Quantum impact on cyber in the UK

Assuring your navigation into the quantum computing era

Technology risk assurance UK: May 2025

The better the question. The better the answer. The better the world works.

EY

Shape the future with confidence

Contents

Quantum technology and the impact on data security

Quantum technology

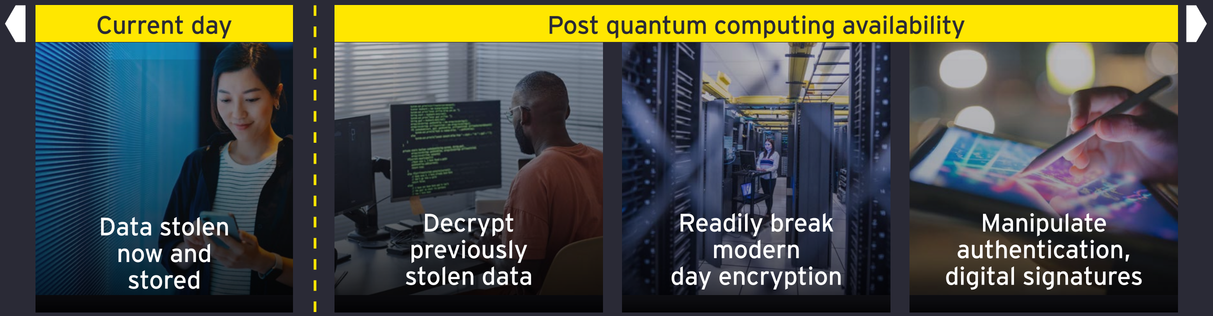
Quantum technology has significant disruption potential. Some examples include: quantum sensing which can achieve unprecedented accuracy and resolution in measurement diagnostics, quantum communication utilising quantum key distribution for secure data transmission, quantum simulation which can solve optimisation problems beyond the conceivable reach of classic computer processors, quantum random number generation (QRNG) which can generate truly random numbers for use in simulation and quantum computing which can help optimise the solution to complex problems as well as enhancing artificial intelligence (AI) capability through faster training of more complex models.

Quantum computers work on quantum bits (or qubits) as opposed to classical bits. Quantum technology is rapidly advancing with announcements from major players and a full-scale quantum computer is now expected to be ready **with significant risk (probability x impact) in the next decade.** They are known to solve certain problems exponentially faster than a classical computer.

This can lead to huge opportunities in sectors such as chemical, life sciences, energy, telecommunications, financial services, logistics and many more. Inevitably, the advances in quantum technology can pose significant risks. Quantum computers can efficiently break classical encryption methods such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). Whilst RSA would take a classical computer millions of years to break, this would take a few hours on a cryptographically capable quantum computer. They can also weaken other encryption methods effectively halving their key length, for example Advanced Encryption Standard (AES) and Secure Hash Algorithms (SHA).

There is a need for all organisations to move towards post quantum cryptography to protect their data and assets. Being quantum safe is not something which should be optional. **The advancement in quantum computing is accelerating and the threat is real.**

The impact on data security



Data that remains sensitive across multiple years can be stolen now, to be decrypted once a cryptographically capable quantum computer exists. The day in which this occurs is defined as **"Q-Day"**. This is known as **"Harvest Now – Decrypt Later Threat"** and highlights the need for organisations to consider the quantum threats in their cyber and data governance assurance frameworks now.

National Institute of Standards and Technology (NIST) have been working for several years to define and standardise Post Quantum Cryptography (PQC) algorithms publishing Federal Information Processing Standard (FIPS) 203, FIPS 204 and FIPS 205 in late 2024 as the first industry recommended Post Quantum Secure algorithms. They continue to work on developing further Post Quantum Secure Algorithms.

Quantum regulatory timelines

Regulatory timelines

The National Cyber Security Centre (NCSC) recently published guidance on the timelines for migration to post quantum cryptography in the UK. Previously the National Security Agency (NSA) and NIST have defined migration timelines in the USA. Broadly, they are aligned with 2035 being the goal for all systems to be quantum resistant, however, critical applications and those impacting national security should be migrated to post quantum cryptography sooner.

By 2028
Complete discovery and assessment phase, create an initial migration plan and communicate needs to suppliers.

