Quantum Security Demands Action

...Years Before the Threat Materialises

Most organisations assume quantum computing is a problem for the future - but it's not! Nation-state adversaries are already harvesting encrypted data today, storing it until quantum computers are powerful enough to break current encryption. Sensitive commercial data, intellectual property, financial records, and personal information could be sitting on a hostile server right now. The breach happens now and the disclosure comes later.

The NCSC (National Cyber Security Centre) requires quantum-safe critical infrastructure by 2035, with discovery and migration plans due by 2028 and high-priority systems upgraded by 2031. That first checkpoint is 18 months away. A quantum-safe readiness assessment fixes this fast: full discovery and a prioritised, actionable roadmap within weeks, freeing time for procurement and migration, the parts that actually take years.

2035 is the deadline. 2026 is when readiness begins.

What is the Quantum Safe Assessment?

Gives your organisation the visibility it needs to understand its cryptographic exposure and begin the migration journey while there's still time.

A workshop and scan, run by Celerity with IBM Quantum Safe Explorer and IBM Guardium Cryptography Manager, taking you from cryptographic uncertainty to a board-ready roadmap.

Follows a proven **4-stage methodology** tailored to your sector, scale, and regulatory context.

There is a 1 in 3 chance quantum will break current encryption within a decade. The organisations that act now will be the ones that are ready.

Source: Global Risk Institute Quantum Threat Timeline Report, via SecurityWeek 2025

The Cost of Inaction

Data Already At Risk

Encrypted data with a sensitivity lifetime of 20 years or more is already exposed. Every day without a cryptographic inventory is a day adversaries can add to their stockpile.

A Closing Migration Window

The 2035 NCSC deadline sounds distant. It is not. With discovery, procurement, and migration each taking years, organisations that have not started are already behind.

Invisible Exposure

Most organisations have no idea what encryption they are running or where. You cannot migrate what you cannot see, and what you cannot see cannot be secured.

The Assessment: A Structured 4-Step Approach

	Step	What Happens
1	**Executive Briefing & Workshop**	We brief leadership and discuss quantum risk specific to your sector, the NCSC mandate, and framework considerations with your leadership and technical stakeholders.
2	**Scope & Cryptographic Discovery**	We scope and scan the agreed applications and infrastructure using IBM Quantum Safe Explorer, building a Cryptographic Bill of Materials (CBOM) for the scanned area of the network.
3	**Risk & Prioritisation Analysis**	We identify vulnerable algorithms and prioritise findings using what we learned in the workshop, data sensitivity, system criticality, and regulatory exposure. IBM Guardium Cryptography Manager manages the cryptographic assets once discovered.
4	**Reporting & Roadmap**	We deliver two reports, an Executive Summary and a Technical Report, including a prioritised remediation plan and implementation pathway for post quantum migration.

Your Deliverables

Executive Summary

- How we assessed your estate, what was scanned and how, in plain terms
- What the assessment found, headline Quantum Score and overall exposure rating
- Where the risk is concentrated, critical/major/minor findings, summarised
- Where you stand against the rules, CAF-aligned DSPT and regulatory mapping
- What to do first, and when, prioritised roadmap through to 2035

Technical Report

- What was scanned, and how findings are scored- full methodology
- What the scan found, complete cryptographic inventory (CBOM)
- Findings by object type, certificates, keys, and IT assets in detail
- How to remediate each platform- asset-specific, hostname-level steps
- How to close each finding- remediation guidance by category
- Appendices- full certificate, key, and IT asset inventories

Book Your Quantum Safe Assessment Today!

Contact **marketing@celerity-uk.com** to discuss your requirements and schedule a tailored workshop. You'll receive an Executive Summary and Technical Report covering your cryptographic inventory, prioritised risk register, and a costed post-quantum migration roadmap.

@CelerityLimited
marketing@celerity-uk.com
www.celerity-uk.com

IBM Platinum Partner

Copyright Celerity Limited 2026.
IBM & the IBM Partner logo are trademarks or registered trademarks of their respective owners in the United States and/or other countries. Use of the IBM Business Partner logo does not imply endorsement by IBM. References to IBM products are for informational purposes only.