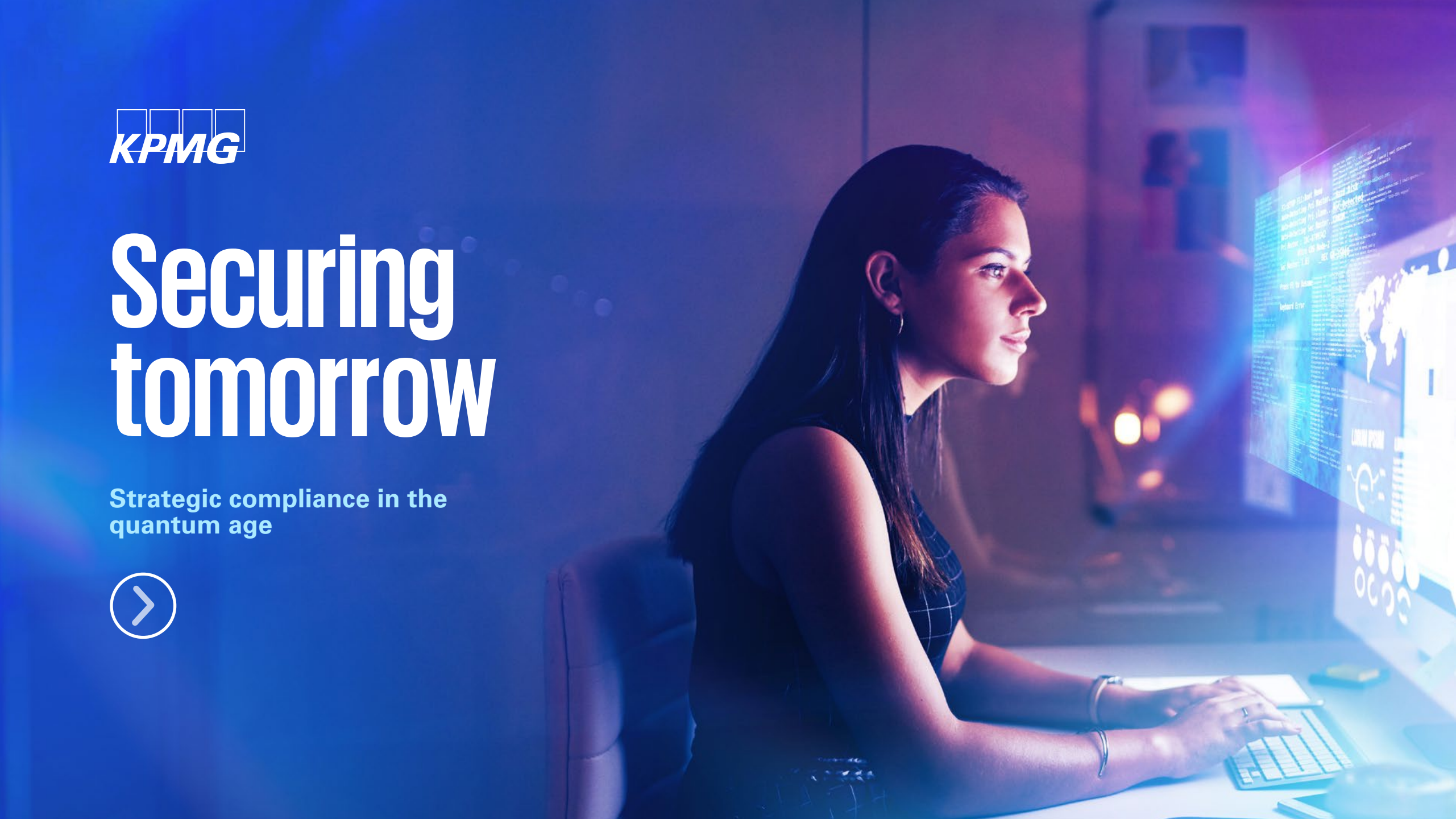
KPMG

Securing tomorrow

Strategic compliance in the quantum age



Why it's time to act

As quantum emerges into the mainstream, organisations and governments are starting to explore its game-changing advantages and threats. This will bring new legislation and new regulations that will change the cyber landscape.

Quantum technology is not just a future consideration, but a more immediate imperative due to regulatory shifts such as the Quantum Computing Cybersecurity Preparedness Act. This new US law mandates federal IT systems to adopt quantum-resistant cryptography, setting a precedent that stretches globally. Businesses operating internationally and with the US face a new reality: adapt to emerging cyber security standards that consider the potential impacts of quantum computing, or risk being locked out of markets that are aligning with new legislative requirements.

