KPMG

Emerging Tech Risk –Quantum

The Quantum Computing Revolution

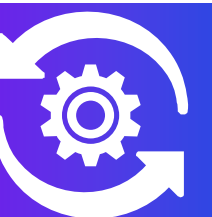
Billions of dollars are being spent globally on building Quantum Computers.

This new type of computation can transform how we tackle a variety of problems across many industries.

Drug Discovery

Financial Modelling

Communication Networks



Process Optimisation

KPMG

Cryptographically relevant quantum computers may become a reality quicker than many anticipate.

Organisations need to start their quantum readiness planning to mitigate the risks now.

KPMG

“Harvest now, decrypt later” attacks

could enable adversaries to steal encrypted files and store them until more advanced quantum computers emerge.

All data that is not quantum secure now, is a liability.

Information systems that rely on cryptographic functions are at risk

Confidentiality

Safeguarding payment information when shopping online.

Integrity

Ensuring that the contents of an email has not been maliciously altered during transit.

Authentication

Authorised access into almost every type of digital system.

Digital Signatures

Prevent the forgery of documents, websites or digital messages and conversations.

Industry Standards and Publications

In August 2024, NIST Released the first 3 finalised Post-Quantum Encryption Standards

Key Encapsulation Standard
- **FIPS 203**

Digital Signature Standard
- **FIPS 204 (Primary Standard)**
- **FIPS 205 (Backup Standard)**

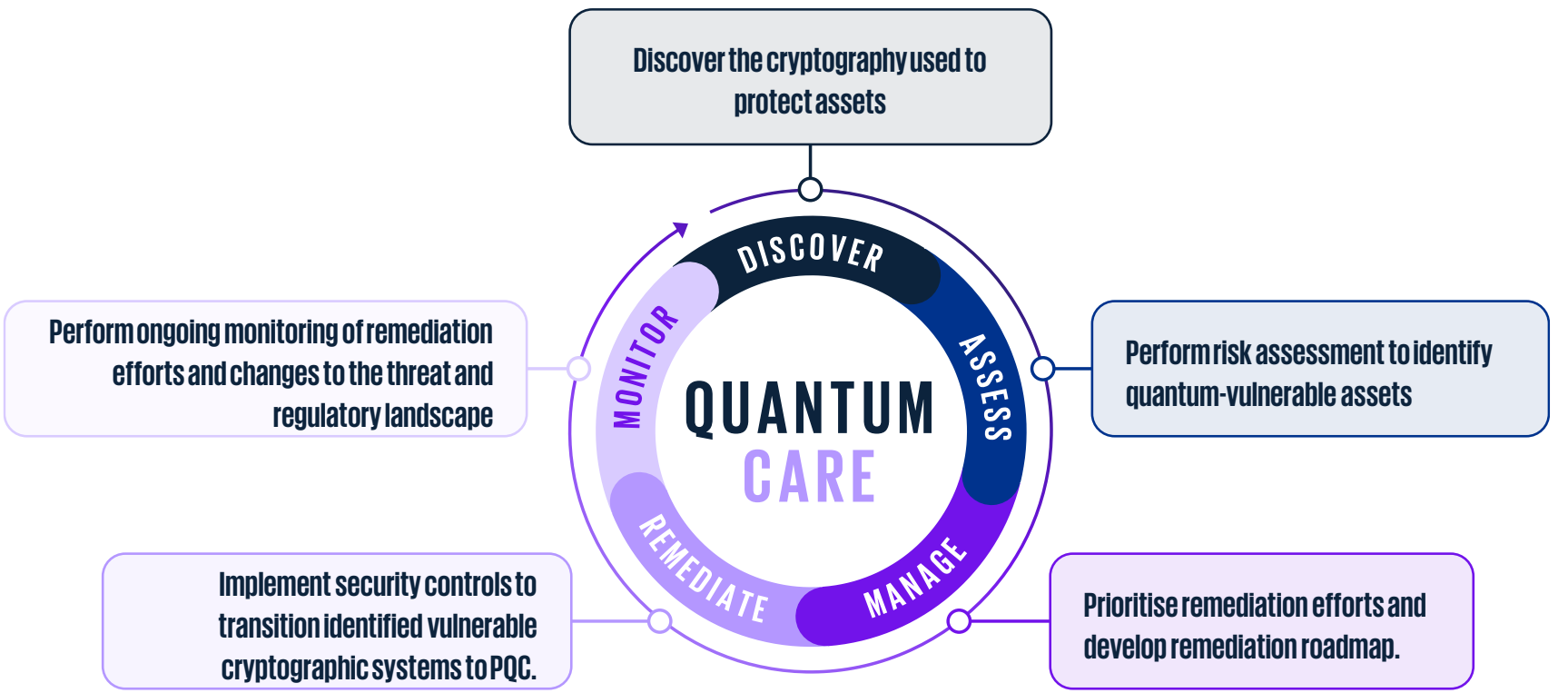
G7 Cyber Expert Group releases recommendations for addressing quantum computing risk - September 2024

- Developing a better understanding of quantum computing, the risks involved, and strategies for mitigating those risks.
- Assessing quantum computing risks in their areas of responsibility.
- Developing a plan for mitigating quantum technology risks.

Monetary Authority of Singapore Advisory on Addressing the Quantum Cyber Security Threat – February 2024

- Monitor developments in quantum computing
- Raise awareness of associated cyber security risks
- Maintain an inventory of cryptographic assets
- Prioritise critical assets for migration to quantum resistant encryption and key distribution
- Develop strategies and building capabilities to address quantum cybersecurity threat

The KPMG Quantum Care framework can help you on your quantum security journey, starting with a readiness assessment and roadmap



Contact us

Eddie Toh
Partner
Cyber, Advisory
KPMG in Singapore
T: +65 6213 3028
E: eddietoh@kpmg.com.sg

Wendy HQ Lim
Partner
Cyber, Advisory
KPMG in Singapore
T: +65 6411 8263
E: wlim@kpmg.com.sg

Paul Lothian
Director
Cyber, Advisory
KPMG in Singapore
T: +65 9724 0297
E: plothian1@kpmg.com.sg

kpmg.com.sg