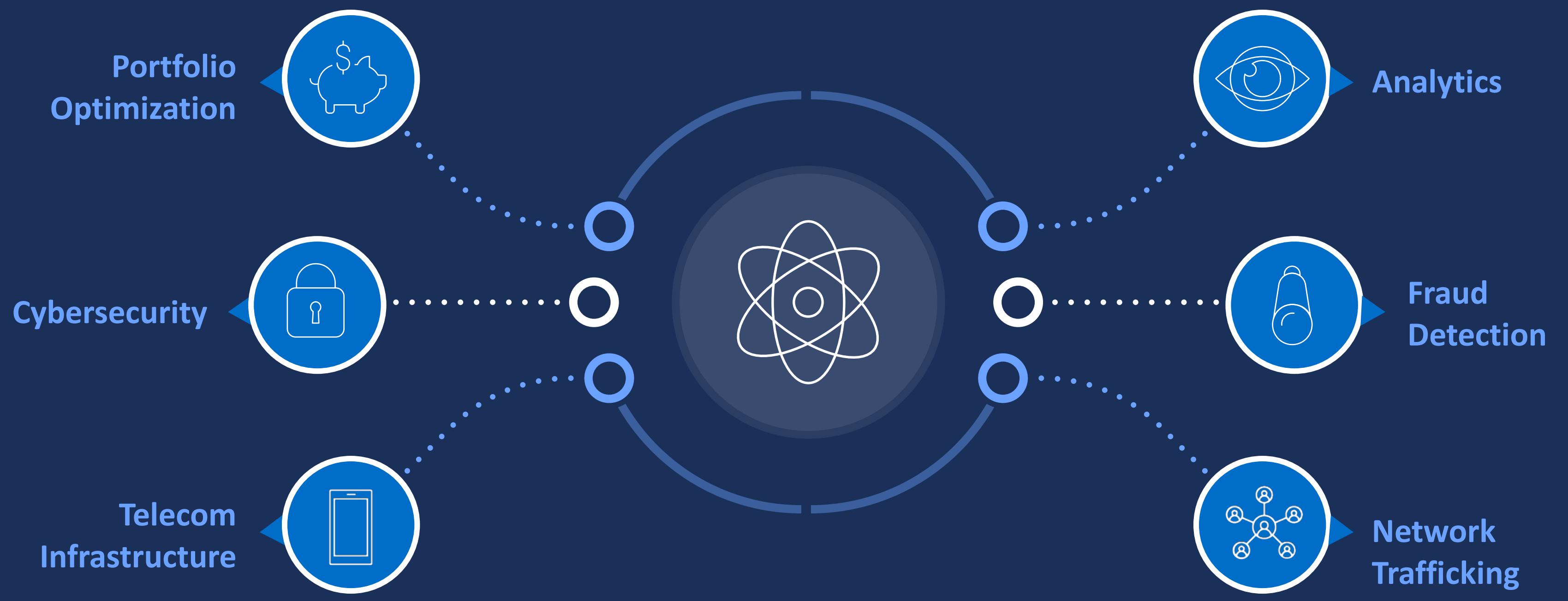
Quantum Opportunity

Why is Quantum Important?

Quantum computing represents a revolutionary leap forward, offering the potential to solve complex problems that are currently beyond the reach of classical computers.

Key Takeaways

Quantum Computing will be a disrupter across a wide-range of applications and fields in the coming years.