By 2031
Complete migration of the most critical assets, ready infrastructure to support a PQC future and redefine your plan for full migration by 2035.

By 2035
Complete migration to PQC for all systems, services and products.

2025

- Understand the implications of quantum computing
- Perform quantum readiness and risk assessments
- Engage with your third-party suppliers and vendors
- Develop a strategic quantum migration plan/roadmap

2028

- Pilot small-scale proofs of concept (e.g., crypto-agility)
- Implement high-priority migration activities
- Redefine your migration plan with a clear roadmap to 2035
- Evaluate quantum opportunities and their potential value to your organisation

2031

- Transition to a quantum-secure ecosystem
- Embrace fully agile cryptography management

2035

- Deploy quantum-based solutions where they offer added value in your organisation

What are the biggest risks?

Breaking encryption

Many encryption standards that have been around for several years are vulnerable to quantum advances. Most of these are commonly used in symmetric and asymmetric encryption techniques. These include: RSA, ECC, Digital Signature Algorithm (DSA) and more. Additionally, many cryptographic libraries are buried and can be hard to find, so it may be difficult to determine which encryption methods are actually being used.

Third-party risk

All software and outsourced functions and services will rely on the vendor to upgrade the cryptography, different vendors will move at different speeds and may not align with your risk appetite.

Regulatory risk

Currently the NCSC has provided the guidance in the UK. In the US, certain companies and industries have firm migration deadlines outlined by the NSA. The UK and other countries are likely to follow.

Upgrading cryptography is complex

There is a shortage of skilled resources who can upgrade systems to post quantum encryption which meets the NIST standards. There are some companies offering this as a service.

Can the system even support an upgrade?

NIST approved post quantum cryptography can be more resource intensive than the current encryption used. Some systems will not be able to handle the additional memory footprint and may have to be deprecated.

Clear planning and roadmap

The NCSC estimate it will take large organisations two-three years to prepare a detailed migration plan and defines the target date for this as 2028. Yet for many, this process has not started. Organisations need to adapt current security processes such as procurement, patching, data loss and asset management.

The relevance of the threat to your organisation

The responses to advancements in quantum computing are going to evolve over time. As the technology continues to advance the regulations, guidance and standards will also continue to develop further. As with any emerging technology, the environment can shift quickly and taking appropriate action early and regularly reviewing the net risk position is the best way for your organisation to be prepared for when this does occur.

Awareness

Is your organisation aware of Quantum and the threats it brings?

Inventory

Do you have an inventory of your assets, the data that they hold (including shelf life) and their current level of cryptography?

Third-party risk

Have you engaged with your vendors or stakeholders regarding post quantum plans?

Planning

Do you have a roadmap to migrate to post quantum cryptography?

Ongoing governance

Is quantum considered in your data governance and cyber security framework?

Quantum readiness assessment

What can we do?

Our value proposition is to build confidence in quantum readiness and assure preparedness for advances in quantum computing and related cyber risks. Protecting your assets against quantum threats requires an initial readiness assessment to evaluate risk exposure, define targeted mitigations and develop a roadmap to achieve crypto-agility.

The need for quantum readiness assessment

Internal Factors

Lack of visibility: Organisations are often unaware of the breadth and scope of cryptographic dependencies in secure network communications, data security and privacy.

Transition complexity: Many legacy systems lack the flexibility to swiftly adopt new cryptographic primitives and algorithms, causing widely used protocols to lag in adapting to the demands of the quantum era.

External Factors

New regulations: Regulations and Guidance (e.g., NCSC) will require organisations to adopt post-quantum cryptography solutions. Ongoing improvement is essential.

Emerging risk and standards: Key security standards emphasise the need to assess emerging cryptographic risks. Standards such as Payment Card Industry Data Security Standard (PCI-DSS) and FIPS either include – or are in the process of introducing – specific controls for managing cryptographic inventories.

Quantum readiness assessment

1 Identify exposure to quantum risk

Identify critical information technology and data assets and their exposure to risk based on susceptibility to quantum computing threats, information retention requirements, evolving regulatory landscape, etc.