Avoiding disruptions and crippling breaches

This quantum era threatens to make current cyber security measures obsolete, exposing sensitive data and critical infrastructure to unprecedented risks. Given the pace of quantum advancements, current cryptographic systems could be fundamentally disrupted as early as 2032. Financial transactions, healthcare records, and national security communications are particularly vulnerable. Without robust quantum-resistant frameworks, organisations risk severe disruptions and breaches that could potentially cripple their operations. The concept of 'Harvest Now, Decrypt Later' underscores the urgency; data encrypted today must withstand future quantum attacks, making outdated systems a ticking time bomb in current procurement strategies.

Working with KPMG to protect against quantum threats

Recognising these challenges, KPMG's Quantum Care Framework is an essential service to help navigate this transition. This comprehensive and strategic initiative is designed to transition organisations to quantum resilience. By partnering with KPMG, companies can align with current and upcoming regulations and protect themselves against the quantum threats on the horizon. KPMG's approach provides a competitive edge in a future where quantum technology defines market viability. In this rapidly evolving landscape, the Quantum Care Framework is a necessary tool for any forward-thinking organisation aiming to thrive in the quantum age, ensuring they remain compliant, secure, and ahead of the curve.

Quantum challenges and cyber security preparedness

Recent advancements in quantum computing present significant challenges to the cryptographic systems essential for national security and economic stability.

Protecting encrypted data

While it may seem like a long time away, cyber experts fear that many state and criminal actors are harvesting encrypted data now, and saving it until it can be decrypted later. Several events fit the profile of Harvest Now, Decrypt Later (HNDL) attacks. In 2016, internet traffic heading to South Korea from Canada was unexplainably and persistently ending up in China. In 2020, data from over 200 networks belonging to companies such as Google, Facebook and Amazon was channelled through Russia. These potential HNDL scenarios highlight the risk that sensitive data with a lifespan of 10–15 years is already vulnerable.

The remediation deadline to protect against this threat is fast approaching, or in some cases may have already elapsed. The longer an organisation delays addressing vulnerable encryption technologies, the greater the volume of data at risk.

In late 2022, the US enacted the Quantum Computing Cybersecurity Preparedness Act, which President Biden signed into law, mandating federal IT systems transition to quantum-resistant cryptography. This legislation emphasises the need for both public and private sectors to enhance their cryptographic frameworks in preparation for quantum capabilities that could decrypt currently secure information.

What is quantum-resistant cryptography?

Quantum computers have the potential to solve certain mathematical problems much faster than today's computers. This capability is likely to break many of the cryptographic systems currently in use, posing significant cyber security risks. Quantum-resistant technology aims to create new cryptographic methods that remain secure even in the presence of powerful quantum computers – relying on mathematical problems that are hard for both quantum and traditional computers to solve.

Quantum-safe cryptography in banking

The Emerging Payments Association Asia (EPAA) has formed a working group on quantum-safe cryptography, with the aim of encouraging the adoption of quantum-safe cryptography in the banking industry. It will involve studying policy, regulation, and operator business processes to develop best practices for the implementation of quantum-safe cryptography, with founding members including HSBC, AP+, Paypal and IBM. The group says that it 'aims to enhance the protection of payment rails and processes in anticipation of advanced quantum computing that will be able to compromise existing cryptography', adding that it will work to 'help define requirements, identify dependencies, use cases, and create a roadmap to implement post-quantum networking'.

Global preparations for quantum resilience

Amid concerns over nations seeking technological advantages, the US Federal Bureau of Investigation (FBI), and the Quantum Information Science Counterintelligence Protection Team (QISCPT) are enhancing collaborations across various sectors to protect technological advancements and prevent espionage. Globally, movements towards quantum readiness are accelerating, evidenced by the World Economic Forum's Quantum Readiness Toolkit and the Monetary Authority of Singapore's cyber security circular to financial leaders.

These initiatives underscore a global commitment to preparing for the transition to a quantum future. This requires a unified effort from industry leaders to shape standards, comprehend legislative changes, and invest in quantum-resistant technologies to safeguard future operations and ensure security in the quantum era.

The quantum threat landscape

The rise of quantum computing poses significant risks to current cryptographic systems, threatening to make them obsolete and leaving numerous sectors vulnerable.