Collateral Optimization

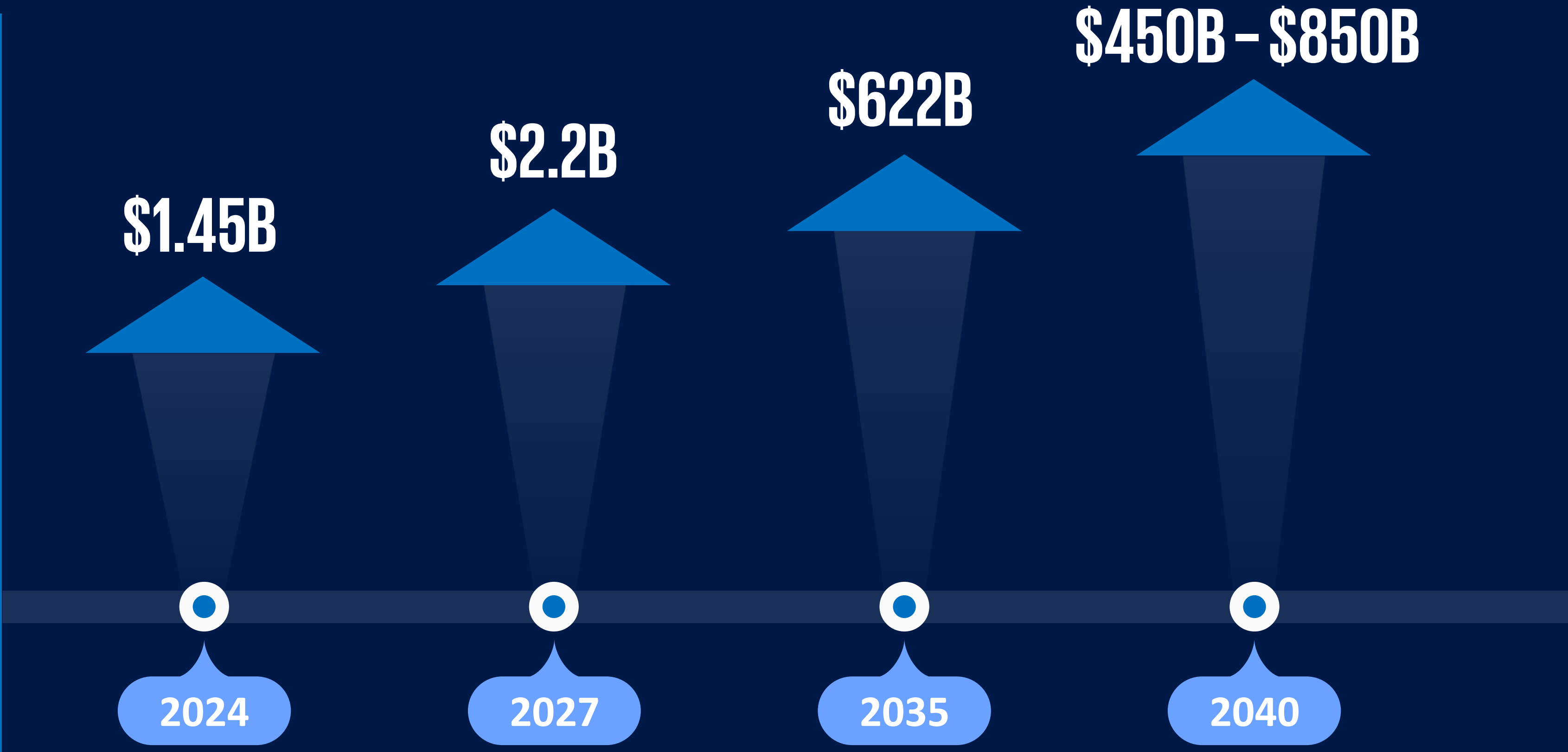
Collateral optimization efficiently allocates and manages collateral assets to meet regulatory requirements while minimizing costs. It involves mathematical and algorithmic strategies to balance risks, liquidity, and profitability.

- HSBC partners with Terra Quantum to apply hybrid quantum technology for collateral optimization.
- Using TetraOpt solver to reformulate problems as Quadratic Unconstrained Integer Optimization (QUIO).
- Solution handles higher dimensionality and non-linear constraints beyond traditional methods.
- Partnership demonstrates quantum computing's practical potential for telecommunications services optimization.

Quantum is Growing

Quantum computing is set to revolutionize the telecommunications sector over the next 15 years by enabling faster and more accurate solutions for complex tasks such as Enhanced Security, Optimized Network Traffic, Error Correction in Transmissions and Infrastructure Optimization, 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