2 GAP analysis

Inventory and gap analysis of cryptographic material for critical assets. Analysis of the resilience of algorithms and protocols in use in relation to advances in quantum computing, identification of safeguards at the operational context level and calculation of residual risk.

3 Define and prioritise initiatives

Evaluate the ecosystem of secure solutions and post-quantum cryptography, proposing remediation processes and technical implementations based on the risks identified, taking into account residual risk, third-party dependencies, technological solutions, complexity and maturity of solutions.

4 Map out the roadmap to crypto agility

Develop a roadmap to crypto-agility, including prioritising the implementation of future-proof solutions, as well as training, all aligned with industry best practices to prepare for an effective and secure transition.

Quantum readiness assurance

EY is supporting Risk Management and Assurance teams across the second and third lines of defence to navigate the quantum era by assessing alignment of enterprise risk appetite with the adoption of quantum-safe risk management processes and the planning for technical cryptographic implementations. Our team forms an initial view of your quantum readiness maturity and collaborates with key stakeholders to undertake assurance assessments, help integrate quantum into existing security improvement programs and produce prioritised tailored recommendations.

These are the key assurance activities to be considered at each stage of developing a post quantum cryptography roadmap. EY can help you to assure you quantum readiness.

Quantum readiness maturity

Basic

- Evaluate the adequacy of risk assessments to consider the impact of quantum computing on relevant business areas.
- Assess the effectiveness of processes for integrating quantum-related risks into the enterprise risk management or cyber framework and ensuring timely, comprehensive reporting to senior management.
- Assess whether third-party risks are identified, inventoried and assessed for pervasive quantum threats.
- Evaluate the process for regulatory horizon scanning and adoption of regulatory requirements into governance and planning.
- Assess mechanisms for training and awareness of quantum technology advancements.

Intermediate

- Review procedures performed to inventory IT infrastructure, data, network traffic communication flows, cryptographic algorithms and implementations (the process referred to as generation of the Cryptographic Bill of Materials). This should include a prioritisation over sensitive data.
- Review procedures used to identify the data shelf life and how current data breaches are handled.
- Assess process for identifying vulnerable cryptographic assets and mapping to impacted data and systems.
- Assess the effectiveness of PQC standards migration planning and implementation of NIST approved algorithms.
- Assess the controls in place to validate third-party PQC implementation and reliability.

Matured

- Assess the embeddedness of quantum-safe processes, tooling and PQC standards in comparison to the standards recommended by NIST and the NCSC.
- Review the measures applied to ensure compliance with evolving regulatory requirements and reporting of quantum risk mitigation.
- Assess the design of a clear roadmap for mitigating quantum risks, to address the Harvest-Now, Decrypt-Later (HNDL) threats and consideration of third-party and operational complexities.
- Evaluate sustainable strategic planning for PQC, crypto-agility, adoption of quantum-based technologies (e.g., QKD), human resource training efforts and alignment with ongoing quantum advancements.

Key contacts

Piers Clinton-Tarestad
Partner/Principal
Technology Risk
EY LLP

United Kingdom
pclintontarestad@uk.ey.com

Matt Dent
Senior Manager
Technology Risk
EY LLP

United Kingdom
matt.dent@uk.ey.com

Krati Laad
Partner/Principal
Risk Consulting
EY LLP

United Kingdom
krati.laad1@uk.ey.com

Steve Holt
Partner/Principal
Technology Risk
EY LLP

United Kingdom
sholt2@uk.ey.com

Narayan Sathia
Director
Technology Risk
EY LLP

United Kingdom
narayan.s@uk.ey.com

Adolf Mugandiwa
Manager
Technology Risk
EY LLP

United Kingdom
adolf.mugandiwa@uk.ey.com

Our presence in the global ecosystem

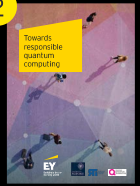
20+ Partnerships with the Global Quantum Ecosystem

IBM | Microsoft | SandboxAQ

1

Quantum Threat Whitepaper by EY and JPMC

2



EY and University of Oxford Quantum Ethics Whitepaper

3

EY Quantum Readiness Survey

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

EYSCORE 004282-25-UK.

UKC-038930.indd (UK) 05/25. Artwork by Creative UK.

ED None

ey.com/uk