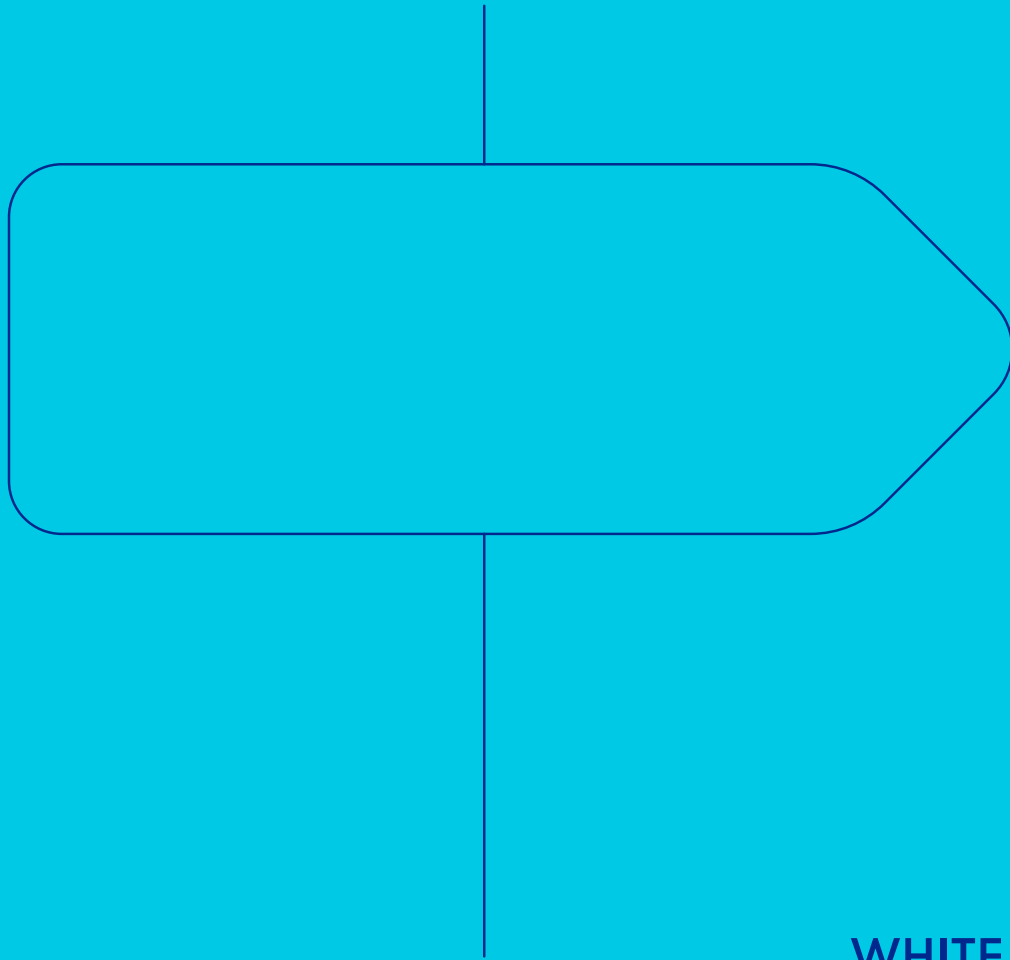




WHITE PAPER

MANAGING THE PQC TRANSITION

Governance, Planning and Investment

About

This document is Volume 2 of a three-volume guide on preparing for the quantum era and transitioning to post-quantum cryptography (PQC). The three volumes¹ are designed for different audiences, moving from awareness and decision-making to governance, financial planning, and technical implementation.

VOLUME 01

Preparing for the Quantum Era

Updated Strategic Guidance

This volume introduces the quantum threat, raises awareness, and provides updates on timelines, policy developments, and the urgency of post-quantum migration. Its target audience is decision-makers.

VOLUME 02

Managing the PQC Transition

Governance, Planning and Investment

This volume explains what is needed to initiate a PQC transition within an organisation, including governance, planning, responsibilities, funding considerations, and coordination across stakeholders. Its target audience is governance, risk and compliance (GRC) teams, project managers and technical coordinators.

VOLUME 03

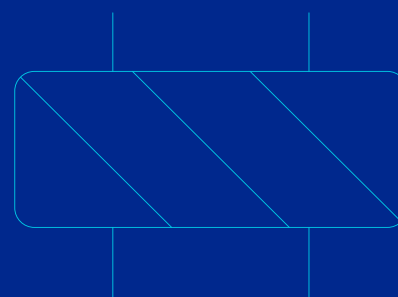
Implementing the PQC Migration

Technical and Migration Guidance

This volume provides technical guidance on post-quantum cryptography and PQC migrations, including algorithm choices, implementation considerations, interoperability, testing, and operational deployment. Its target audience is engineers, developers, IT architecture and operations teams.

¹ The documents can be found here: <https://cybersecuritycoalition.be/resource/white-paper-preparing-for-the-quantum-era>

1	Scope	4
2	Stakeholder Guidance	5
2.1	Security Leadership	5
2.2	Project Managers And Technical Coordinators	5
2.3	Governance, Risk Management And Compliance (GRC)	6
2.4	Procurement	7
3	Roadmap & Timeline For Transition	8
3.1	Planning Principles	8
3.2	Near-Term Next Steps	8
3.3	Reference Roadmap	9
4	Governance & Programme Management	10
4.1	Why Governance Matters For PQC	10
4.2	Dedicated Programme Vs. Integration	11
4.3	Two-Layer Governance Model	12
4.4	Roles And Responsibilities	14
4.5	Executive Buy-In And Board Oversight	15
4.6	Governance Best Practices	15
4.7	Programme Execution Model	17
4.8	Closing Perspective	17
5	The Business Case & Financial Planning	18
5.1	Why Is This Needed?	18
5.2	Phased Execution	18
5.3	Cost Categories	19
5.4	Template And Methodology	20
5.5	Calibration And Reasonableness Checks	21
5.6	Articulating ROI And Value: Risk Reduction, Compliance & Agility	22
6	Risk Framing & Migration Prioritisation	23
6.1	Risk Dimensions	23
6.2	Practical Prioritisation Guidelines	23
7	Real-World Example: Incumbent Telecom Operator	25
8	What's Next?	27
9	Collaboration & Continuous Learning	28
10	External Guidance	29
11	Acronyms	30
12	Appendix	32
13	Team	36



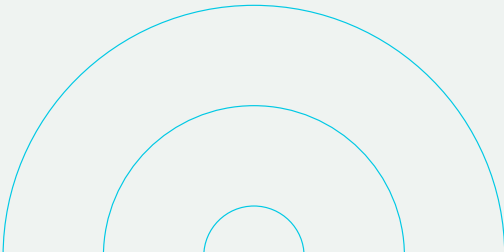
Scope

This volume helps organisations answer the question: What is needed to initiate, govern, fund, and coordinate a PQC transition?

Volume 2 is the bridge between executive urgency and technical execution. It does not attempt to define migration patterns in detail. Instead, it provides the organisational, financial, and governance scaffolding required to make the technical work in Volume 3 feasible, funded, prioritised, auditable, and sustainable.

The intended outcome is a controlled transition programme: one that is risk-based, funded, integrated into existing governance processes, aligned with external timelines, and capable of moving from discovery to pilots and then to migration waves.

Volume 3 will build on this foundation by translating the programme roadmap into technical execution, providing detailed guidance on cryptographic discovery, solution selection, migration architectures, testing approaches, implementation patterns, and operational integration. Together, the two volumes help organisations move from strategic planning to practical deployment.



TOPIC	WHAT THIS VOLUME PROVIDES	WHAT VOLUME 3 COVERS INSTEAD
ROADMAP	Milestones, sequencing, programme phases.	Technical implementation details.
GOVERNANCE	Steering Committee, Programme Office, RACI, reporting, escalation.	Interoperability management, shared infrastructure coordination.
RISK	Prioritisation logic, risk assessment.	Detailed cryptographic inventory.
COMPLIANCE	Regulatory compliance, audibility, evidence.	Controls and implementation validation.
PROCUREMENT	Vendor roadmaps, contractual readiness.	Technical requirements.
FINANCE	Cost categories, phased budgeting, business case.	Technical cost considerations and trade-offs.

Stakeholder Guidance

Several groups play a decisive role at this preparation stage. This chapter sets out what each of them is expected to contribute.

2.1 Security Leadership

Post-quantum cryptography is not a technology refresh with a defined completion date. It is a long-horizon change in the way organisations manage cryptographic risk. The question for security leadership is not whether to act, but how to phase action in the face of a risk whose timing cannot be pinned down.

Security leadership should position PQC as a strategic resilience issue, not merely as a compliance or cryptography project. The most important near-term actions are organisational: funding and scoping a quantum-readiness assessment, assigning ownership across security, architecture, compliance, and infrastructure, adding PQC to risk reporting, and engaging vendors on their PQC roadmap commitments.

Security leaders should ensure that:

- * PQC appears in enterprise risk registers and Board or Steering Committee reporting.
- * A named executive sponsor is accountable for direction, prioritisation, and funding.
- * The PQC roadmap is linked to enterprise architecture, security strategy, cloud strategy, PKI strategy, identity strategy, and procurement.
- * PQC is framed as resilience and continuity, not only as future compliance.

