QUANTUM
THINK TANK

Insight that protects. Foresight that leads

# Assessing Quantum Impact

By Tooba Qasim

January 2026

www.cyberlondon.com | Info@cyberlondon.com

## How Organisations Can Identify Their Vulnerabilities

Quantum computing has not yet reached the point where it can break classical encryption, but the clock is already ticking. The risk is not about the present moment; it is about the long-term exposure of systems, data and infrastructure that rely on cryptography that will eventually become fragile. Many organisations are beginning to hear about post-quantum cryptography (PQC), but few have taken the time to identify where quantum risks actually lie inside their own environments. Without this understanding, any transition effort becomes guesswork.

This is where a quantum impact assessment becomes essential. It is the process of identifying which systems, applications and data streams will be affected by the shift to PQC. Put simply, it helps organisations answer a crucial question: **where does quantum matter for us?** Every organisation has a different risk profile, a different technology stack, a different regulatory landscape, and a different tolerance for disruption. A proper impact assessment turns the broad, global "quantum threat" into a concrete, organisational action plan.

Before we break down how such an assessment works, it is useful to understand what "impact" means in this context. The impact is not only about whether a quantum computer can break encryption tomorrow. It is about the **operational**, **technical**, **financial**, and **strategic** consequences of using cryptographic systems that may become obsolete or breakable in the coming years. It is also about recognising the long-term importance of certain types of data that remain sensitive far beyond the moment they are generated.

## What Is a Quantum Impact Assessment?

A quantum impact assessment is a structured method for uncovering cryptographic dependencies and vulnerabilities across an organisation. It examines how cryptography is used, where it lives, what data it protects, and what risks emerge if that cryptography becomes compromised in a post-quantum world. While the term may sound technical, the concept is simple: understand what you have before planning how to secure it.

In many organisations today, cryptography is everywhere. It protects databases, mobile apps, identity systems, virtual private networks, cloud workloads, internal APIs, IoT devices, payment systems, and even firmware. In some cases, teams do not realise how deep cryptography runs in their environment, because it often sits quietly in the background, doing its job without drawing attention.

A quantum impact assessment brings these hidden elements to the surface. It shows which systems rely on RSA and elliptic curve cryptography (ECC), which systems rely on long-lived keys, which applications store high-value data, and which components may struggle to support larger PQC keys and certificates. More importantly, it identifies **priority areas** that must be addressed first in a PQC migration plan.

## Understanding Where PQC Matters: A Step-by-Step Approach

A strong impact assessment does not require perfection. It requires structure, clarity, and the willingness to trace cryptography through the places where it quietly operates. While every organisation is different, most assessments follow a set of common steps.

### 1. Build an Inventory of Cryptographic Assets

The very first step is building a complete and accurate inventory of all cryptographic assets used across the organisation. This is sometimes called “crypto discovery” or “crypto mapping.” The goal is to trace where cryptography is applied, how it is configured, and what technologies underpin it.

An inventory may include elements such as:

- encryption protocols used in servers and applications
- TLS configurations
- VPN tunnels
- certificates and certificate authorities
- public key infrastructures
- hardware security modules
- IoT device firmware
- cloud workloads and APIs
- databases and storage encryption

- digital signature schemes
- authentication mechanisms

In practice, this step can be eye-opening. Many organisations find cryptographic components they did not know existed, including legacy systems using outdated keys or embedded devices running old cryptographic libraries. Mapping these dependencies is fundamental to understanding where quantum vulnerabilities may appear.

**2. Identify Sensitive and High-Value Data**

Quantum impact is not equal across all data. Some information loses value quickly, while other data must remain secure for decades. A key part of the assessment involves identifying:

- confidential business information
- personal data and protected information
- intellectual property
- financial records
- medical or genomic data
- government or national security information
- strategic communications
- identity and authentication data

The sensitivity of data determines how urgently the system protecting it must transition to quantum-safe methods. For example, a marketing dashboard containing monthly sales figures is not as critical as encrypted customer identity records that must remain private for many years.

**3. Identify Systems That Rely on RSA and ECC**

RSA and ECC are the two pillars of classical public-key cryptography. Unfortunately, they are also the two families of algorithms most vulnerable to future quantum attacks. While these algorithms remain safe today, the long-term risk makes it necessary to identify every system that uses them.

