northdoor
Store IT · Protect IT · Use IT

Quantum Safe readiness

From “we know quantum is a risk” to a costed, prioritised migration plan, with Northdoor and IBM

- **Discover and inventory:** find every algorithm, key and certificate in use, and produce a Cryptography Bill of Materials.
- **Assess and comply:** score quantum risk against policy and regulation, and build a prioritised risk register and roadmap.
- **Manage lifecycle:** centralise and automate keys and certificates, so a later change of algorithm is fast rather than painful.
- **Protect and adapt:** test and deploy post-quantum and hybrid cryptography, starting with the most sensitive long-life data.

“Quantum-safe migration is a multi-year programme, not a patch, and the organisations that start with visibility of their cryptography will be the ones able to move at a sensible, affordable pace.”

Summary

Northdoor can take a client from “we know quantum is a risk” to a costed, prioritised migration plan by working through IBM’s four-step Quantum Safe programme: Discover and inventory, Assess and comply, Manage lifecycle, and Protect and adapt.

This note explains why the subject now belongs on the board agenda, what each of the four steps involves, which IBM technology supports it, and where Northdoor adds value.

Quantum-safe migration is a multi-year programme, not a patch, and the organisations that start with visibility of their cryptography will be the ones able to move at a sensible, affordable pace.

Why act now

The risk is present today, even though a cryptographically relevant quantum computer is not. Three factors make the case for starting now.

- **Harvest now, decrypt later.** Adversaries can capture encrypted data today and hold it until it can be decrypted. Any data that must stay confidential for 10 to 25 years, such as customer records, intellectual property or long-term contracts, is already exposed.
- **The standards are set.** NIST published its first post-quantum standards in August 2024: FIPS 203 (ML-KEM, derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, derived from CRYSTALS-Dilithium) and FIPS 205 (SLH-DSA). IBM researchers co-developed three of the four algorithms NIST originally selected, which gives IBM’s tooling particular credibility.
- **The timeline is long.** IBM Institute for Business Value research puts the average full migration at around 12 years, because cryptography is embedded in applications, networks, APIs, infrastructure and the supply chain.

For UK organisations, the NCSC set out indicative migration milestones in March 2025:

By	Milestone
2028	Define migration goals, complete discovery and build an initial plan
2031	Complete the highest-priority migrations and refine the plan
2035	Complete migration to post-quantum cryptography

Read alongside DORA for financial services and the forthcoming Cyber Security and Resilience Bill, this means boards will increasingly be asked to evidence a plan. IBM’s research also found that “Quantum-Safe Champions” report overall resilience nearly three times greater than the least-ready organisations, so the work pays a security dividend well before quantum arrives.