2.2 Project Managers And Technical Coordinators

Project managers and technical coordinators are the central audience for this volume. Their role is to translate strategic intent into an executable programme.

They should coordinate:

- * Workstream planning and dependencies.
- * Inventory and discovery activities.
- * Risk prioritisation workshops.
- * Vendor evidence collection.
- * Pilot planning and lessons learned.
- * Migration wave sequencing.
- * Budget planning and tracking.
- * Reporting to the PQC Programme Office and Steering Committee.
- * Integration with change, architecture, security, procurement, compliance, and operational processes.

They do not need to make all technical cryptographic decisions themselves. However, they must ensure the right technical experts, application owners, platform teams, vendor contacts, and risk stakeholders are involved at the right time.

Security leadership should position PQC as a strategic resilience issue, not merely as a compliance or cryptography project.



2.3 Governance, Risk Management And Compliance (GRC)

Embedding PQC into governance, risk and compliance processes is what secures both regulatory alignment and sustained oversight throughout the transition.

2.3.1 Governance

Organisations should treat post-quantum cryptography (PQC) as a governed organisational capability, not only as a set of technical controls or policy updates. This means assigning executive sponsorship, defining clear ownership and accountability, and integrating PQC into existing governance forums for risk, architecture, procurement, compliance, and security oversight.

PQC governance should ensure that key decisions are made consistently across the organisation, including prioritisation of high-risk use cases, approval of migration roadmaps, acceptance of residual risk, vendor dependency management, and escalation of blockers.

Policies, standards, and controls are essential, but they should be positioned as supporting governance artefacts: instruments that translate leadership decisions into enforceable, auditable, and repeatable requirements. This includes maintaining cryptographic asset visibility, defining crypto-agility expectations, updating procurement and architecture criteria, and ensuring that progress can be monitored and evidenced over time.

By embedding PQC into existing governance structures, organisations make quantum readiness part of normal risk and compliance management rather than an isolated initiative. The result is a transition path that is owned, prioritised, funded, enforceable, and auditable.

2.3.2 Risk Management

From a risk perspective, PQC must be treated as a long-horizon, strategic cybersecurity risk rather than a purely technical upgrade. The uncertainty around quantum timelines does not reduce the risk; if anything, it makes early action more necessary, particularly where data confidentiality or system trust must be preserved over long periods.

Organisations should:

- * Integrate PQC into enterprise risk management frameworks and risk registers.
- * Assess exposure based on data sensitivity, retention periods, and system lifecycles.
- * Prioritise systems where migration timelines may exceed the remaining security lifetime.
- * Assess concentration risk by identifying the proportion of critical assets dependent on the same vendor, cryptographic library, platform or common upstream software component.
- * Track risk evolution over time as migration progresses and external dependencies evolve.

This approach ensures that PQC is continuously evaluated, prioritised, and aligned with overall risk appetite and business impact.

PQC must be treated as a long-horizon, strategic risk rather than a purely technical upgrade.



2.3.3 Compliance And Audit Teams

Regulatory frameworks such as NIS2 increasingly require organisations to adopt state-of-the-art cryptographic practices, making PQC integration not only a forward-looking measure but also a compliance necessity.

Compliance and audit teams must be able to demonstrate a controlled and traceable transition path towards quantum readiness.

This includes:

- ★ Integrating PQC into audit frameworks, control testing, and compliance reporting.
- ★ Ensuring visibility on dependencies, vendor readiness, and migration status.
- ★ Providing evidence that PQC is actively managed as an ongoing risk, not a future concern.

2.4 Procurement

PQC considerations must extend across the supply chain, as vendor dependencies can significantly affect the overall transition timeline.

Organisations should:

- ★ Embed PQC requirements into procurement policies, contracts, and supplier selection criteria.
- ★ Require vendors to disclose their use of cryptography and provide clear PQC transition roadmaps.
- ★ Integrate PQC into third-party risk assessments, audits, and security questionnaires.
- ★ Monitor and track vendor readiness through structured and repeatable mechanisms.



This approach ensures that critical suppliers do not become bottlenecks in the transition and that external dependencies evolve in line with internal readiness.

Additionally, earlier vendor support for PQC enables faster migration, reducing both quantum-related risks and the costs of delaying the transition.

A practical starting point is to run quantum-readiness surveys, which provide a structured way to assess vendor maturity and identify gaps early.

Example: Citi Quantum Readiness Survey (see 10. External Guidance).

Roadmap & Timeline For Transition

3.1 Planning Principles

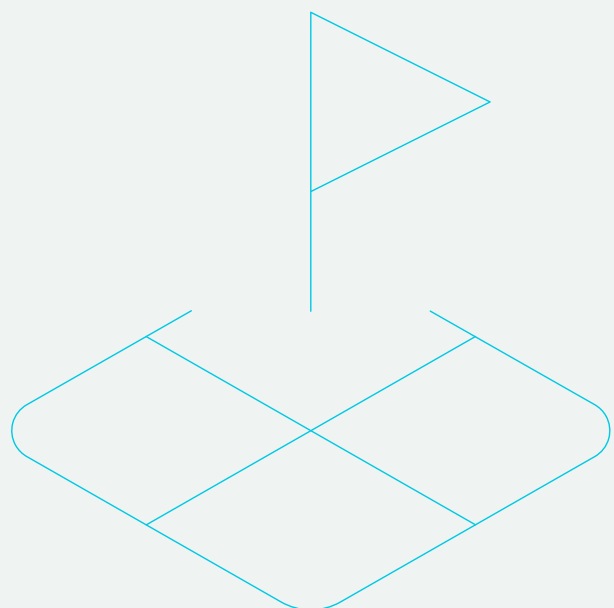
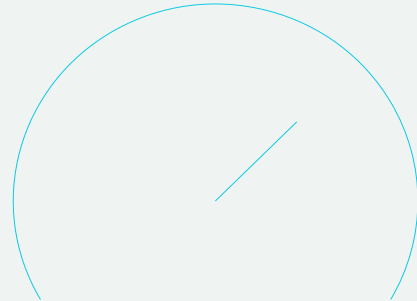
A PQC transition should be planned as a phased, risk-based and iterative programme. Its roadmap should align with regulatory expectations and technical readiness, and cover inventory, risk assessment, awareness, pilots, migration planning and the eventual transition of high-, medium- and low-risk systems.

The roadmap should follow four principles:

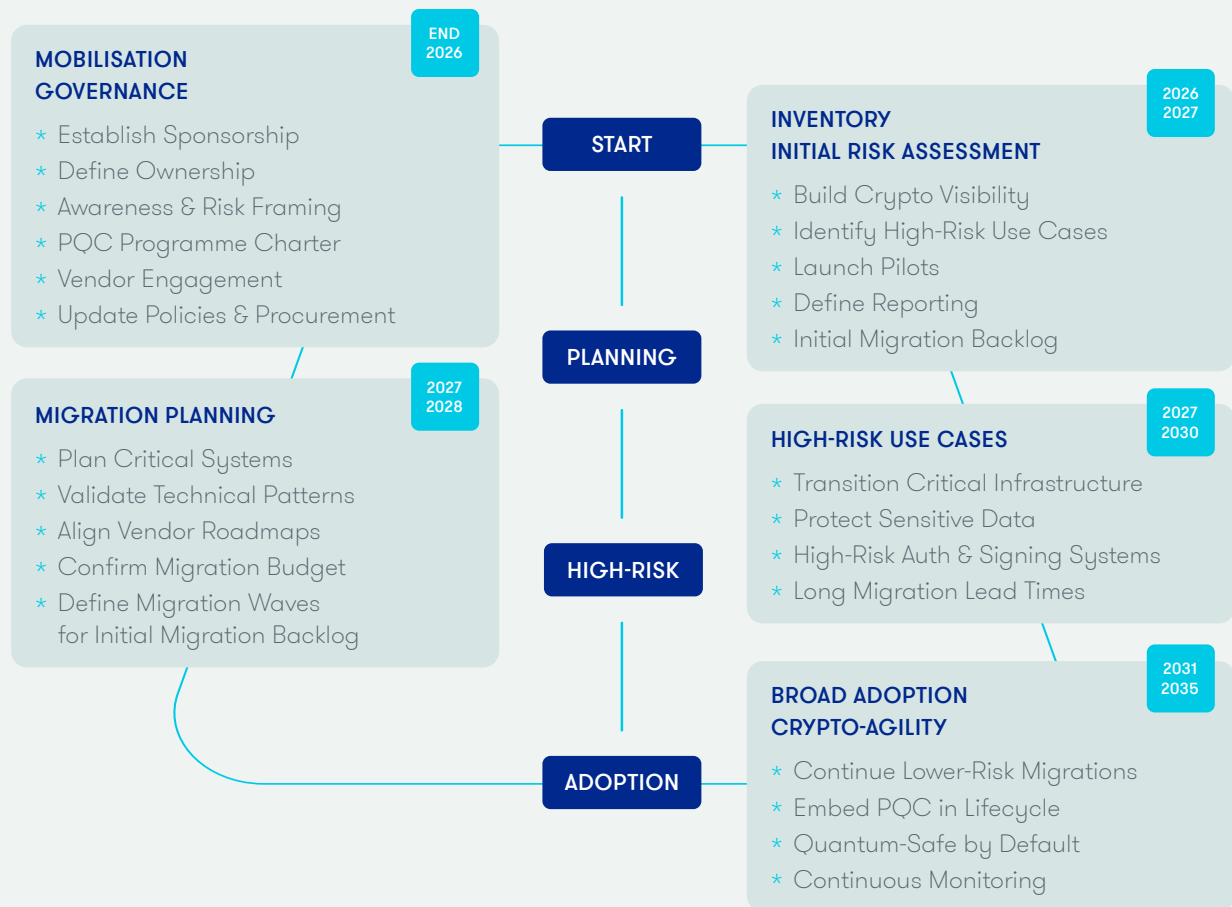
- ★ **Start with the highest-risk use cases**
Prioritise systems protecting long-lived sensitive data, critical infrastructure, authentication, signing, firmware, certificates, and systems with long replacement cycles.
- ★ **Run inventory and migration in parallel**
A complete inventory is valuable, but waiting for perfection can delay action. Known gaps, assumptions, responsible owners, and actions to address outstanding discovery gaps should be documented and regularly reviewed. Inventory activities should continue throughout the programme, and significant new findings should be used to update risk assessments, priorities, and migration plans.
- ★ **Use pilots to build confidence**
Early pilots — for example, hybrid TLS in controlled environments — help test governance, vendor readiness, operational impact, and technical feasibility without committing the whole enterprise at once.
- ★ **Embed PQC into existing governance**
PQC should be integrated into risk management, architecture review, secure development, procurement, supplier management, compliance, and change processes rather than treated as an isolated initiative.