Optimization in Telecommunications

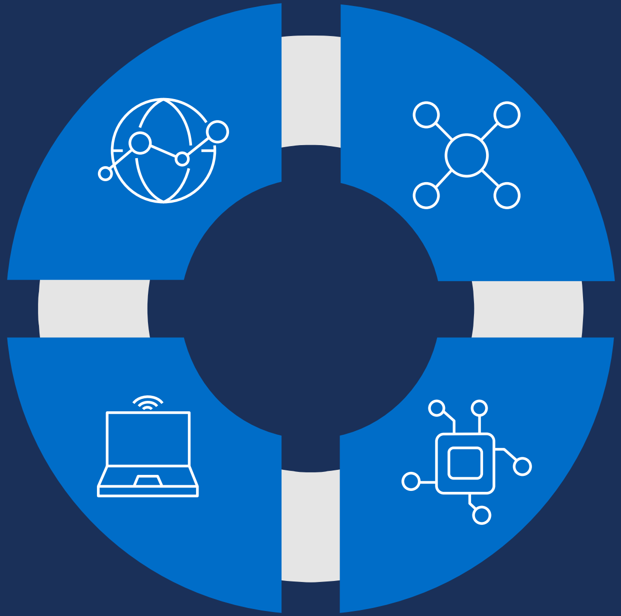
Quantum Approximate Optimization Algorithm (QAOA) and Quantum Monte Carlo methods are being explored for complex financial problems. These algorithms can solve optimization problems more efficiently than classical methods

AT&T

Partnering with academia for quantum encryption to enhance network security.

General Use Cases

Fraud detection, dynamic portfolio rebalancing, and accelerated risk simulations using quantum algorithms.



BT (British Telecommunications)

Testing quantum key distribution for secure telecom networks.

Vodafone

Exploring quantum techniques for network optimization and enhanced encryption.

Quantum Engagements

PQC Readiness Sprints

- Cryptographic inventory audits: Map RSA/ECC dependencies in legacy systems.
- Hybrid algorithm testing: Simultaneously deploy NIST-approved PQC (ML-KEM) + lattice-based alternatives.
- Workforce upskilling: Quantum risk workshops for CISOs, DevSecOps PQC implementation labs.

Migration Assistance

- HSM upgrades: FIPS 140-3 compliant modules for quantum-safe key generation.
- TLS/SSH transitions: IETF-compliant hybrid handshakes (e.g., PQ/OAEP combos).
- Code signing modernization: PQC code-signing certificates for IoT firmware.

Optimization Projects

Hybrid quantum-classical systems:

- Financial portfolio optimization (35% faster Monte Carlo simulations).
- Pharma molecular modeling (quantum-enhanced docking studies).
- Supply chain crypto-agility: Third-party vendor PQC compliance audits

Quantum Case Studies

KPMG has already assisted in aiding organizations using quantum annealing to optimize problems resulting in tangible gains.

Key Takeaways

Quantum computing is actionable now. Organizations need to begin understanding the problems which make good candidates for quantum optimizations

UK Service

Reduced annual technician milage by 52%. Optimization time reduced from 2 hours to 2 minutes

EU Telco

Utilized quantum computing to check optimize cell phone tower locations for optimal connectivity and servicing

Migration

PQC Readiness -Large International Bank, Large US Bank, Large US Auto Manufacturer

