Quantum Security Demands Action

...Years Before the Threat Materialises

Most organisations assume quantum computing is a problem for the future. It is 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 requires all organisations operating critical infrastructure or handling sensitive data to be quantum-safe by 2035. Working backwards, cryptographic migration takes five or more years, procurement two to three years, and discovery alone takes 18 to 24 months.

What is the Quantum Safe Assessment?

Give your organisation the visibility it needs to understand its cryptographic exposure and begin the migration journey while there is still time to complete it.

A structured, IBM-led workshop delivered by Celerity experts will take your organisation from cryptographic uncertainty to a board-ready roadmap.

The assessment follows a proven **five-step 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 Five-Step Approach

	Step	What Happens
1	**Executive Briefing**	Align leadership on quantum risk, the NCSC 2035 mandate, and what your organisation needs to do and by when.
2	**Cryptographic Discovery**	Scan applications and infrastructure using IBM Quantum Safe Explorer to build a complete Cryptographic Bill of Materials (CBOM).
3	**Risk & Gap Analysis**	Identify vulnerable algorithms and prioritise findings by data sensitivity, system criticality, and regulatory exposure.
4	**Target Architecture**	Design a PQC-ready future state aligned to NCSC guidance and your organisation's technology strategy.
5	**Roadmap & Next Steps**	Deliver a costed, prioritised remediation plan with a clear implementation pathway for post-quantum migration.

Your Deliverables

Complete Cryptographic Inventory
Every cryptographic asset across your estate mapped and documented, cloud, hybrid, and on-premises, many for the first time.

A Prioritised Risk Register
Vulnerable algorithms ranked by data sensitivity, system criticality, and regulatory exposure so you know exactly where to focus first.

A PQC-Ready Target Architecture
A future-state design aligned to NCSC guidance and your technology strategy, ready to hand to your delivery teams.

A Costed Remediation Roadmap
A phased, fully costed migration plan with a clear implementation pathway your board can approve and your teams can execute.

Clarity on Your Compliance Position
A plain view of where you stand against NCSC timelines, cyber insurance requirements, and relevant regulatory obligations.

An Executive Summary Ready for Sign-Off
Everything leadership needs to make informed decisions, presented in language that works in a boardroom, not just a security team.

Book Your Quantum Safe Assessment

Contact **marketing@celerity-uk.com** to discuss your requirements and schedule a tailored workshop. You'll receive a comprehensive CBOM report, prioritised risk register, and practical PQC migration roadmap to support your organisation's quantum-safe journey.

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

IBM Platinum Partner