3.2 Near-Term Next Steps

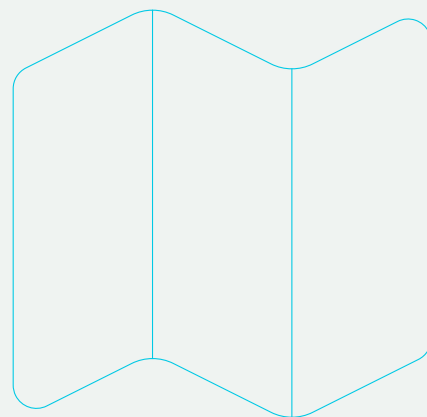
Organisations should start by forming a core PQC team and running a workshop on quantum risk, so that IT and security leaders share the same picture. In parallel, they should secure executive sponsorship and budget for a formal PQC programme.



3.3 Reference Roadmap



These reference dates draw on the EU coordinated roadmap's recommended milestones² and on BIPT's supervised sectoral timetable for Belgian telecommunications operators³.



² <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>

³ <https://www.bipt.be/operators/publication/communication-of-13-january-2026-on-minimum-requirements-and-roadmap-for-the-post-quantum-transition-in-the-telecommunications-sector>

Governance

& Programme Management

4.1 Why Governance Matters For PQC

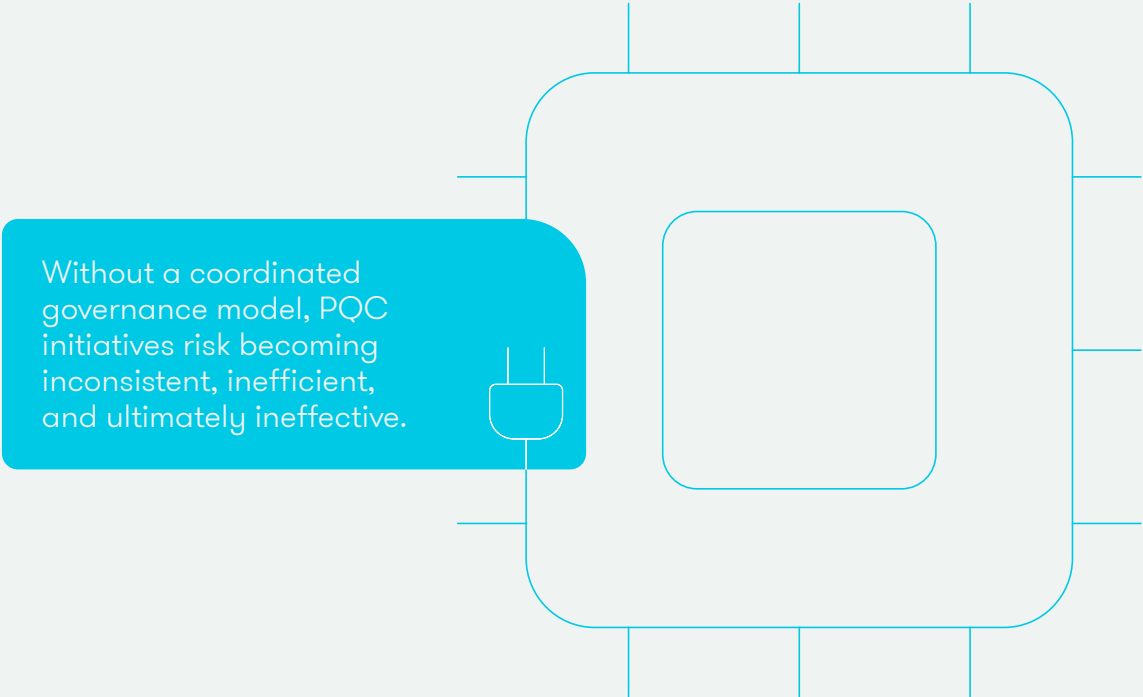
Transitioning to post-quantum cryptography is not a typical technology upgrade. It is a long-duration, enterprise-wide transformation that spans infrastructure, applications, vendors, and regulatory obligations. Most organisations will face a multi-year, potentially decade-long journey in which classical and post-quantum cryptography must coexist.

This introduces structural challenges:

- * Cryptographic assets are deeply embedded, interdependent and often poorly inventoried.
- * Dependencies span multiple teams and third parties.
- * Migration sequencing must avoid operational disruption.

PQC migration spans infrastructure, applications, identity, certificates, cloud, operational technology, and a wide range of vendors, often requiring funding across multiple budgets and competing with other business priorities.

Without clear governance, efforts quickly become fragmented — different teams may independently run pilots or build inventories, without a unified view of risk, dependencies, or progress. Without a coordinated governance model, PQC initiatives risk becoming inconsistent, inefficient, and ultimately ineffective.



Without a coordinated governance model, PQC initiatives risk becoming inconsistent, inefficient, and ultimately ineffective.

4.2 Dedicated Programme Vs. Integration

A dedicated PQC programme and integration into existing governance frameworks each offer distinct advantages, and in practice they should be seen as complementary rather than mutually exclusive. A standalone programme provides the visibility, focus, and central coordination needed to initiate the transition, secure funding, and manage complex dependencies across teams and vendors.

In contrast, integrating PQC into existing governance structures — such as risk management, architecture, procurement, and compliance — ensures long-term sustainability, regulatory alignment, and shared ownership across the organisation, but may initially lack urgency, coordination and clear accountability.

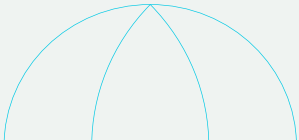
As a result, most organisations benefit from starting with a dedicated programme to build momentum and structure, then progressively embedding PQC into existing governance frameworks to make it part of business-as-usual operations.

	ADVANTAGES	DISADVANTAGES
STANDALONE	* High visibility and clear prioritisation. * Strong central coordination and ownership. * Easier to track progress, KPIs, and dependencies. * Faster mobilisation in early phases. * Dedicated funding and resources. * Clear accountability (programme lead, Steering Committee).	* Additional governance overhead. * Risk of duplication with existing processes. * Can become siloed from enterprise architecture and risk frameworks. * Dependency on a limited number of specialists. * May lose momentum once priorities shift or funding decreases. * Harder to embed into long-term operations ("business as usual").
GOVERNANCE INTEGRATION	* Leverages existing frameworks (risk, SDLC, procurement, compliance). * Lower overhead; avoids creating parallel structures. * Easier alignment with regulations (NIS2, DORA, CRA). * More sustainable long-term ("business as usual"). * Broader ownership across the organisation (not siloed). * Better integration with other transformation initiatives (cloud, IAM, PKI, etc.).	* May lack initial visibility and urgency. * Competes with existing priorities within those structures. * Risk of slow progress if not explicitly prioritised. * Harder to coordinate cross-domain dependencies without central control. * Accountability can become diffuse.

4.3 Two-Layer Governance Model

A successful PQC transition requires a formal governance framework with clear ownership, executive sponsorship, and cross-functional coordination.

A clear distinction should be made between strategic governance and programme execution. Organisations should establish both a PQC Steering Committee and a dedicated PQC Programme Office (PMO) to govern and operationalise the multi-year PQC transformation effort.



	MAIN BODY	PURPOSE
STRATEGIC GOVERNANCE	PQC STEERING COMMITTEE	Sets direction, approves scope, owns risk appetite, secures funding, resolves prioritisation conflicts, and reports to executive leadership.
PROGRAMME EXECUTION	PQC PROGRAMME OFFICE (PMO)	Coordinates execution, tracks dependencies, manages reporting, maintains the migration backlog, coordinates pilots, and supports workstreams.

4.3.1 PQC Steering Committee

The Steering Committee should include senior representation from security, IT, infrastructure, enterprise architecture, risk, compliance, procurement, legal/data protection where relevant, and business domains with critical services.