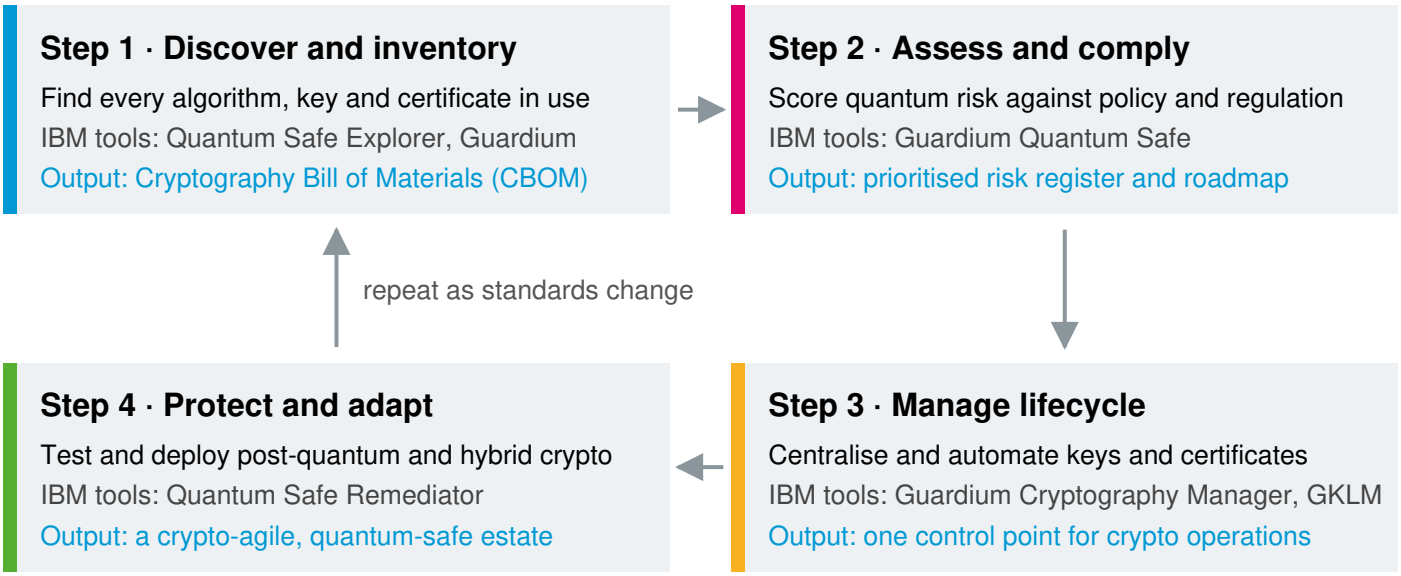
“Quantum-Safe Champions” report overall resilience nearly three times greater than the least-ready organisations

IBM Institute for Business Value

IBM's four-step Quantum Safe programme

IBM's Guardium quantum-safe portfolio frames readiness as four steps towards crypto-agility, each backed by specific IBM software.

Quantum-safe readiness is a repeating four-step cycle



IBM Quantum Safe programme · 4 steps in a continuous cycle

The steps run in order the first time, then repeat: new applications, suppliers and standards mean the inventory and risk picture must be refreshed continuously.

Clients may have seen IBM's earlier three-part model of Discover, Observe and Transform. The four steps refine it: Discover and Assess correspond to Discover and Observe, while Transform is split into Manage lifecycle and Protect and adapt, recognising that governing keys and certificates is a discipline in its own right.

Step 1: Discover and inventory

The first step gives the client a complete, evidence-based picture of where cryptography is used, because an organisation cannot protect what it cannot see.

What happens. IBM Quantum Safe Explorer scans application source and binaries, including home-grown code, and can sit in CI/CD pipelines so new code is checked as it is written. Guardium Cryptography Manager discovers cryptographic objects and IT assets across the estate, detects unknown or "shadow" cryptography, and maps dependencies, ownership and usage. Together they produce a Cryptography Bill of Materials (CBOM): every algorithm, key, certificate and library, and where it sits.

How Northdoor helps.

- Scope the discovery with the client, agreeing which business services, applications and platforms come first, so the exercise is manageable rather than exhaustive on day one.
- Deploy and configure the IBM tooling, and run the scans alongside the client's own teams.
- Include the platforms that generic scanners often miss, drawing on Northdoor's IBM Power, storage and hybrid cloud experience.
- Link cryptographic findings to the data they protect, using Northdoor's data discovery and classification capability, so each finding carries a business context.

Client outcome. A baselined CBOM and a clear view of exposure, which is the discovery milestone the NCSC expects organisations to reach by 2028.

Step 2: Assess and comply

The second step turns the inventory into a prioritised list of risks, so that effort and budget go where the business impact is greatest.

What happens. Guardium Quantum Safe, part of IBM Guardium Data Security Center, provides a continuous view of cryptographic posture. It flags outdated or quantum-vulnerable algorithms, checks usage against regulatory and internal policies, prioritises violations for remediation, and can raise tickets directly in ServiceNow or Jira. It also produces audit-ready reports for risk committees and regulators.

How Northdoor helps.

