

Managing the Quantum Threat Horizon

A Management Perspective on a Technological Problem and an Early Roadmap for GRC Professionals

September 2026

A Management Perspective on a Technological Problem and an Early Roadmap for GRC Professionals

Through its processing power, the development of quantum computing could make almost all current encryption algorithms vulnerable

A look at the situation as we can understand it today:

- Where do we stand?
- What are the threats — and what roadmap for GRC professionals?
- How do the certainties, uncertainties and near-certainties break down?

The Certainties

Technological

- Quantum computing is under active development; AI is accelerating the research.
- Use cases affecting current cryptographic methods are established
- Post-quantum cryptography standards are finalised; hybrid PQC is already in production at scale: Migration to resistant products is a live option today.
- We are heading towards a 'Q-Day', when the first tangible case of compromise of current algorithms will come to light

Regulatory

The situation highlights three long-established families of good practice, reflected in all data-security regulations:

- Protecting sensitive data through encryption
- Keeping encryption methods at the state of the art as technology evolves
- Maintaining some form of monitoring of emerging threats that could affect sensitive data

This is now a named regulatory topic: NCSC UK (2028/2031/2035), NSA CNSA 2.0 (2027), the G7 Cyber Expert Group roadmap (Jan 2026) and the EU/ENISA roadmap all point the same way. It must sit on the GRC agenda.

The issue is being masked by the monumental background noise around AI

The Uncertainties

- No firmly fixed horizon for Q-Day — but the target dates around it are not vague: NIST deprecates RSA-2048/ECC by 2030 and disallows them by 2035; NCSC's full-migration target is 2035. Technical estimates for a cryptographically relevant quantum computer cluster between 2030 and the mid-2040s.
- No fully structured threat profile yet beyond the two classes on the next slide; exactly how pre-quantum processes will be affected is not yet tangibly clear.
- The first threats are most likely to be linked to nation states or state-sponsored actors, given the expected technological complexity
- Intelligence appears to indicate that HNDL collection is under way, but at what scale — and whom should we believe in the current geopolitical context?

How will AI have changed our environments and practices by Q-Day?

Two Threats, Not One

The debate is fixated on confidentiality (HNDL) but a second, independent threat (TNFL) targets integrity and authentication — and needs its own remediation track.

HNDL

Harvest Now, Decrypt Later

Adversaries capture encrypted traffic today and store it, to decrypt once a quantum computer exists. A confidentiality risk that is already live.

Hits: long-lived sensitive & personal data. Owner lens: data governance + DPO.

TNFL

Trust Now, Forge Later

Once a quantum computer can break signatures, an attacker can forge code-signing certs, PKI/X.509 chains and auth tokens — no harvested data required.

Hits: code signing, roots of trust, secure boot. Owner lens: PKI + architecture.

HNDL threatens what you stored / **TNFL** threatens what you sign and trust

The Regulatory Base is Converging

Five bodies, one broadly aligned picture: a c. 2028–2035 window, inventory-first, hybrid-by-default. No single jurisdiction has to carry the argument alone.

Body	Key milestones / contribution
NCSC (UK)	Three-phase roadmap: discovery/plan by 2028, priority migration by 2031, full migration by 2035
NIST / NSA (US)	FIPS 203/204/205 finalised (2024); RSA/ECC deprecated by 2030, disallowed 2035; CNSA 2.0 mandates PQC on new NSS from 2027
G7 Cyber Expert Group	Jan 2026 financial-sector roadmap; 2035 target, 2030–2032 for critical systems; co-chaired by the Bank of England
ETSI	TR 103 619 — reusable inventory → plan → execute migration framework and assessment questionnaire
ENISA / EU Commission	Coordinated Implementation Roadmap: national plans 2026, high-risk use cases 2030, full transition 2035; hybrid schemes emphasised

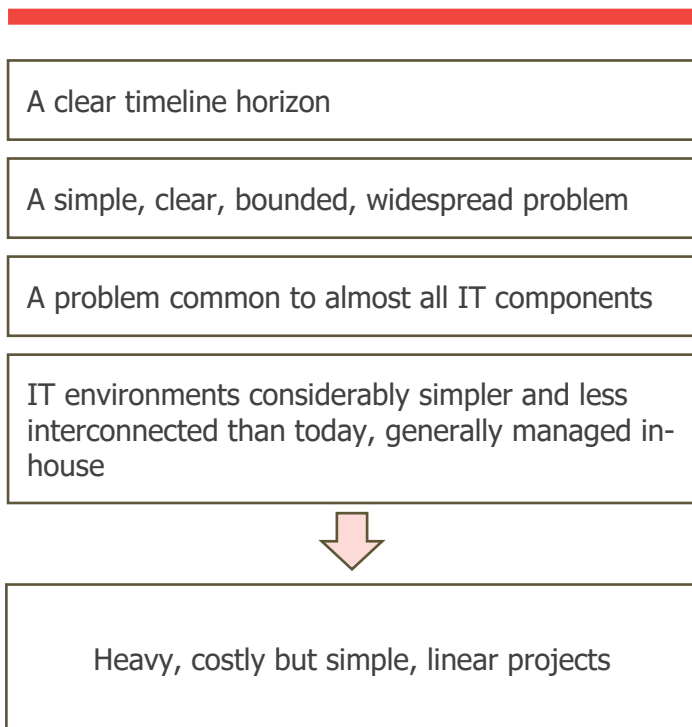
The mandates now exist and agree. The open question is execution — and time.