Key characteristics

- * Executive sponsorship
Typically led by a CISO, CTO, or CIO.
- * Board visibility
Regular reporting on quantum risk posture and migration progress.
- * Senior cross-functional representation
 - * Security & Cryptography.
 - * IT / Infrastructure.
 - * Application Development.
 - * Risk & Compliance.
 - * Procurement / Vendor Management.
 - * Enterprise Architecture.
 - * Legal and Data Protection [where applicable].

Responsibilities

- * Define and approve PQC strategy and target state.
- * Approve roadmap, priorities, and risk appetite.
- * Secure funding and executive alignment.
- * Oversee vendor and supply chain risk exposure.
- * Monitor progress and escalate strategic risks.
- * Report to executive leadership and the board.

The Steering Committee should regularly challenge persistent budget underspend, recurring migration delays, growing vendor dependency risks, and ageing exceptions.

The Steering Committee acts as the strategic compass of the PQC journey, ensuring the organisation moves deliberately rather than reactively through a transformation expected to span many years.

4.3.2 PQC Programme Office (PMO)

Organisations should establish a Programme Office (PMO) responsible for driving and coordinating the PQC transformation.

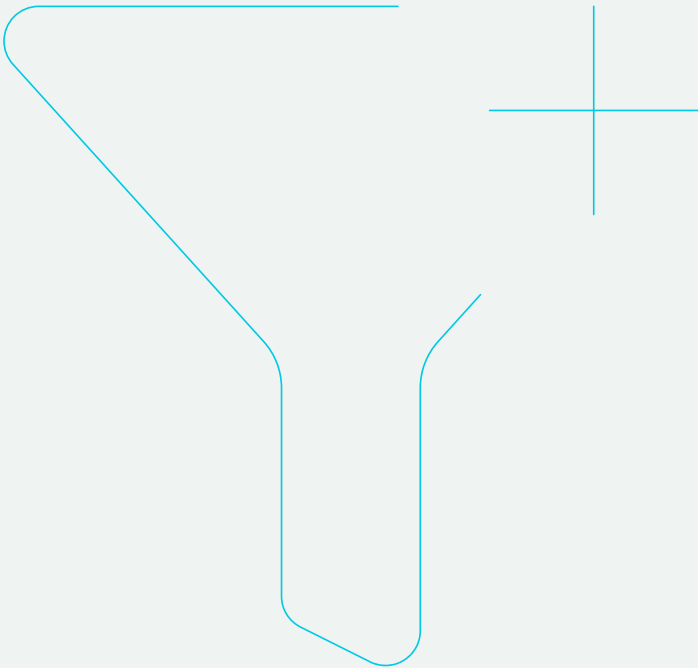
Key characteristics

- * Dedicated coordination function
Central team responsible for programme orchestration.
- * Structured leadership
Programme manager supported by technical migration coordinators.
- * Centralised visibility
Unified tracking of progress, dependencies, and risks.
- * Cross-functional liaison
Bridge between strategic governance and operational teams.
- * Consistency driver
Ensures alignment across business units and workstreams.

Responsibilities

- * Coordinate enterprise-wide PQC activities and workstreams.
- * Maintain the migration inventory and tracking repository.
- * Manage dependencies across systems, vendors, and platforms.
- * Track progress, KPIs, and risk exposure.
- * Support prioritisation of systems and use cases.
- * Ensure alignment with regulatory and compliance expectations.
- * Escalate issues and blockers to the Steering Committee.

The PMO functions as the operational engine room of the PQC transition, translating strategic intent into coordinated execution across a highly distributed technology landscape.



4.4 Roles And Responsibilities

Clarity of ownership is essential. PQC migration touches many domains, and ambiguity quickly leads to stalled execution.

The RACI-style model below shows how responsibilities are typically distributed.

This structure ensures that decision-making authority and execution responsibility are clearly separated but tightly coordinated.

	EXECUTIVE SPONSOR	STEERING COMMITTEE	PMO	SECURITY ARCHITECTURE	APPLICATION PLATFORM OWNERS	PROCUREMENT	RISK COMPLIANCE	INTERNAL AUDIT
PQC STRATEGY	A	R	C	C	C	I	C	I
ROADMAP APPROVAL	A	R	C	C	C	C	C	I
INVENTORY COORDINATION	I	C	A/R	C	R	C	C	I
RISK PRIORITISATION	A	R	R	C	C	I	R	I
TECHNICAL STANDARDS	I	A	C	R	C	I	C	I
VENDOR READINESS	I	C	A/R	C	C	R	C	I
MIGRATION EXECUTION	I	C	A/R	C	R	C	C	I
AUDIT EVIDENCE	I	C	R	C	C	C	A/R	R

R = RESPONSIBLE

A = ACCOUNTABLE

C = CONSULTED

I = INFORMED

4.5 Executive Buy-In And Board Oversight

PQC migration requires sustained executive commitment, for three reasons:

- * Long timelines (often 5–10+ years).
- * Significant investment in systems and processes.
- * Dependencies on external vendors and standards evolution.

Therefore:

- * PQC should be framed as a strategic risk initiative, not just a technical upgrade.
- * Regular board-level reporting should include:
 - * PQC readiness of critical systems.
 - * Vendor compliance status.
 - * Residual quantum risk exposure.

4.6 Governance Best Practices

4.6.1 Establish Clear Policies And Standards

Update the organisation's cryptography policy to explicitly include:

- * Approved PQC and hybrid algorithms.
- * Crypto-agility requirements.
- * Migration timelines and priorities.
- * Key management and lifecycle considerations.

This creates a single source of truth that guides all teams.

4.6.2 Implement Structured Progress And Risk Reporting

Define a consistent reporting cadence (e.g. quarterly).

Reporting should combine:

- * Migration progress against roadmap.
- * Percentage of systems assessed/migrated.
- * Risk exposure trends.
- * Vendor readiness.

Dashboards help, where they can be maintained: they turn a complex programme into a picture that supports decisions. Dashboards should focus on trends, forecast completion, emerging risks, and decisions required — not just on completed tasks.

Recommended indicators include:

- * **Budget execution against plan**
This indicator could identify a programme that has secured funding but is not progressing at the expected pace.
- * **Migration progress and forecast-to-complete**
Tracks delivery against milestones and highlights potential schedule slippage.
- * **Vendor dependency exposure**
Monitors critical migrations dependent on third-party PQC support and identifies vendor-blocked assets requiring escalation or alternative treatment.
- * **Exception ageing**
Tracks the duration of approved exceptions, waivers, and risk acceptances to ensure that temporary measures do not become permanent risks.

4.6.3 Leverage Existing Processes

There is no need to build a parallel governance structure from scratch.

Instead:

- ★ Use existing architecture boards to approve PQC designs.
- ★ Use risk committees to track quantum-related risks.
- ★ Use procurement workflows to enforce vendor compliance.

Adapt these processes to include PQC criteria rather than duplicating them.

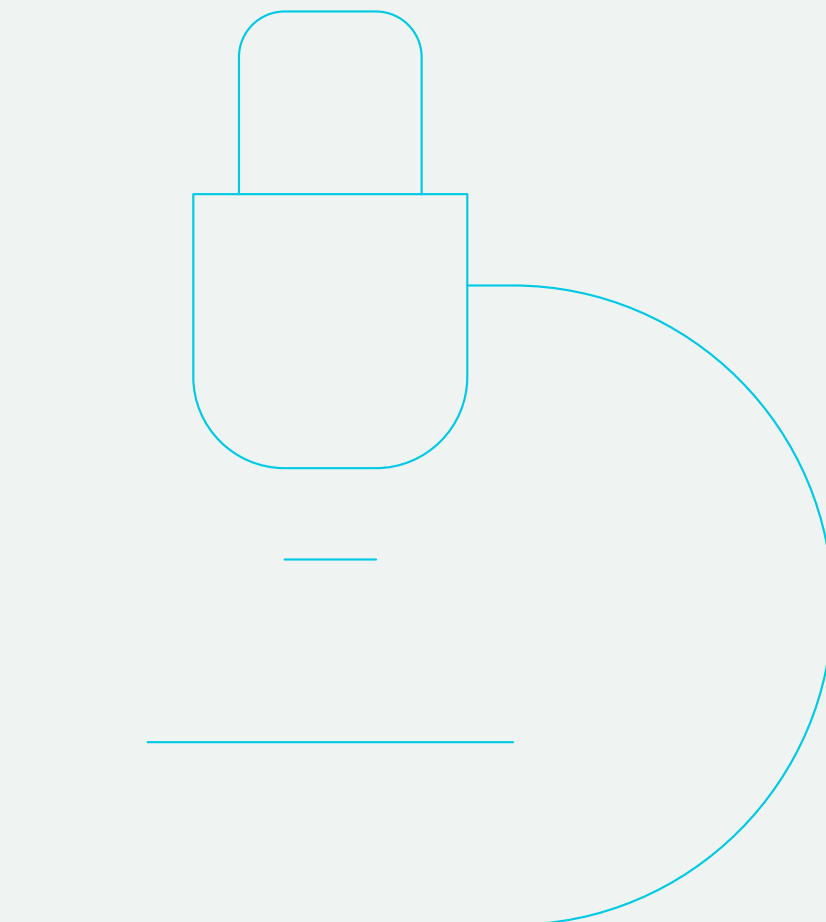
4.6.4 Drive Cross-Functional Coordination

PQC is inherently interdisciplinary.

