Governance and Risk Management

By Tooba Qasim

Making Quantum Risk a Board-Level Conversation

For many organisations, post-quantum cryptography still sounds like something that belongs deep inside IT or security teams. It is often framed as a future technical upgrade, something engineers will "deal with later" once standards mature or tools become easier to deploy.

That framing is increasingly inaccurate.

Quantum risk is not just a cryptographic issue. It is a **strategic risk**, one that affects data longevity, regulatory exposure, operational resilience and organisational trust. And like other strategic risks, cyber resilience, supply-chain dependency, or regulatory compliance, it ultimately sits at the **governance level**, not just the technical one.

Why quantum risk belongs at the board table

Boards and executive teams are used to dealing with risks that evolve slowly but have long-term consequences. Climate risk, for example, or pension liabilities. Quantum risk fits into that same category.

The core challenge is timing. Cryptographically relevant quantum computers may not exist today but decisions made **now** determine whether an organisation will be exposed **later**. Data collected, encrypted and stored today may need to remain confidential for 10, 20, or even 30 years. If that data becomes readable in the future, the damage cannot be undone retroactively.

From a governance perspective, this raises familiar questions:

- Are we adequately protecting long-lived sensitive data?
- Are we exposed to future regulatory or legal consequences?
- Do we understand our dependency on cryptographic systems we do not fully control?
- Are we planning for change or assuming stability?

These are not engineering questions. They are **risk appetite and accountability questions**, the kind boards already deal with in other domains.

Ownership: Who is actually responsible for quantum risk?

One of the most common governance gaps around PQC is unclear ownership.

Quantum risk does not sit neatly in one function. It touches security architecture, IT operations, compliance, procurement, legal and even product strategy. When responsibility is diffuse, action tends to stall.

In mature organisations, quantum risk should be **explicitly owned**, even if execution is delegated. That ownership typically sits with:

- The CISO or Head of Security as the operational risk owner
- The CIO or CTO as the transformation owner
- And executive leadership or the board as the accountability layer.

The key is not creating a new silo but ensuring that **quantum risk is named**, tracked and reported in the same way as other material cyber risks. If a risk is not owned, it is rarely managed.

Treating PQC as part of enterprise risk, not a special case

One mistake organisations often make is treating post-quantum cryptography as something entirely new and separate from existing risk frameworks. In reality, PQC fits naturally into structures that already exist.

Most organisations already operate with some form of enterprise risk management framework whether aligned to ISO 27001, NIST CSF, COSO, or internal governance models. PQC does not need a new framework. It needs to be **mapped into existing ones**.

For example, quantum risk can be expressed as:

- a **confidentiality risk** related to long-term data protection,
- a **technology obsolescence risk** tied to cryptographic algorithms,
- a **third-party risk** where vendors control key systems,
- a **compliance risk** as regulators begin to set expectations,

- and a **strategic risk** linked to digital trust and resilience.

Once framed this way, PQC stops being abstract. It becomes something that can be assessed, prioritized and reviewed alongside other cyber and operational risks.

From technical debt to cryptographic debt

Another useful governance lens is the idea of **cryptographic debt**.

Just as technical debt accumulates when systems are built without planning for change, cryptographic debt builds up when encryption is deployed without visibility, agility, or lifecycle management. Hard-coded algorithms, undocumented certificates, legacy protocols and opaque vendor dependencies all increase future migration cost and risk.

Boards do not need to understand cryptography to understand debt. What matters is recognising that **the longer migration is delayed, the harder and more expensive it becomes**. Governance conversations should focus less on "which algorithm" and more on "how exposed are we to change?"

Reporting and oversight: what good governance looks like

Good governance does not mean constant board-level technical briefings. It means structured oversight.

At a practical level, this might include:

- regular reporting on cryptographic dependencies and migration readiness,
- clear milestones aligned to national or regulatory timelines,
- risk indicators related to long-lived data and legacy systems,
- and explicit inclusion of PQC considerations in procurement and architecture decisions.

When PQC appears in risk registers, audit discussions and strategic roadmaps, it becomes part of normal organisational decision-making not an emergency response.

A shift in mindset, not just controls

Perhaps the most important governance change is cultural. Quantum risk challenges a long-standing assumption in cybersecurity: that encryption, once deployed can be trusted indefinitely.

Post-quantum planning forces organisations to accept that **cryptography has a lifecycle** and that long-term security depends on the ability to adapt. That mindset shift from static protection to managed evolution is ultimately a leadership responsibility.

Looking ahead

Post-quantum cryptography will be implemented by engineers, tested by architects and deployed by operations teams. But whether an organisation succeeds in that transition depends largely on governance.

When quantum risk is recognised as a board-level issue, assigned clear ownership and integrated into enterprise risk frameworks, preparation becomes proactive rather than reactive. That is the difference between reacting to disruption and managing it.

In the preparation phase, governance is not about making technical decisions. It is about ensuring the organisation is **ready to make them well at the right time and with clear accountability**.