- Run a risk workshop with security, risk and business owners to weigh each exposure by the sensitivity and shelf life of the data it protects, the core test for harvest-now-decrypt-later risk.
- Translate the client's obligations, for example DORA, NIS2, UK GDPR and sector guidance, into policies the tooling can enforce and report against.
- Assess supply-chain exposure through Northdoor's third-party risk management service, and help the client ask key vendors for their own quantum-safe roadmaps.
- Produce a board-level readout that positions quantum safety as a business continuity and competitiveness issue, not an IT housekeeping task.

Client outcome. A prioritised risk register, a policy baseline and an initial migration roadmap that the board can approve and fund.

Step 3: Manage lifecycle

The third step puts keys and certificates under central, automated control, which is the foundation that makes a later change of algorithm fast rather than painful.

What happens. Guardium Cryptography Manager centralises lifecycle operations in a single tool, automating key generation and certificate renewal and enforcing consistent policies across the organisation. IBM Guardium Key Lifecycle Manager (GKLM) adds centralised key management for IBM and non-IBM storage, cloud storage and applications.

How Northdoor helps.

- Design the target operating model: who owns cryptographic policy, who approves change, and how exceptions are handled.
- Integrate lifecycle management with existing PKI, HSMs, storage and cloud key services, reusing what the client already owns wherever possible.
- Implement GKLM for storage encryption, an area where Northdoor's IBM Storage and Power expertise is directly relevant.
- Offer ongoing operation of the platform through Northdoor's managed security services, for clients who prefer not to build this skill in-house.

Client outcome. Fewer certificate-related outages, a single point of control over cryptography, and the operational readiness to swap algorithms when required.

Step 4: Protect and adapt

The fourth step is where vulnerable cryptography is actually replaced or shielded, starting with the highest-priority systems from Step 2.

What happens. IBM Quantum Safe Remediator enables hybrid classical and post-quantum environments, tests remediation patterns while measuring algorithm performance in real-world conditions, and defends against harvest-now-decrypt-later attacks through infrastructure integration. For some traffic it can apply protection via an adaptive proxy without code changes, which buys time for systems that are hard to modify. Guardium Cryptography Manager adds encryption of sensitive data and an assessment of which post-quantum algorithms are efficient and feasible for each use case.

How Northdoor helps.

- Select the right remediation pattern for each system: proxy protection, hybrid cryptography, library upgrade or re-engineering. Straight replacement is rarely the most efficient route.
- Pilot on a contained, high-value service to prove performance and compatibility before wider rollout.

- Build crypto-agility into the architecture, so future changes of algorithm do not require wholesale re-engineering.
- Feed each change back into the inventory and risk view, closing the loop to Step 1.

Client outcome. The most sensitive long-life data protected first, measurable progress against the NCSC's 2031 priority milestone, and an estate that can adapt to future standards.

How we work with you

Northdoor would typically engage in three phases, with the first phase a self-contained readiness assessment that gives the client value even if they pause there.

Phase	Steps covered	Key deliverables
1. Quantum Safe Readiness Assessment	Discover and inventory; Assess and comply	Scoped CBOM, prioritised risk register, policy baseline, board readout and initial roadmap
2. Remediation programme	Manage lifecycle; Protect and adapt	Lifecycle platform live, pilot remediation proven, rollout plan by priority tier
3. Managed crypto-agility	All four, continuously	Ongoing scanning, posture reporting, certificate and key operations, annual roadmap refresh

Why Northdoor. Northdoor is an IBM Gold Business Partner with three decades of experience helping organisations govern and protect their data. We combine hands-on delivery of the IBM Guardium and Quantum Safe portfolio with deep knowledge of the IBM Power, storage and hybrid cloud platforms on which much critical data still runs. Our data governance, compliance and managed security services mean the quantum-safe programme connects to the client's wider risk agenda rather than sitting in isolation.

Recommended next steps

1. Hold a 90-minute executive briefing with the client's CISO and risk leadership to agree the business case and sponsor.
2. Agree the scope of the Readiness Assessment: priority business services, platforms and data sets.
3. Confirm access to code repositories, infrastructure and key stakeholders for the discovery scans.
4. Book a board readout date at the end of Phase 1, so the roadmap is approved and funded while momentum is high.