Encourage:

- ★ Shared ownership across teams.
- ★ Regular cross-functional workshops.
- ★ Centralised documentation and standards.

Without this, the programme risks becoming a collection of isolated migrations that do not quite fit together.



4.7 Programme Execution Model

A PQC transition programme should be structured into parallel workstreams, centrally coordinated by the PMO to ensure alignment and consistency.

The high-level roadmap set out in Chapter 3 provides a foundation that can be further decomposed into detailed, executable workstreams.

Example workstreams:

WORKSTREAM	PURPOSE	KEY OUTPUTS
GOVERNANCE AND RISK	Create oversight, decision rights, risk appetite, escalation, and reporting.	Charter, governance model, risk register, reporting cadence.
INVENTORY AND TOOLING	Build visibility into cryptographic use and dependency chains.	Asset inventory, cryptographic inventory, CBOM/SBOM inputs, ownership map.
PRIORITISATION	Rank systems by data lifetime, criticality, exposure, migration complexity, and trust function.	Prioritised migration backlog.
POLICY AND STANDARDS	Embed PQC and crypto-agility into internal policies and standards.	Cryptography policy updates, procurement language, architecture principles.
VENDOR AND PROCUREMENT	Understand supplier readiness and contractual dependencies.	Vendor surveys, roadmap evidence, contractual clauses, risk exceptions.
PILOTS AND VALIDATION	Test migration patterns in controlled environments.	Pilot results, performance findings, implementation lessons.
MIGRATION WAVES	Execute migration by risk tier and dependency group.	Wave plans, cutover plans, rollback plans, evidence packs.
MONITORING AND ADAPTATION	Track standards, vulnerabilities, vendor changes, and migration effectiveness.	Dashboards, periodic reassessments, updated roadmap.

4.8 Closing Perspective

A PQC transition is less like a sprint and more like a long expedition across shifting terrain. The cryptographic landscape will evolve, standards will mature, and priorities will change.

Governance is what keeps the expedition on course. With a strong programme structure, clear accountability, and sustained executive engagement, organisations can turn PQC from an abstract future risk into a controlled, measurable and ultimately successful programme.

The Business Case & Financial Planning

5.1 Why Is This Needed?

For most organisations, post-quantum migration is a multi-year transformation programme touching applications, infrastructure, identity platforms, vendor contracts, compliance processes, operational procedures and security governance. This makes early quantification essential.

Without a structured estimate of the expected effort, organisations risk underestimating the scale of the transition, delaying budget discussions, or discovering too late that critical systems cannot be upgraded within the required timeframe.

A business case is needed to:

- * Estimate the scale of work.
- * Avoid underfunding discovery and planning.
- * Sequence spending across budget cycles.
- * Align migration with technology refresh cycles.
- * Fund pilots before enterprise rollout.
- * Make vendor and hardware replacement dependencies visible.
- * Support risk acceptance where migration cannot be completed immediately.

5.2 Phased Execution

Unlike a one-off technology upgrade, a quantum-safe transition is a long-term programme spanning a decade or more for large organisations. A critical-infrastructure operator, for example, might plan for 10–12 years of effort to reach full PQC adoption. This extended timeline reflects the need to phase the work: establishing governance and inventory, then upgrading the highest-risk systems, and gradually migrating medium- and low-risk assets.

Advantages of a phased approach:

- * Spread costs across multiple budget cycles (multi-year phasing).
- * Align PQC upgrades with natural technology refresh cycles (e.g. end-of-life replacements).
- * Embed PQC investments into existing hardware or software upgrade plans.
- * Take advantage of overlaps with other initiatives, for example cloud transformation or NIS2/DORA compliance programmes.

Without a structured estimate of the expected effort, organisations risk underestimating the scale of the transition.



5.3 Cost Categories

The business case may include the following cost categories, which can be aligned with the workstreams described in Section 4.7.

COST CATEGORY	EXAMPLES
GOVERNANCE AND RISK	PMO, reporting, steering, risk management, coordination.
INVENTORY AND TOOLING	Discovery tooling, asset enrichment, CBOM/SBOM processing, integration with CMDB/GRC.
TECHNICAL ASSESSMENT	Application reviews, platform assessments, PKI analysis, HSM/vendor readiness.
VENDOR AND PROCUREMENT	Product upgrades, roadmap commitments, contract changes, external assessments.
PILOTS AND MIGRATION EXECUTION	Engineering effort, testing, release management, rollback planning.
OPERATIONS AND ONGOING MONITORING	Crypto policy review, dashboarding, audit evidence.
TRAINING AND AWARENESS	Security, architecture, procurement, application owner, and operations training.

5.4 Template And Methodology

To help organisations quantify the PQC effort and build a business case, we provide a simplified cost estimation template (Excel workbook) alongside this white paper. This template is structured to capture the major cost inputs discussed above and project them over the programme timeline. The goal is to let organisations tailor assumptions (e.g. size/complexity, duration, scope) and compute an approximate budget.

The template does not produce a precise quote; it provides a starting point. Organisations should adjust the assumptions (e.g. use internal labour rates and include any extra categories unique to their situation). The structure ensures that no major cost category is overlooked and that

the timeline of spend is visible (e.g. light in early years for inventory and design, heavy in later years for implementation, with some steady ongoing maintenance cost).

Using such a model allows the PQC lead to present the business case with concrete figures — e.g. ‘We estimate a €X million total programme cost over Y years, peaking at €P million in the busiest year.’ Having an evidence-based, itemised forecast increases credibility when seeking budget approval, as it demonstrates a well-thought-out plan rather than an arbitrary number.

It also enables quick sensitivity analysis: e.g. ‘What if we compress the timeline to 7 years?’



Below is an outline of how the template is organised:

* Example Values

Global default assumptions: default values per complexity level (Low/Medium/High).

* Workstream defaults

Default values for each workstream (Governance, Inventory, etc.).

* Phasing defaults

Workstreams are allocated as percentages across years (reflecting likely phasing: e.g. more spend on inventory in years 1–2, on implementation in later years).

* Complexity Tier

Choose the Complexity Tier. This sets the high-level scenario parameters.

* Programme Summary Dashboard

A summary tab automatically aggregates the total cost per year of the programme across all workstreams, and provides a CapEx vs OpEx breakout for each year and in total. This gives a consolidated view of the multi-year budget for the PQC programme.

5.5 Calibration And Reasonableness Checks

Published figures can provide useful reference points for calibrating estimates, provided they are treated as indicative. Estimates should also be reviewed and refined throughout the programme as discovery activities and practical migration experience provide greater visibility into actual costs and resource requirements.

5.5.1 Discovery And Inventory

Discovery is far more complex than procuring and deploying a scanning tool. As a result, organisations frequently underestimate the budget required to establish a comprehensive cryptographic inventory.

Automated discovery solutions may fail to identify embedded cryptography, customised applications, inaccessible environments, shadow IT assets, or vendor-managed implementations. Manual validation, asset enrichment, architectural analysis, and supplier engagement remain essential components of a comprehensive cryptographic inventory.

One estimate⁴ suggests that a large-enterprise discovery programme may require approximately \$2 million to \$5 million, involving 5 to 15 specialists over a period of six to twelve months. The same source estimates \$0.5 million to \$1.5 million for a mid-sized organisation. These figures should be viewed only as directional reference points, as actual costs depend heavily on organisational complexity, asset diversity, and the maturity of existing inventory processes.

⁴ <https://postquantum.com/pqc-governance/pqc-migration-cost>

5.5.2 Implementation And Replacement

Implementation typically becomes the largest cost component of a PQC migration programme. However, its relative share should be derived from organisation-specific analysis rather than assumed through predefined allocations.

Key cost drivers include:

- * Application modifications.
- * Integration, interoperability, and regression testing.
- * Public Key Infrastructure (PKI) and identity-management changes.
- * Vendor-provided upgrades and product replacements.
- * Operational deployment.
- * The replacement or decommissioning of systems that cannot support PQC or hybrid cryptographic approaches.

For guidance on estimating implementation costs, including practical examples, refer to the Framework for Estimating the Costs of Migrating to PQC listed under 10. External Guidance.

5.5.3 Maintaining A Living Estimate

At each major programme milestone, generic assumptions should be replaced with observed organisational data, allowing the estimate to progressively improve in accuracy and confidence.

This iterative approach enables organisations to transition from estimates and broad industry benchmarks towards evidence-based forecasting that reflects their own architecture, supplier landscape, operational constraints, and migration progress.

5.6 Articulating ROI And Value: Risk Reduction, Compliance & Agility

Justifying PQC investments requires reframing return on investment in terms of risk mitigation and strategic value rather than revenue. Unlike traditional initiatives, a quantum-safe programme primarily delivers value by avoiding future losses and ensuring long-term continuity.

Organisations can also contain costs by aligning PQC adoption with existing hardware and software renewal cycles. These are the moments at which vendors can be required to include PQC support, which reduces incremental investment.

Key points to articulate in the business case include:

* Regulatory Compliance & Fine Avoidance

In regulated sectors, authorities such as BIPT (Belgian Institute for Postal Services and Telecommunications) have begun establishing minimum requirements for the transition to PQC. Delayed or inadequate action may therefore contribute to audit findings, enforced remediation, or financial penalties.

