KPMG

Q-PREP

Quantum Preparedness and Readiness Evaluation Program

Quantum computing is rapidly advancing, threatening to break traditional encryption and expose sensitive data. Starting your postquantum cryptography (PQC) journey now helps ensure your organization stays ahead, safeguarding critical assets against tomorrow's quantum risks.

The time is now

The urgent need for PQC readiness stems from the rapid advancement of quantum computing, which threatens to break traditional encryption methods like Rivest–Shamir–Adleman public-key cryptosystem and elliptic curve cryptography, exposing sensitive data to future attacks. As quantum technology nears practical application, organizations must proactively adopt quantum-resistant algorithms to safeguard critical assets and ensure compliance with emerging regulatory standards. Delaying PQC readiness risks catastrophic breaches and operational disruptions, making it essential to start the transition now to stay ahead of the quantum threat curve.

Q-PREP

The KPMG quantum preparedness and readiness evaluation program (Q-PREP) framework provides a logical, seven-step roadmap to guide organizations toward PQC preparedness, addressing the complexities of transitioning to quantum-resistant security in a structured and strategic manner. By systematically tackling the challenges of quantum threats, Q-PREP helps ensure organizations can safeguard critical assets, maintain operational continuity, and comply with evolving standards. This framework combines technical knowledge and strategic foresight to deliver a clear path to quantum resilience. The following seven steps lay out a coherent and actionable path to achieve quantum readiness.

The process begins with preparation and scope, aligning PQC objectives with business goals to set a solid foundation. Next, the cryptographic asset inventory maps algorithms, keys, and certificates, identifying quantum-vulnerable assets. Risk and data governance prioritizes risks and establishes compliance policies, clarifying data priorities and requirements.

The PQC solutions exploration phase evaluates quantum-resistant algorithms for smooth integration within existing infrastructure. Transition plan development crafts a strategic, incremental migration plan to help minimize disruptions. Implementation and remediation deploys PQC solutions, validates their effectiveness, and resolves vulnerabilities uncovered during the process.

Q-PREP culminates in continuous monitoring, helping ensure sustained resilience by adapting to emerging threats and evolving standards. This cohesive roadmap simplifies the intricate challenge of quantum preparedness into a manageable, forward-thinking strategy.

> "Migrating to postquantum cryptography is like conducting a symphony across a vast IT landscape, retuning keys, algorithms, and certificates without missing a note. The complexity lies in mapping hidden cryptographic assets in legacy systems and integrating quantum-resistant solutions seamlessly. Any oversight could expose critical data to quantum attacks."
>
> — **Dr. Aaron Kemp**
> US Quantum Lead, KPMG LLP

PQC roadmap

The path to readiness

Building a roadmap for PQC readiness presents significant challenges due to the complexity and evolving nature of quantum threats. Organizations often struggle with identifying all cryptographic assets across their systems, as legacy infrastructure and decentralized information technology (IT) environments can obscure vulnerabilities. Additionally, the lack of standardized PQC algorithms and the need for cryptographic agility—ensuring systems can adapt to new standards—complicate planning. Resource constraints, including limited expertise and budget, further hinder progress, while the urgency to comply with emerging regulations, such as those emphasizing quantum-resistant frameworks, adds pressure to act swiftly. Furthermore, integrating PQC solutions without disrupting existing operations requires careful planning to avoid costly downtime. The dynamic pace of quantum advancements also demands ongoing updates to strategies, making long-term readiness a moving target.

Preparation and scope
Define project objectives and align with business goals to establish a clear foundation for the PQC transition

Cryptographic asset inventory
Catalog all cryptographic assets, including algorithms, keys, and certificates, to identify quantum-vulnerable systems and prioritize PQC transition efforts

Risk and data governance
Establish policies and frameworks to manage cryptographic data lifecycle, ensuring compliance, security, and alignment with quantum-resistant standards

Implementation and remediation
Deploy quantum-resistant cryptography across systems, validate effectiveness, and address vulnerabilities through targeted remediation actions

Transition plan development
Create a strategic plan outlining timelines, resources, and milestones for migrating to PQC solutions with minimal operational disruption

PQC solutions exploration
Evaluate and test quantum-resistant algorithms and protocols to identify scalable, compatible solutions for organizational needs

Continuous monitoring
Maintain long-term resilience by monitoring emerging quantum threats, updating algorithms, and adapting to evolving standards

KPMG quantum

KPMG quantum leverages extensive experience in quantum technologies and cybersecurity to guide organizations through the complexities of PQC adoption. Through the Q-PREP framework, KPMG LLP helps your organization build a tailored PQC roadmap, helping ensure quantum resilience and compliance with emerging standards.

Contact us

Dr. Aaron Kemp
US Quantum Lead,
KPMG LLP
T: 404-358-3138
E: aaronkemp@kpmg.com

Dr. Lekshmy Sankar
US Quantum Security Lead,
KPMG LLP
T: 303-495-8125
E: lekshmysankar@kpmg.com