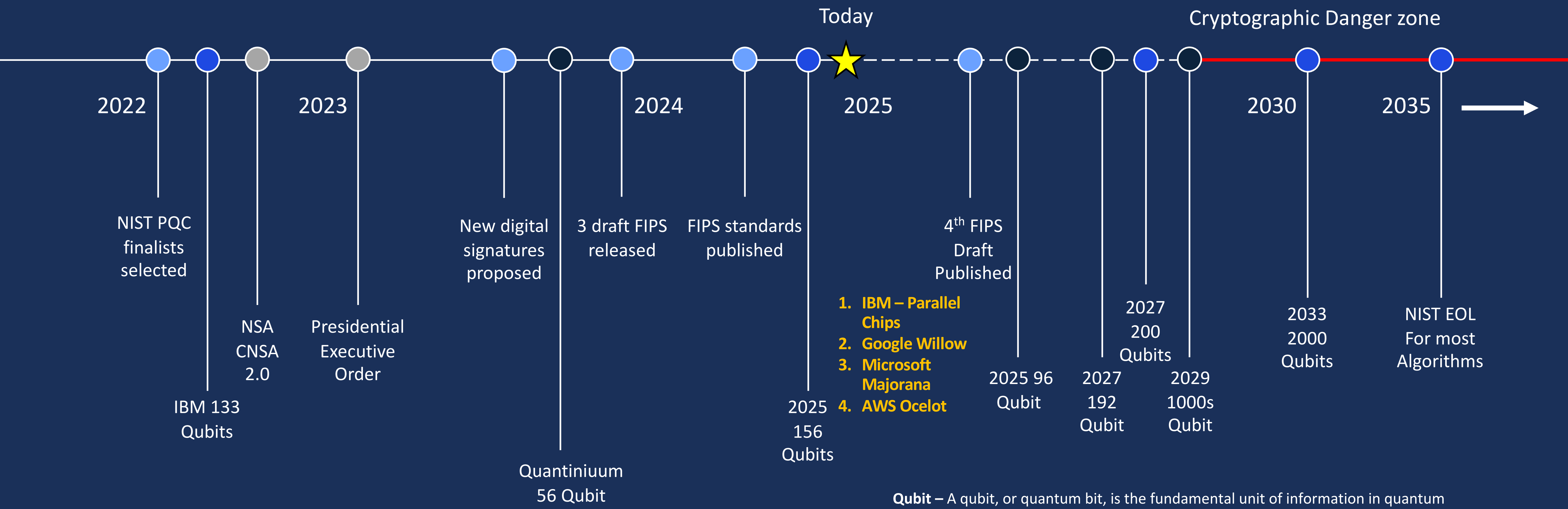
Quantum Risk

The PQC Hype Train

- Despite alarming headlines, organizations have time to implement a phased, hybrid approach which can mitigate quantum threats without disruption by conducting thorough cryptographic inventories, prioritizing critical systems, and maintaining crypto-agility—allowing for a smooth transition that balances security needs with operational stability
- Organizations should begin their post-quantum cryptography transition as NIST will deprecate current algorithms (RSA, ECDSA, DH) by 2030 and fully disallow them by 2035
- ”Harvest now, decrypt later" attacks already threaten sensitive data with long-term value

Quantum is Now. Q-Day is Coming…

CNSA 2.0 Migration timeline (preferred for NSS by mid-2020s, required by early 2030s



1. **IBM – Parallel Chips**
2. **Google Willow**
3. **Microsoft Majorana**
4. **AWS Ocelot**

Qubit – A qubit, or quantum bit, is the fundamental unit of information in quantum computing. Unlike a classical bit, which can only represent 0 or 1, a qubit can exist in a superposition of both states simultaneously, leveraging quantum mechanical properties like superposition and entanglement to perform complex computations more efficiently

Why is Quantum Important?

NIST’s releasing of the first Post Quantum Cryptography (PQC) Standards allows organizations to begin planning for the PQC migration! For 2025 the OCC has begun asking questions around quantum and 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.

Security and Risk Governance

Post-Quantum Cryptography (PQC)

Threats to Current Encryption:

Quantum computers can break traditional encryption methods like RSA and ECC, necessitating a shift to PQC. This transition is critical to safeguard financial transactions and data.

NIST Standards:

NIST has published standards for PQC, with a migration deadline by 2030. Financial institutions must begin adopting quantum-resistant cryptography to protect against future threats.

NIST Cryptographic Deprecation

Timeline to End of Life:

NIST's draft report outlines the transition to post-quantum cryptography, with quantum-vulnerable algorithms phased out by 2030 and fully disallowed by 2035. The plan emphasizes adopting quantum-resistant standards to safeguard against future quantum computing threats.

NIST Guidance:

NIST is deprecating widely-used cryptographic algorithms vulnerable to quantum attacks, including RSA, ECDSA, EdDSA, Diffie-Hellman (DH), and Elliptic Curve Diffie-Hellman (ECDH).

FS-ISAC Guidance

Quantum-Resistant Cryptography:

FS-ISAC advocates for adopting quantum-resistant cryptography to safeguard the integrity of the global financial network. Their guidance includes maintaining robust cyber hygiene practices and conducting thorough risk assessments.

PCI Industry Guidance:

FS-ISAC provides detailed guidance for transitioning to quantum-resilient standards in the payment card industry, emphasizing the importance of proactive planning.