* Reducing Breach Risk & Cost of Inaction

The cost of inaction can be quantified: consider the potential cost of a breach of long-lived sensitive data (data breach costs, customer churn, incident response). A PQC programme serves as an insurance policy against such future events. The return here lies in avoiding a loss, but that risk reduction still carries a real expected value (some models frame it as an annual cost-of-inaction figure).

* Protecting Long-Lived Data & Customer Trust

For industries like telecom, finance, or healthcare, data must often remain confidential for decades. Securing this long-lived data preserves customer trust — clients expect their personal and confidential data to remain safe even as technology evolves. By becoming quantum-safe, the organisation safeguards its brand reputation, preventing the damage to trust that would follow if attackers were to decrypt historical data in the future.

* Competitive Differentiation

Being an early ‘quantum-safe’ organisation can be a market differentiator. Customers, especially in B2B markets and public-sector procurement, may prefer vendors that can demonstrate a quantum-safe posture. The business case can mention potential commercial upside: while difficult to quantify, early movers may win deals or command a premium by providing higher assurance.

* Crypto-Agility = Future Cost Avoidance

A major intangible return on a PQC programme is improved crypto-agility across systems. By investing in agile frameworks now (e.g. abstraction layers for crypto, automated certificate management), the organisation sets itself up to handle future cryptographic changes far more quickly and at lower cost. This means that if any new vulnerability or algorithm update arises (quantum-related or not), the cost and time to respond will be far lower than today.

* Preserving ‘Licence to operate’

For critical infrastructure companies and financial institutions, quantum security will increasingly be seen as part of the basic duty of care. Falling behind could result not just in fines but in loss of business contracts or government accreditations. The PQC programme therefore ensures that the company can continue to operate in its market without disruption or external intervention.

Risk Framing & Migration Prioritisation

6.1 Risk Dimensions

PQC risk should be assessed across two complementary dimensions.

- ★ Confidentiality risk
The potential exposure of sensitive information due to cryptographic failure.
- ★ Trust and authenticity risk
The potential breakdown of confidence in identities, integrity, and security decisions that rely on cryptographic assurance.

Treating only one dimension creates blind spots, because a system may appear protected from disclosure while still being exposed to failures of trust, validation, or assurance.

Considering both dimensions enables effective prioritisation by focusing on the areas where cryptographic failure would have the greatest security impact.

	EXAMPLES	GOVERNANCE IMPLICATION
CONFIDENTIALITY RISK	Sensitive traffic, stored encrypted archives, long-lived customer data, state secrets, health or financial data.	Prioritise data with long confidentiality lifetimes and systems with slow migration timelines.
TRUST AND AUTHENTICITY RISK	PKI, certificates, code signing, firmware signing, secure boot, document signing, identity systems.	Identify signing and trust infrastructure early.

6.2 Practical Prioritisation Guidelines

As in traditional vulnerability management, it is almost impossible to tackle every problem at once. High-risk assets should be addressed first in a PQC migration strategy. This can be in the discovery phase, by scanning and investigating high-risk assets first, or in the remediation phase, by fixing the critical cryptographic vulnerabilities found on high-risk assets first. This measure of criticality helps organisations direct their effort where it counts most.

Organisations should begin the migration with a proof of concept or a quick win, for example by migrating less critical web servers to post-quantum TLS, to get familiar with the migration process. After this first deployment,

further rollout of PQC should follow a risk-based approach where critical systems or assets are migrated first.

Note: It is important to recognise that not all assets can be migrated to PQC immediately. Certain assets, particularly those that depend on digital signatures or digital certificates, may currently face migration constraints due to the evolving maturity of post-quantum certificate and signature ecosystems and the limited availability of broadly supported implementation standards. Despite these constraints, such assets should retain the prioritisation score initially assigned during the migration assessment, reflecting their

continued cryptographic exposure and long-term migration requirements. Where migration is not yet technically or operationally feasible, the resulting residual risk should be formally assessed, documented, and actively managed until a viable and widely supported migration path becomes available.

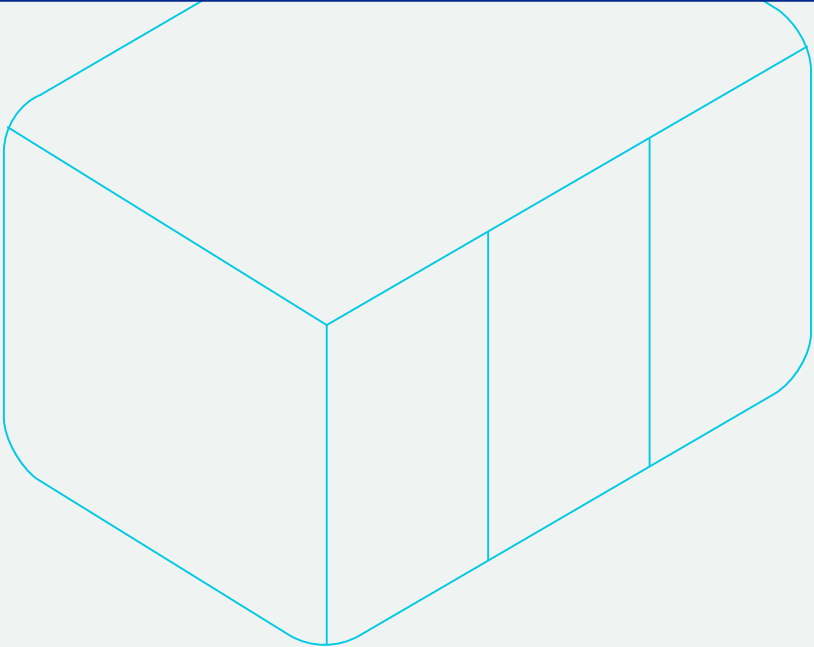
The following model is proposed to assess the criticality of cryptographic assets. It supports both a high-level evaluation and a more granular assessment by incorporating additional metrics where needed.

The PQC Migration Priority Calculator⁵ can be used to apply and validate this approach in practice.

It is very likely that external TLS connections score very high because of their internet exposure. Files exchanged over the internet using SFTP, and downloadable signed content, will also score high. Internal TLS connections will score lower, and databases encrypted with symmetric algorithms will be found at the lower end of the scale.

See Appendix for the details of the risk model.

METRIC	HIGH-LEVEL ASSESSMENT	FINE-GRAINED ASSESSMENT
PROTECTED ASSET CRITICALITY (C)	✓	✓
EXPOSURE LEVEL (E)	✓	✓
CRYPTOGRAPHIC VULNERABILITY (V)		✓
RETENTION/LIFETIME (R)		✓
ESTIMATED WORKLOAD (W)	✓	✓



⁵ <https://quantumsafe.be/prioritise>

Real-World Example: Incumbent Telecom Operator

7.1 The PQC Journey At The Incumbent Telecom Operator

The incumbent telecom operator is a national critical infrastructure provider with long-lived data and systems. Recognising the risk that emerging quantum computers pose to its networks and encrypted data, the operator treats post-quantum cryptography (PQC) as a strategic resilience and regulatory priority.

The PQC journey at incumbent telecom operator began in 2025 as part of an initial quantum risk assessment. A 2026 requirement from the national telecommunications regulator to produce a formal PQC transition plan then acted as a catalyst, placing quantum readiness alongside the operator's other regulated risk topics.

To justify the upgrades and sequence them across asset lifecycles measured in decades, the company applied a Quantum-Safe Business Case Framework (QS-BCF), which quantifies the cost of inaction against the cost of migrating early.

The result is a phased, three-horizon roadmap:

- ★ An initial foundation phase to build inventory and skills.
(Horizon 1, through ~2027)

- ★ A domain execution phase upgrading core network, IT systems, and key infrastructure.
(Horizon 2, ~2028–2030)

- ★ A full integration phase to embed PQC throughout operations, aligned with European quantum-readiness targets.
(Horizon 3, ~2031–2035)

7.2 PQC Governance And Execution

The PQC transition is a long-term transformation. To manage this, the telecom operator has established a structured governance and programme management approach, bringing together cross-functional working groups across security, IT, network architecture, risk and compliance, and procurement. Security policies are being updated to incorporate PQC within broader security and resilience initiatives. Over time, these efforts will be further embedded into existing risk management and compliance frameworks, ensuring a sustainable and integrated approach.

7.3 Early Vendor Engagement And Hands-On Pilots

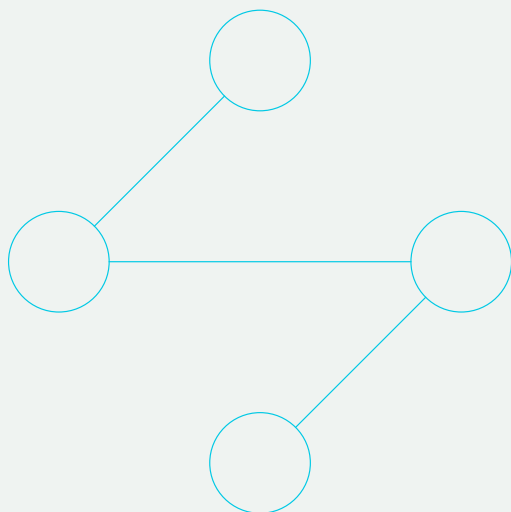
The telecom operator engaged its technology suppliers and broader ecosystem early in the process. The company is issuing quantum-readiness surveys to vendors, asking about their PQC roadmaps, dependencies, and timelines. This proactive vendor engagement informs procurement decisions, helps synchronise upgrade timelines, and encourages suppliers to accelerate their own quantum-safe product development.