As quantum capabilities advance, with cryptographically relevant quantum computers (CRQC) potentially emerging by 2037 and significant developments expected by 2032, there is pressure on industries and governments to develop quantum-resistant technologies. The economic impact of quantum technology could approach US$1.3 trillion by 2035, a projection underscored by the US government's US$3.7 billion investment in this area. The quantum threat varies across sectors: financial transactions and data, patient and pharmaceutical data in healthcare, national infrastructure, secure communications, and technological innovations are all at risk of security breaches.

The risk of outdated cryptography

The reliance on outdated cryptographic systems exposes organisations to a range of malicious activities that could severely disrupt operations. Cyber security vulnerabilities could potentially enable attackers to manipulate documents through forged updates or fraudulent authentication, decrypt confidential historical data, and alter legal documents undetected, by counterfeiting digital signatures.

Further risks include the creation of fake website identities and software downloads, which can mislead users and spread malware, as well as extortion attacks where attackers demand ransom under the threat of disclosing sensitive data. For instance, we could see a future where banking or retail websites are copied, and it's impossible to tell the real from the fake.

Building quantum-resilient infrastructure

Organisations need to stay ahead of developments from cryptographic standards organisations and begin testing and deploying lattice-based signature schemes, which are currently considered resistant to quantum attacks.

Microsoft have initiated a Quantum Safe Project which focuses on their transition to quantum safety and the adoption of post quantum cryptography standards across their products, services and data centres.

Encryption breakdown and data retention

Quantum computing poses a significant threat to current cryptographic algorithms, such as RSA, ECC, and symmetric key algorithms, which rely on computational complexities that quantum computers can potentially solve in eight hours, as opposed to 300 trillion years for today's computers.

To mitigate these risks, organisations need to proactively integrate post-quantum cryptography (PQC) algorithms, which are currently under development. Standard-setting bodies like the National Institute of Standards and Technology (NIST) in the US are responsible for standardising post-quantum cryptography and making these mathematical tools available, so that organisations can integrate them into their encryption infrastructure.

Additionally, re-evaluating data retention policies to limit the duration that sensitive data is stored can help minimise exposure. Implementing strict policies to retain data only when necessary, and securely deleting data that is no longer needed, is essential for enhancing data security in anticipation of quantum computing advancements.

IBM has developed Quantum Safe, a set of tools, capabilities and approaches for securing enterprise for the quantum future. It has also created quantum-resilient infrastructure in their mainframes to enable dual-signing schemes using lattice-based post-quantum cryptography.

Secure communication and blockchain threats

Quantum computing poses severe risks to secure communication protocols like VPNs (Virtual Private Network) and SSH (Secure Shell), as well as to the cryptographic foundations of blockchain and cryptocurrencies. For example, the threat to Bitcoin, would be the compromise of cryptographic hashes, affecting blockchain integrity and mining. Grover's algorithm poses a risk to cryptographic hashing and Shor's algorithm can crack the encryption used to protect individual wallets.

Based in Canberra, Australia, Quintessence Labs is at the forefront of using quantum technology in cybersecurity, developing tools such as qStream, a quantum random number generator that provides full entropy encryption keys, and qOptica, their solution for Quantum Key Distribution.

Quantum compliance as a strategic imperative

In the evolving quantum era, adherence to quantum compliance is becoming a strategic inevitability, central not just for maintaining security but to ensure a competitive edge and meet legal requirements.

Vulnerable supply chains and technologies

As quantum computing advances, it exposes significant weaknesses, such as inconsistent security measures in supply chains involving multi-tiered hardware and software suppliers. This risk is compounded by the growing reliance on Software as a Service (SaaS) models, which further exposes companies to quantum threats if not properly managed. It is critical for companies to secure their information through detailed contractual agreements, stringent assurance policies, and a thorough understanding of where critical information and communication technology (ICT) assets are located within the supply chain.

With over 20 billion digital devices anticipated to require updates or replacements within the next 10 to 20 years to support quantum-safe communications, organisations need to reassess their procurement strategies today. This dual pressure of enhancing supply chain security and updating procurement processes to include quantum-resistant technologies, is critical for companies to manage budgetary impacts effectively and maintain competitive advantage.

Bridging corporate knowledge gaps

A lack of understanding about quantum computing and its implications on current technological infrastructures can significantly compromise an organisation's preparedness against cyber attacks. A solution is to develop comprehensive training programs for IT and security teams. These programs should focus on quantum computing and its security implications and could include hosting seminars with quantum experts and establishing knowledge-sharing platforms to enhance understanding and awareness.

This taskforce aims to outline requirements, identify dependencies, use cases, and develop a roadmap for implementing post-quantum networking, mitigating risks associated with future quantum computers.