PCI DSS 4.0 and CA Reporting

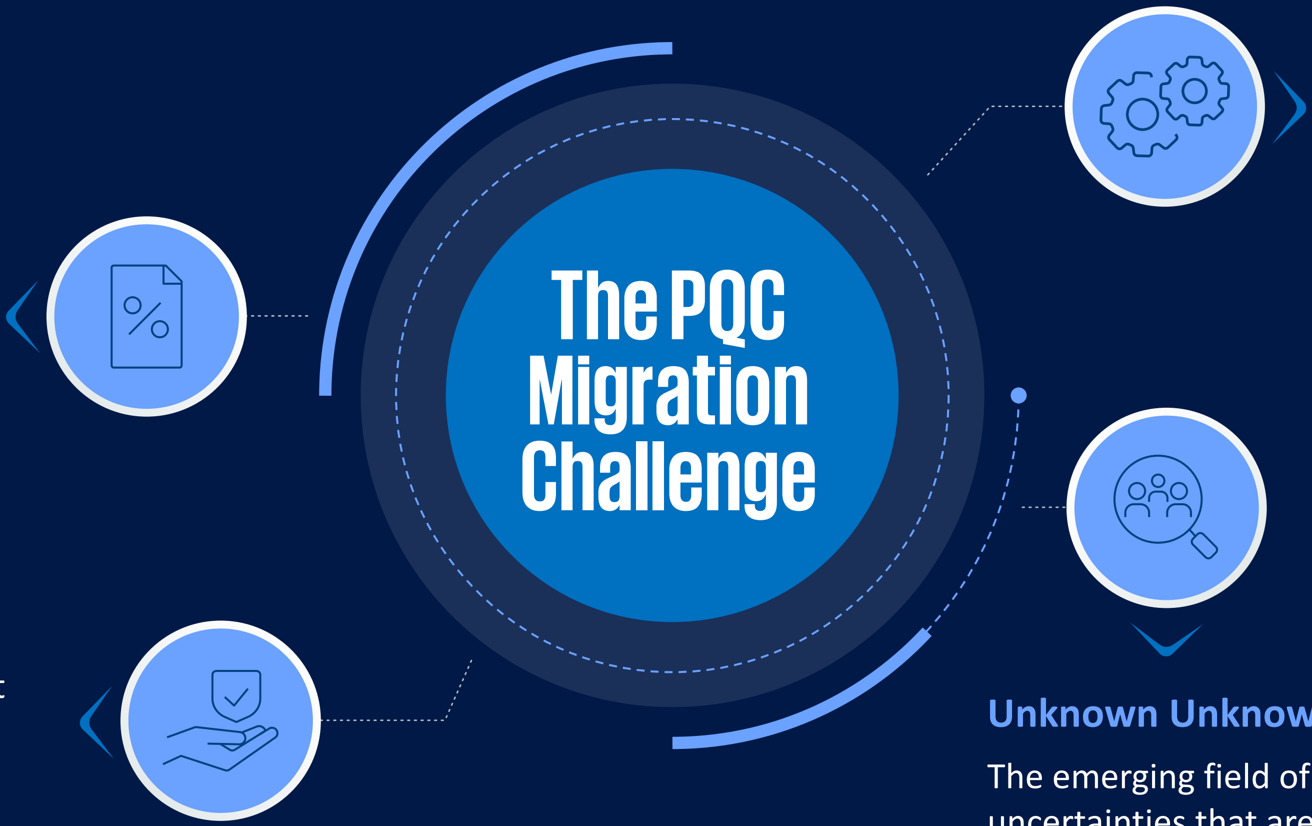
Cryptographic Agility:

PCI DSS 4.0 requires maintaining an inventory of cryptographic ciphers and planning for PQC migration by 2035.

Organizations must monitor industry trends and document procedures for ongoing surveillance of cryptographic standards.

CA Reporting:

Compliance with PCI DSS 4.0 involves regular reporting on cryptographic practices to ensure readiness for quantum threats.



The PQC Migration Challenge

Technical Debt

Enterprises often rely on legacy systems that lack the flexibility to integrate or support advanced PQC algorithms, necessitating substantial overhauls or upgrades that can be both time-consuming and costly.

Supply Chain Security

The interconnected nature of modern supply chains means that any weakness in a partner's cryptographic infrastructure can pose significant vulnerabilities, making it essential to coordinate and enforce PQC standards across a diverse array of suppliers and stakeholders.

Vendor Management

Ensuring that third-party vendors are aligned with PQC protocols can be complicated, as it involves comprehensive audits, negotiations, and often depends on the vendors' own readiness to adopt quantum-resistant technologies.

Unknown Unknowns

The emerging field of quantum computing introduces uncertainties that are difficult to anticipate, including unforeseen vulnerabilities and complexities in new PQC algorithms, making it challenging for enterprises to fully prepare and ensure comprehensive security against future quantum threats.