The operator is also planning to run proof-of-concept projects, deploying hybrid cryptography (mixing classical and PQC algorithms) in controlled environments to validate the performance of new algorithms and to assess readiness of vendor products and infrastructure components.

7.4 Measuring Maturity And Progress

The telecom operator created a Quantum-Safe Readiness Model (QSRM) as a structured maturity framework to measure and manage its PQC programme. The model evaluates readiness across six dimensions: (1) strategic awareness and leadership commitment, (2) governance and organisational ownership, (3) cryptographic visibility and inventory, (4) vendor and supply-chain readiness, (5) technical capability and crypto-agility, and (6) change readiness and workforce enablement. Each dimension is assessed against four cumulative maturity levels, progressing from Level 1, Ad hoc/Reactive, through Level 2, Aware/Scoping and Level 3, Structured/Planning, to Level 4, Integrated/Executing.

This model serves as a sequencing tool to ensure foundational capabilities are in place before large-scale execution. In practice, QSRM assessments help the telecom operator confirm that critical prerequisites (such as strong internal governance structures and a comprehensive cryptographic inventory) are established before embarking on major migrations or upgrades. By periodically re-evaluating its maturity, the telecom operator can objectively track progress over time, support executive reporting, and align programme milestones with external deadlines.



7.5 Transferable Lessons

The company's journey shows that making critical infrastructure quantum-safe is a multi-faceted effort requiring strategic planning, cross-functional cooperation, targeted experimentation, and industry collaboration.

* Strong internal governance & executive sponsorship

Executive buy-in ensures sustained funding and attention, making PQC a board-level topic rather than an isolated technical project. By securing early support from leadership and embedding PQC into risk and compliance reporting, the telecom operator helped to align organisational priorities with long-term security needs.

* Cross-functional programme structure

The operator's approach relies on central coordination and draws on expertise from cybersecurity, network engineering, IT architecture, legal/regulatory and procurement teams. This ensures holistic planning and execution, recognising that PQC spans cryptographic upgrades, IT systems, business risk and vendor coordination.

* Phased approach with pilots

Starting with cryptographic inventory and quantum risk assessments, the telecom operator has identified critical assets with long confidentiality requirements and lengthy upgrade timelines. Small-scale pilots (e.g. exploring hybrid TLS implementations in non-production or limited-scope environments) provide vital lessons before broad rollout.

* Vendor engagement & standards alignment

Recognising the importance of the supply chain, the telecom operator engages vendors early to evaluate their PQC readiness and influence their decisions on implementing quantum-safe algorithms.

What's Next?

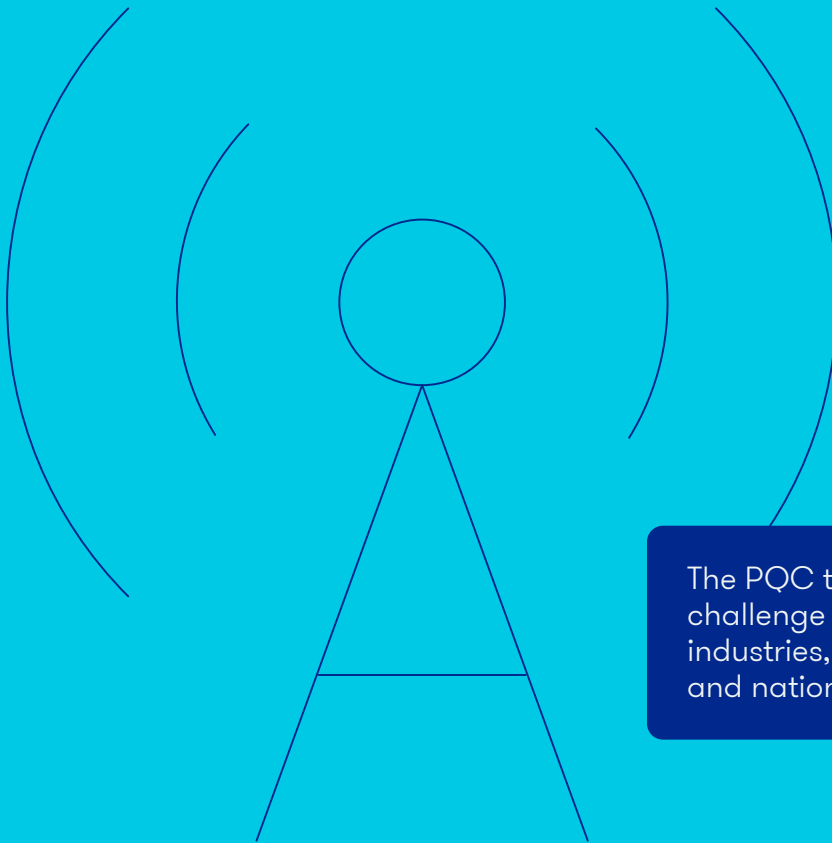
The transition to post-quantum cryptography is no longer a future consideration — it is an active, industry-wide transformation that must begin now. Regulatory momentum, ecosystem initiatives, and early adoption efforts across sectors such as telecom, finance, and government are rapidly converging. Organisations that delay run the risk of falling behind, both in compliance and in their ability to protect long-lived data and critical systems against future quantum threats. The next step is therefore clear: move from awareness and planning into structured execution.

While this volume has focused on governance, programme structure, and financial planning, the next volume provides the technical guidance required to operationalise the transition. It addresses how to implement PQC in practice — covering cryptographic inventory, crypto-agility, hybrid migration strategies, TLS and PKI evolution, and the practical challenges of deploying post-quantum algorithms in real-world environments.

The next step is clear: move from awareness and planning into structured execution.



Ultimately, organisations that take action now will not only mitigate quantum-related risks but also strengthen their overall cybersecurity posture. By investing in PQC readiness, they enhance resilience, improve cryptographic governance, and build trust with customers, partners, and regulators. The journey ahead is complex, but with the right governance foundation and a clear path towards technical implementation, it becomes a manageable — and strategically valuable — transformation.



The PQC transition is a collective challenge that spans industries, supply chains, and national boundaries.



Collaboration & Continuous Learning

The PQC transition is not an isolated effort. It is a collective challenge that spans industries, supply chains, and national boundaries. Organisations are encouraged to actively participate in industry groups and knowledge-sharing forums such as the Quantum Circle and the Cyber Security Coalition.

Sharing experiences from pilots, aligning on best practices, and contributing to open tools or training initiatives will accelerate progress for all. In practice, sectors such as telecom, banking, and government can benefit significantly from mutual learning and coordinated approaches.

External Guidance

PQC Migration Handbook

* <https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook>

Official AIVD publication providing practical guidance for organisations to mitigate quantum-computing risks to cryptography and structure a PQC migration programme.

PQC Migration Framework Marin Ivezić/Applied Quantum

* <https://pqcframework.com>

Open-access practitioner framework for enterprise-wide PQC migration, covering governance, cryptographic inventory/CBOM, risk-prioritised roadmaps, pilots, and vendor governance. The framework covers eight phases, plus cross-cutting concerns, with sector extensions for financial services, payments, telecommunications, critical infrastructure and OT, government and defence, and digital assets.

Framework Cryptography Policy For The Central Government

* <https://www.nldigitalgovernment.nl/document/framework-cryptography-policy-for-the-central-government>

Dutch Digital Government framework for drafting cryptography policy, relevant as a governance template for embedding cryptography processes, architecture principles, and implementation requirements into enterprise policy.

Framework For Estimating The Costs Of Migrating To PQC

* <https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-forum-digital-infrastructure-resilience-cfdir>

This paper was developed to provide collective insight into the costing factors which are already present for a successful quantum-safe migration.

Citi Quantum Readiness Survey

* <https://www.citibank.com/tts/surveys/2025/2362659-quantum-readiness/form.jsp>

Citi supplier questionnaire capturing vendor PQC awareness, migration plans, algorithm support, deprecation timelines, certification plans, and testing readiness; useful as a practical model for third-party quantum-readiness assessments.

PQC Maturity Model PKI Consortium

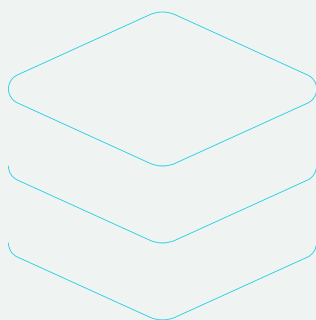
* <https://pkic.org/wg/pqc/pqcm>

A vendor-facing framework defining six maturity levels (0–5) for post-quantum cryptography adoption in products and services — helping organisations assess supply-chain readiness during procurement.

The QRAMM Assessment Toolkit

* <https://qramm.org/toolkit-overview.html>

Comprehensive Excel-based tool for evaluating organisational quantum readiness across 120 questions with automated scoring, dynamic visualisations, and compliance mapping to 8 major frameworks.