The Near-Certainties

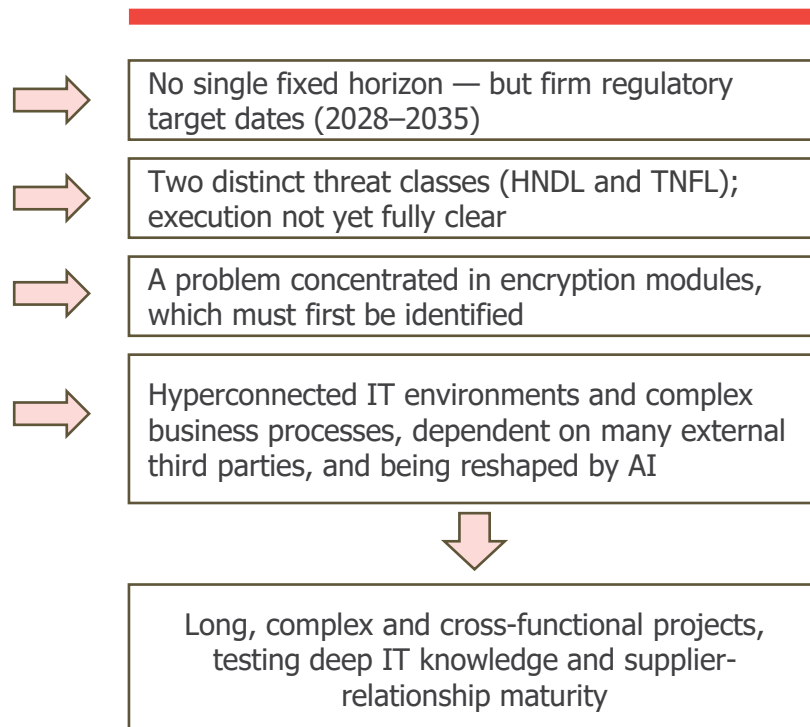
- Mobilising executive committees and other leaders, who are fixated on AI, around a complex topic with poorly defined timelines and stakes will not be easy
- We are heading not only towards Q-Day but also towards a Y2K-style 'panic' movement; but beware of simplistic parallels: the PQC challenges are considerably more complex than those of Y2K (next slide)
- It remains the role of GRC stakeholders to push — perhaps even champion — the topic , and to anchor it to the external timelines that already exist rather than waiting for absolute certainty.

Revisiting the Y2K parallel

Y2K



PQC



How to act today?

1- Take the issue seriously now, without waiting for absolute certainty

- Raise the topic on the GRC agenda (if it is not already there)
- Treat it as a regulatory topic in its own right — it is (NCSC, CNSA 2.0, G7, EU/ENISA).
- Put Governance first: Who owns it? At what level? Who will assess the enterprise's level of exposure?
- Start prioritising now, without waiting for the inevitable panic movement hijacks all other priorities and resources
- Map internal milestones to the published timelines: Discovery/plan by 2028, priority migration by 2031, full migration by 2035.
- Act with particular urgency for critical infrastructure and any organisation processing large volumes of long-lived sensitive data (HNDL) or relying heavily on digital signatures and PKI (TNFL).
- Prepare the enterprise for a potentially long and complex compliance effort

How to act today?

2- An inventory of the enterprise's cryptographic tools/assets is essential

- To assess the level of exposure, feasibility and cost of achieving post-quantum compliance (and manage the end-of-life or unsupported platforms where it will not be possible)
- This is where to start — and it need not start from a blank page: ETSI TR 103 619 and the CISA/NSA/NIST playbook provide a ready methodology.

BUT

- Such an inventory is unlikely to already exist, so resources must be allocated for it to be built
- In a context where the necessary knowledge is likely to be dispersed across development, infrastructure and security teams and their suppliers
- And where the priorities of all those teams are currently focused almost entirely on AI and its challenges
- Hence the importance of a clear, robust governance, ownership and sponsorship framework established from the outset (see point 1)
- Avoiding an endless debate around prioritisation and resourcing is the clearest pitfall to avoid today; this is a clear leadership matter

How to act today?

3- Three relative 'quick wins' that internal governance bodies can validate now

- Mandate hybrid resistant encryption for all new and in-flight projects where possible — e.g. X25519 + ML-KEM for new TLS/VPN, and ML-DSA (or SLH-DSA for high assurance) for new code-signing and PKI. Proven, not experimental.
- Add a section on suppliers' post-quantum approach and maturity to assessment questionnaires and periodic reassessments.
- Embed 'crypto-agility' — the ability to swap algorithms without re-architecting — as a design principle in architecture standards and vendor contracts now, ahead of the full inventory.

Extend, Don't Duplicate

Existing function	Where PQC intersects it	Action
ISMS / cryptographic policy (CISO)	An update to a control that already exists — ISO 27001:2022 Annex A 8.24	Amend the approved-algorithm list; add PQC + RSA/ECC deprecation dates
Data classification & retention	HNDL exposure = sensitivity × retention, already tracked	Feed existing registers into inventory prioritisation
Data protection / DPO	HNDL is largely a personal-data risk, not only IT security	Name the DPO a formal PQC stakeholder from the outset
Third-party / supplier risk	Supplier PQC maturity extends an existing workflow	Add PQC questions to the existing TPRM cycle
Enterprise / security architecture	Crypto-agility (and Trust Now, Forge Later) is an architecture principle	Mandate hybrid + agile patterns at design review
Enterprise risk / board committee	Quantum exposure is one line in the existing register	Score it with the existing methodology and cadence

PQC is not a new discipline competing on a crowded agenda — it should extend structures that already exist, each with an owner, a policy and an audit trail.



Contact us

Corix Partners Limited

contact@corixpartners.com

<https://corixpartners.com>

Smart Cyber Group

<https://smartcyber-group.com>