Common places where RSA and ECC appear include:

- HTTPS and TLS certificates

- S/MIME email encryption
- SSH keys
- VPN authentication
- digital signatures for software and firmware
- secure boot processes
- mobile authentication flows
- cloud identity platforms
- Wi-Fi authentication
- blockchain and distributed ledger systems

In large enterprises, it is common to find thousands of RSA keys still active, some with expiration dates stretching far into the future. These are precisely the systems that will require quantum-safe alternatives, hybrid modes, or accelerated upgrades.

**4. Highlight "Data with Long-Term Confidentiality" Requirements**

This category is one of the most critical and often overlooked. Some data must remain confidential for years, decades, or even a lifetime. When attackers harvest encrypted data today with the intention of decrypting it in the future using quantum capabilities, this category becomes extremely vulnerable.

Examples include:

- health and genetic data (lifelong relevance)
- national security information (decades of relevance)
- intellectual property (patents, formulas, engineering designs)
- financial histories
- industrial telemetry
- legal contracts
- identity credentials
- trade secrets

If an organisation relies on RSA or ECC to protect these types of long-term information, the risk is immediate. It means the clock has already started, because attackers can harvest that data today and wait for the tools of tomorrow.

**5. Assess Third-Party and Vendor Dependencies**

No organisation operates alone. Nearly all modern environments depend on vendors, partners, cloud providers, managed service firms, and software suppliers. A quantum impact assessment must evaluate:

- which vendors handle critical data
- which vendors manage encryption or authentication
- which cloud services rely on RSA or ECC
- which third-party APIs transmit sensitive data
- whether vendors have PQC roadmaps or support hybrid modes

Vendor readiness will become one of the biggest dependencies in PQC migration. An organisation may be prepared internally, but if its identity provider, firewall vendor, or payment gateway is not ready, it becomes a bottleneck.

Evaluating vendor maturity is therefore essential. This includes asking suppliers for PQC roadmaps, timelines, and compliance strategies.

**6. Determine Priority Migration Areas**

Not every system needs immediate replacement. A strong impact assessment concludes by identifying which systems must transition first. Priority is usually determined by combining three factors:

1. Sensitivity of the data involved
2. Use of quantum-vulnerable algorithms like RSA or ECC
3. Operational importance of the system

For example:

- A public-facing login system using ECC to verify user identities may be a top priority.
- An internal development server storing non-sensitive data may be a lower priority.
- A database containing customer SSNs may require urgent hybrid protection.

- A supply chain interface managed by a third-party vendor may require contractual updates.

A quantum-safe transformation becomes manageable only when these priorities are understood and documented.

**A Short, Practical Checklist**

This checklist summarises the essential elements of a quantum impact assessment:

- Have you mapped all cryptographic assets across your systems?
- Do you know which algorithms (RSA, ECC, AES, SHA) each system uses?
- Have you identified the most sensitive and long-lived data?
- Do you know where RSA and ECC are used for encryption, signatures, or key exchange?
- Have you located systems that cannot easily support larger PQC keys or certificates?
- Have you evaluated third-party vendors for PQC readiness?
- Have you identified your high-priority migration targets?

Even a simple version of this checklist can dramatically improve clarity and readiness.

## The Road Ahead

A quantum impact assessment is more than an inventory exercise. It is the first real step toward quantum-safe readiness. It helps organisations build a clear understanding of where cryptography lives, how critical it is, what risks quantum technology introduces, and where to focus initial efforts. By assessing data sensitivity, system importance, vendor dependencies, and algorithmic vulnerabilities, organisations can create an actionable roadmap for PQC migration.

In our view, the organisations that take this step early will be significantly ahead of the curve. Quantum migration is not a last-minute activity. It requires planning, coordination, technical adaptation, and strategic alignment with vendors and regulators. Impact assessments reveal where that journey begins and where it must gain momentum. As the global movement towards quantum-safe standards accelerates, the organisations with a clear understanding of their vulnerabilities will be the ones that transition smoothly, efficiently, and confidently.

---

*About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security*

*protocols and exploring*