

Post-Quantum Cryptography (PQC)



PQC Essentials - a standardised route to quantum readiness

Quantum risk is a business continuity issue today.

Long-life sensitive data may already be exposed to harvest-now-decrypt-later (HNDL) attacks. Organisations need to understand where vulnerable cryptography is used, which trust paths matter most, and how to sequence a practical transition.

How CGI can help

As one of the first NCSC assured Cyber Security consultancies for PQC Discovery and Migration Planning, CGI provides a trusted, standardised route through four connected stages, moving organisations from shared understanding to evidence-based priorities and an actionable transition plan.

01

Establish the context and business case

Align leaders and stakeholders on quantum risk, HNDL exposure, business impact and the case for action.

02

Discover and assess

Examine where vulnerable cryptography and trust dependencies exist across applications, cloud environments, Application Programming Interfaces (APIs), Public Key Infrastructure (PKI), Key Management Systems (KMS) and third parties.

03

Evaluate readiness

Test crypto-agility and crypto control-plane readiness across technology, identities, certificates, key wrapping, Bring Your Own Key (BYOK), backup and recovery.

04

Plan the transition

Sequence change against business risk, regulatory pressure, vendor readiness, operational complexity and continuity needs.

What PQC Essentials delivers

Each stage produces a defined decision-making artifact, giving leaders a clear evidence base for investment, sequencing and implementation.

Output	What it provides
Executive risk and investment case	Agreed scope, business impact, governance, investment rationale and priorities.
Cryptographic dependency inventory	A consolidated Cryptographic Bill of Materials (CBOM) covering algorithms, keys, certificates and dependencies across applications, networks, infrastructure, cloud, IT, OT and third parties.
Quantum risk heatmap and priority register	Ranked exposure based on data sensitivity, HNDL risk, criticality and remediation complexity.
Crypto-agility and readiness assessment	Gaps affecting transition across technology, identity, PKI, key management, cloud controls, recovery and suppliers.
Phased migration roadmap and action backlog	A sequenced plan of priorities, dependencies, decisions, vendor actions and transition risks.

Beyond PQC Essentials

CGI can support implementation, helping organisations turn the roadmap into controlled change. This can include:

- PQC pilots and proofs of concept, including hybrid TLS approaches.
- PKI transition and certificate lifecycle changes.
- KMS and HSM integration, key-wrapping changes and cloud key-management patterns.
- Vendor engagement, dependency management, governance and assurance.

The value of PQC Essentials

The value is not simply identifying cryptography. PQC Essentials provides a consistent way to determine which data, keys and trust paths create the greatest future exposure - and what should be addressed first.

Your organisation, quantum-ready, with CGI

CGI combines NCSC-assured PQC discovery and migration-planning capability with cryptographic expertise, operational understanding and regulatory alignment to help organisations prepare for the post-quantum era with practical, actionable outcomes



About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit : cgi.com/uk/cyber-security

Email : cyber.enquiry.uk@cgi.com