Cryptographic Change

Understanding Cryptographic Agility

•Definition: Ability to replace cryptographic algorithms with minimal impact on system functionality.

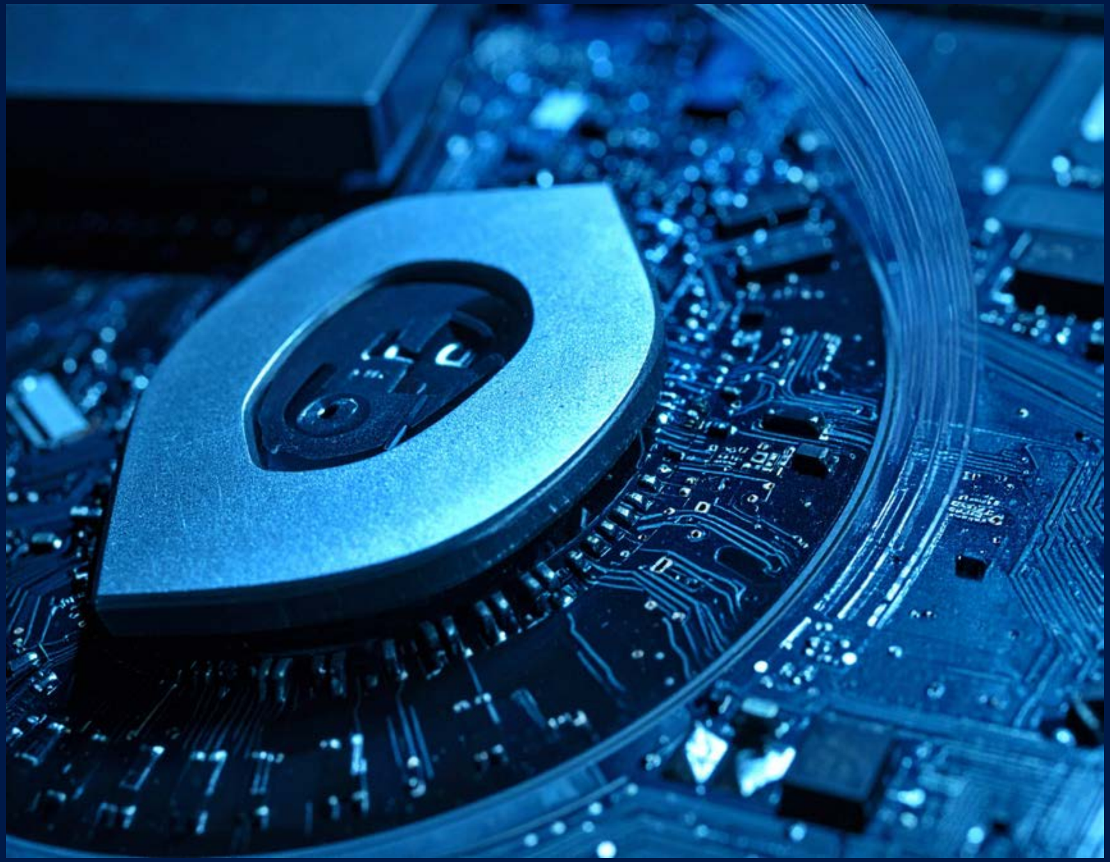
•Purpose: Facilitates smooth transitions to new cryptographic methods, such as post-quantum cryptography (PQC).

•Key Benefits:

- Reduces cost, time, and resources during algorithm updates.
- Minimizes information security risks during transitions.

•Relevance to Hybrid Cryptography:

- Supports adoption of hybrid systems during migration.
- Enables shift from hybrid to full PQC or other future methods.



KPMG

Introduction to Hybrid Cryptography

•**Definition:** Combines post-quantum cryptography (PQC) with another public-key system (PQC or traditional) for the same cryptographic objective

•**Common Objectives:** Digital signatures and key establishment

•**Goal:** Achieve security of the strongest method in the combination

•**Non-Hybrid Examples:**

- Out-of-band key contributions (e.g., passwords, quantum key distribution).
- Different cryptosystems at different protocol layers.
- Public-key encryption with symmetric cryptography (e.g., RFC 9180).

Vendor Migration

Vendor Integration to Migration Roadmap

Ensures Interoperability: Aligning with vendors' post-quantum cryptography (PQC) plans prevents compatibility issues across systems and services.