Existing and emerging quantum guidelines

The White House, through National Security Memoranda 10, has directed specific actions for federal agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography. The objective is to promote a timely transition of the Nation's

Meanwhile, NATO has already updated its cryptographic systems to be quantum-safe, and companies like HSBC and JP Morgan are investing in the use of Quantum Key Distribution for quantum secure trading networks.

The telecommunications sector, for instance, has started gearing up for the quantum era. Last year, the Global System for Mobile Communications Association (GSMA) initiated the Post-Quantum Telco Network Taskforce. Founding members, including major players like IBM and Vodafone, are collaborating to outline policy, regulation, and operational processes that safeguard telecom operations from quantum threats.

cryptographic systems to interoperable quantum-resistant cryptography. This will include activities such as establishing a cryptographic bill of materials (CBOM), working groups to advance adoption of quantum-resistant cryptography and following the release of quantum-resistant cryptography standards from NIST, a timeline for the deprecation of quantum-vulnerable cryptography by 2035.

Implementing a Quantum Care Strategy with KPMG

KPMG's Quantum Care Framework

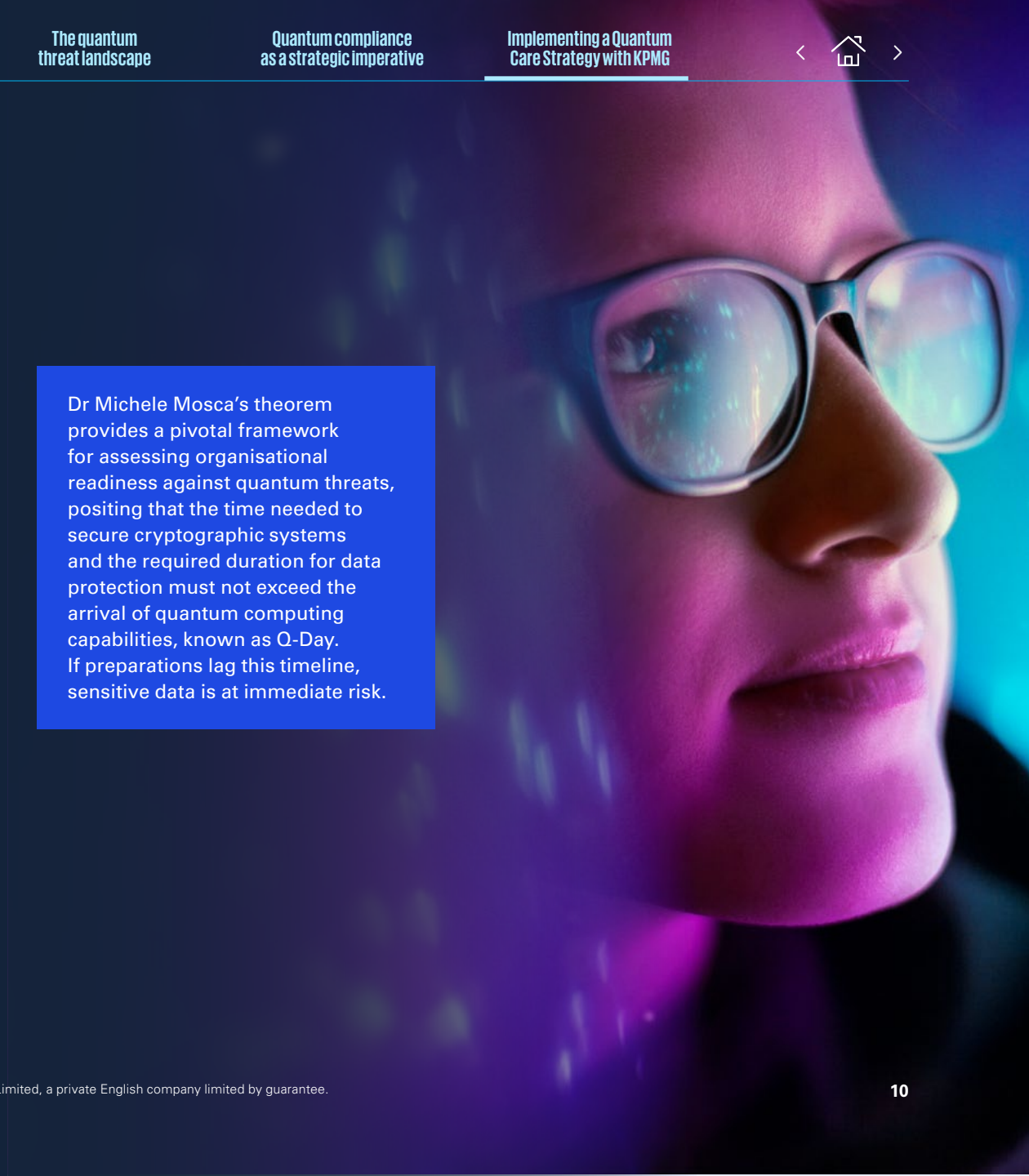
Given the uncertainties of quantum computing development and increasing regulatory scrutiny, many organisations – particularly those with resource constraints – face challenges in prioritising quantum readiness, risking non-compliance and potential vulnerabilities. In response, KPMG has developed Quantum Care, a comprehensive. strategy to prepare industries and organisations against quantum threats.