Mitigates Supply Chain Risks: Coordinated migration reduces vulnerabilities in third-party components during the transition to PQC.

Streamlines Compliance: Incorporating vendor timelines ensures adherence to regulatory and industry PQC standards.

Optimizes Resource Allocation: Synchronized schedules with vendors avoid redundant efforts and resource conflicts.

Accelerates Deployment: Leveraging vendors' PQC expertise and updates speeds up your organization's migration process.

Reduces Long-Term Costs: Proactive alignment minimizes future rework or emergency updates due to misaligned vendor plans.

PQC Roadmap" questions for vendors

What can you share about your roadmap for including post-quantum cryptography (PQC) in your [Product / Service], such as a timeline for when PQC support will be available to customers for all quantum-vulnerable public key cryptography usage by your [Product / Service]?

Will support for PQC in your [Product / Service] be made available through patches or updates under existing contracts and purchases?

Will your [Product / Service] require customers to replace existing hardware or make system architecture changes to support the PQC migration?

PQC Roadmap” questions for vendors cont.

How will your [Product / Service] support cryptographic agility to allow flexible administration of configurations for planned cryptographic migration, or an unplanned and immediate migration to remediate a weakness in an algorithm?

What operational/configuration guidance will you be providing customers on how to migrate your [Product / Service] to utilize PQC?

When your [Product / Service] is updated to support PQC, will you ensure the cryptography is independently validated for implementation assurance, for example FIPS 140-3 certification under the Cryptographic Module Validation Program (CMVP)?

Are your 3rd party suppliers aware of and addressing the quantum computing threat, and are you evaluating how their PQC posture may impact your business operations and your customers?

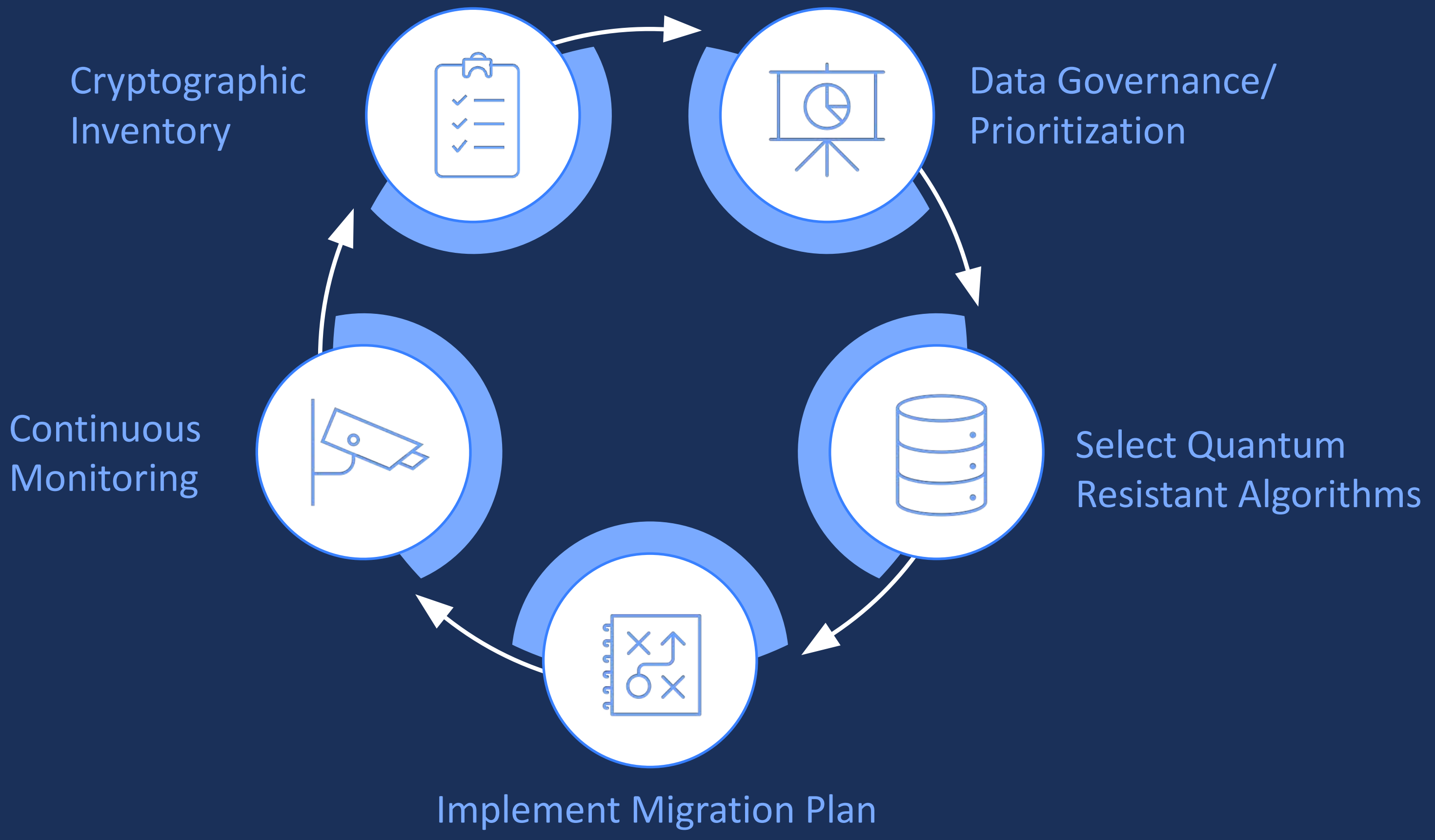
What's Next?