KPMG's methodology is designed to help organise and enhance an organisation's cyber security for quantum resilience. This involves evaluating risks and implementing strategic defences, ensuring that organisations are well-prepared for the quantum future. For businesses looking to secure their operations against quantum threats, partnering with KPMG to audit and enhance quantum resilience is not just a strategic move – it's an essential process to ensure future viability and security in a rapidly evolving technological landscape.

Quantum risk assessment

Understanding the risk is crucial for laying the groundwork for deeper analysis and action. It focuses on educating clients about the quantum threat, ensuring they understand the significant risks posed by quantum computing advancements. During this phase, KPMG also identifies which assets are most at risk from quantum threats, performs an assessment of these critical assets, and helps clients understand their overall risk profile. This phase is essential for clients to recognise the importance of proactive measures and to prioritise their cyber security efforts effectively.

Dr Michele Mosca's theorem provides a pivotal framework for assessing organisational readiness against quantum threats, positing that the time needed to secure cryptographic systems and the required duration for data protection must not exceed the arrival of quantum computing capabilities, known as Q-Day. If preparations lag this timeline, sensitive data is at immediate risk.



KPMG's Quantum security journey

KPMG self assesment

As part of our journey towards quantum security resilience, our Cyber team carried out a quantum risk assessment on KPMG Australia, using the Quantum Care methodology.

The first step of the process was to identify asset categories that are more susceptible to a harvest-now-decrypt-later attack. Key assets were then selected for each category to include in the risk assessment.

We worked across our organisation, with asset owners, security and business SMEs to extract the necessary information to perform the assessment.

The benefit of this approach was that it provided a holistic view of the quantum cyber risk for our management and served as a learning process for the internal risk and cyber teams. This is a significant long-term issue, so organisations will need to broaden cyber expertise and empower their organisations to manage this increasing and ongoing risk.

Is your organisation quantum ready?

While it is uncertain when Q-Day will arrive, the nature of HNDL attacks requires action today. Getting ahead of legislation and embedding quantum-resilient infrastructure will require significant preparation that requires action now.

"KPMG's Quantum Care Methodology emphasises a proactive and structured response to the challenges of quantum computing. It ensures that organisations not only understand the quantum threats but are also well-prepared to implement robust quantum-resistant measures."

MICHAEL EGAN
Director Quantum Technologies

Quantum Care

The core phase implements a lifecycle approach to asset protection that encompasses several key activities:

- **Discovery**: This phase aims to involve the necessary stakeholders, to ensure comprehensive protection strategies are developed, to map out the technologies at risk, while considering the sensitivity of the information.
- **Risk assessment**: Here, the focus shifts to performing an assessment to determine the level of risk each asset is exposed to if its encryption is broken. This assessment helps in developing a high-level roadmap for remediation and creating a detailed inventory of the cryptographic controls in use.
- **Management**: In the management step, detailed remediation recommendations are formulated, and the remediation roadmap is refined. This determines the prioritisation of the remedial actions.
- **Remediation**: The remediation activities include implementing enhancements to existing security controls, integrating cryptographic agility, and adopting post-quantum cryptography (PQC). These measures are crucial for safeguarding against the threats posed by quantum computing.
- **Monitoring**: The final step involves continuous monitoring of the risks identified during the assessment, the effectiveness of the cryptographic measures implemented, and the evolving quantum threat and regulatory landscape.

Reach out to the team to see how we can help you mitigate risk and prepare for a secure quantum future.

Contact

Michael Egan
Director, Quantum Technologies
+61 3 9288 5671
megan5@kpmg.com.au

James Mabbott
Partner in Charge, KPMG Futures
+61 2 9335 8527
jmabbott@kpmg.com.au

KPMG.com.au

June 2024. 1267994742FUT.