Quantum Risk Assessments

The urgent shift to post-quantum cryptography (PQC) is critical to protect data against new quantum threats.

Quantum Resistance

Planning for post-quantum cryptography (PQC) migration should begin now due to the imminent threat posed by quantum computing.

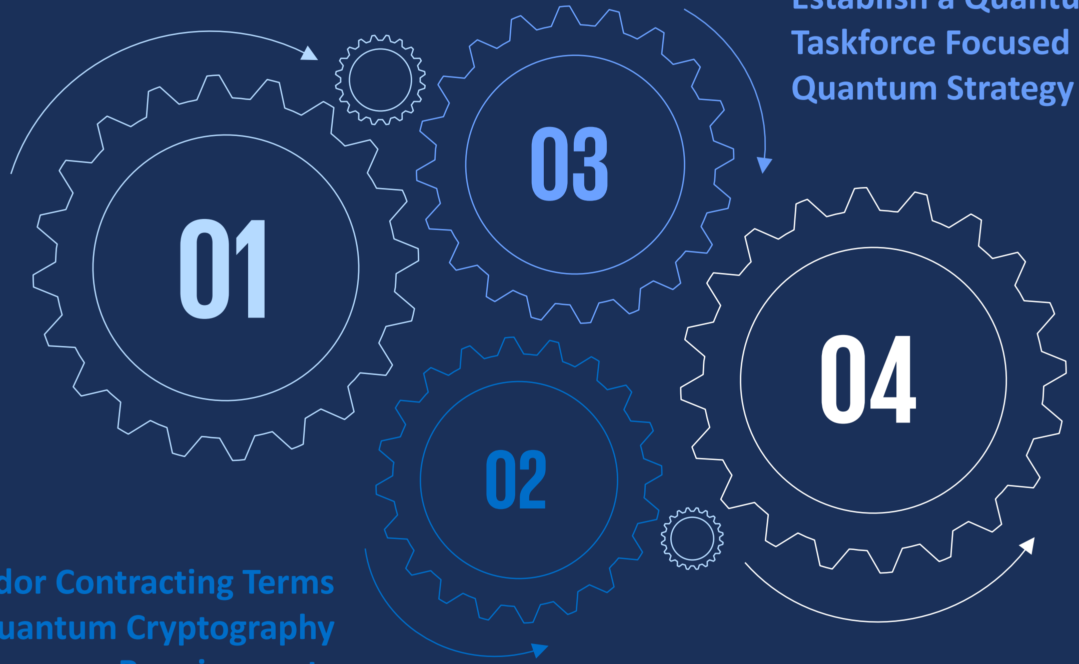


Call to Action

As your organization prepares for the advent of quantum computing, there are several critical considerations you should keep in mind:

Key Takeaways

Quantum computing has entered the utility age and organizations need to begin preparations for new computing paradigm.



Evaluate Your Exposure to Quantum Risk

Align Vendor Contracting Terms to Post Quantum Cryptography Requirements

Establish a Quantum Taskforce Focused on Enterprise Quantum Strategy

Scan the Horizon for Quantum Disruption!

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.