Acronyms

AES	Advanced Encryption Standard
API	Application Programming Interface
BIPT	Belgian Institute for Postal Services and Telecommunications
CCB	Centre for Cybersecurity Belgium
CBOM	Cryptography Bill of Materials
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CRA	Cyber Resilience Act
CTO	Chief Technology Officer
DORA	Digital Operational Resilience Act
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie–Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
GRC	Governance, Risk Management and Compliance
HSM	Hardware Security Module
IAM	Identity and Access Management
IT	Information Technology
KPI	Key Performance Indicator



NIS2	Network and Information Systems Directive 2
OT	Operational Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMO	Programme Management Office
PQC	Post-Quantum Cryptography
QS-BCF	Quantum-Safe Business Case Framework
QSRM	Quantum-Safe Readiness Model
RACI	Responsible, Accountable, Consulted and Informed
RSA	Rivest–Shamir–Adleman
SBOM	Software Bill of Materials
SDLC	Software Development Life Cycle
SFTP	Secure File Transfer Protocol
TLS	Transport Layer Security

Appendix

This model provides a structured methodology for prioritising asset migration to PQC. It evaluates the characteristics and risk profile of individual assets and supports two calculation approaches, enabling organisations to select the level of assessment granularity appropriate to their environment. The resulting score ranges from 0 to 1, where higher values indicate greater urgency for migration. While the model is designed as a broadly applicable framework suitable for most enterprise environments, it can be customised to reflect organisation-specific risk factors, operational requirements, and migration priorities.

Asset Classification

Exposure Level (E)

Internet-exposed systems are at higher risk of ‘harvest now, decrypt later’ and ‘trust now, forge later’ attacks.

Public exposure	(1.0)
Partner-accessible	(0.7)
Internal exposure	(0.4)

Protected Asset Criticality (C)

This metric captures the sensitivity or criticality of the data that is protected by the cryptography.

Public data	(0.1)
Internal operational	(0.4)
Intellectual Property	(0.7)
PII (personal data)	(0.85)
Business-critical software or firmware	(0.85)
Financial data	(0.9)
Legal or contractual records	(0.9)
Medical / health data	(0.95)
Highly sensitive (defence, auth secrets, crypto keys)	(1.0)

Estimated Workload (W_i)

< 1 month [0.5]

1 – 3 months [0.6]

3 – 6 months [0.7]

6 – 12 months [0.8]

12 – 18 months [0.9]

> 18 months [1.0]

Cryptographic Vulnerability (V_i)

RSA 1024 [1.0]

RSA 2048 [1.0]

RSA 3072 [0.9]

RSA 4096 [0.8]

ECDHE P-256 [0.95]

ECDHE P-384 [0.9]

ECDHE P-521 [0.8]

RSA Signatures 1024 [0.9]

RSA Signatures 2048 [0.8]

RSA Signatures 4096 [0.7]

ECDSA P-256 [0.8]

ECDSA P-384 [0.7]

Ed25519 [0.8]

Ed448 [0.7]

TLS (RSA Key Exchange) [1.00]

TLS (ECDHE P-256) [0.95]

TLS (ECDHE P-384) [0.9]

AES-128 [0.30]

Where a single device or process holds several cryptographic assets:
 $V = \text{MAX}(\text{vulnerability of the different cryptographic assets})$

Retention Period (R) Or Asset Lifetime

This metric captures the temporal exposure of an asset to quantum threats. Retention periods primarily influence ‘harvest now, decrypt later’ risk, as data requiring long-term confidentiality may be decrypted before the end of its confidentiality lifetime. Asset lifetime primarily influences ‘trust now, forge later’ risk, as long-lived assets that are not migrated or rotated before the advent of cryptographically relevant quantum computers become vulnerable to forgery.

For Data Retention

< 1 year (0.4)

1–5 years (0.7)

> 5 years (1.0)

For Asset Lifetime

Replacement or end-of-life before 2030 (0.4)

Replacement or end-of-life before 2035 (0.7)

Replacement or end-of-life after 2035 (1.0)

Risk Score

The total risk score can be computed by selecting the relevant criteria and applying a weight to each criterion. Whichever approach is chosen, it must meet the following conditions:

Factors ≥ 0 and ≤ 1 , the higher the factor, the more important

The total sum of the weights needs to be 1

The output range ≥ 0 and ≤ 1 , higher means migrate earlier

Once the score has been calculated, it can be mapped as follows:

SCORE RANGE	PRIORITY LEVEL	ACTION
0.80 – 1.00	Critical	Immediate migration
0.60 – 0.79	High	Plan in next phase
0.40 – 0.59	Medium	Include in roadmap
< 0.40	Low	Monitor/defer

EXAMPLES

Internet-Exposed Website Showing Public Data

When using a simple metric for PQC migration:

$$\text{Priority} = (0.5 \times C) + (0.3 \times E) + (0.2 \times W)$$

$$C = 0.1 \quad (\text{Public data})$$

$$E = 1.0 \quad (\text{Public exposure})$$

$$W = 0.5 \quad (\leq 1 \text{ month due to changing TLS configuration, testing compatibility})$$

$$\begin{aligned} \text{Priority} &= (0.5 \times 0.1) + (0.3 \times 1.0) + (0.2 \times 0.5) \\ &= 0.45 \end{aligned}$$

→ **INCLUDE IN ROADMAP**

Patient Record System Is Exchanging Medical Data Via TLS API

When using a more fine-grained approach for PQC migration:

$$\text{Priority} = (0.3 \times C) + (0.2 \times E) + (0.2 \times V) + (0.15 \times R) + (0.15 \times W)$$

$$C = 0.95 \quad (\text{Medical/health data})$$

$$E = 1.0 \quad (\text{Public exposure})$$

$$V = 0.95 \quad (\text{Uses ECDHE with P-256 + AES-128 TLS})$$

$$R = 1.0 \quad (10 \text{ years})$$

$$W = 0.7 \quad (3\text{--}6 \text{ months — compatibility with legacy systems})$$

$$\begin{aligned} \text{Priority} &= (0.3 \times 0.95) + (0.2 \times 1.0) + (0.2 \times 0.95) + (0.15 \times 1) + (0.15 \times 0.7) \\ &= 0.93 \end{aligned}$$

→ **IMMEDIATE MIGRATION**

Digitally Signed Vehicle Firmware

When using a more fine-grained approach for PQC migration:

$$\text{Priority} = (0.35 \times C) + (0.15 \times E) + (0.15 \times V) + (0.25 \times R) + (0.1 \times W)$$

$$C = 0.85 \quad (\text{Business-critical firmware})$$

$$E = 1.0 \quad (\text{Public exposure})$$

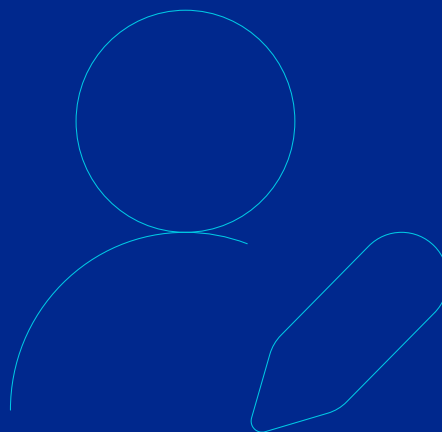
$$V = 0.8 \quad (\text{RSA 2048 signature})$$

$$R = 1.0 \quad (\text{End-of-life not expected before 10 years})$$

$$W = 0.9 \quad (\text{Design, implementation, validation, and rollout phases})$$

$$\begin{aligned} \text{Priority} &= (0.35 \times 0.85) + (0.15 \times 1.0) + (0.15 \times 0.8) + (0.25 \times 1.0) + (0.1 \times 0.9) \\ &= 0.91 \end{aligned}$$

→ **IMMEDIATE MIGRATION**



Team

This white paper is the result of a collaborative effort, bringing together expertise from the Belgian Cyber Security Coalition, the Quantum Circle, and the Centre for Cybersecurity Belgium (CCB). It has been produced to the best of the contributors' abilities.

Development Team

Sarah Ampe

Manager Digital Risk
EY

Charles De Paepe

Consultant Digital Risk
EY

Dimitri Plaisier

Chapter Owner System Architects
Proximus Group

Joachim Vererfven

Solutions Engineer
Proximus Group

Johan Kestens

Architect/Product Owner
Link2Trust

Werner Vermeylen

CISO
Klarrio

Expert Reviewers

Peter Spiegeleer

Enterprise Security Architect
Proximus Group

Jelle Wieme

Cybersecurity Engineer
CCB

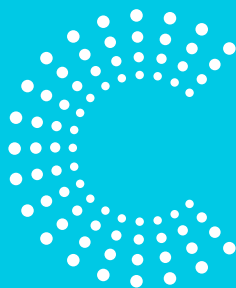
Julio Gonzalez-Saenz

Consultant
InnoQlar

Marin Ivezić

CEO
Applied Quantum





CYBER SECURITY **COALITION**

The mission of the Cyber Security Coalition is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem. We do so by bringing together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform aimed at fostering information exchange, operational peer-to-peer collaboration, making recommendations for more effective policies and guidelines, and finally carrying out joint awareness-raising campaigns aimed at citizens and organisations. More than 1,700 representatives of our 220+ member organisations participate in our activities and as such contribute to our mission.

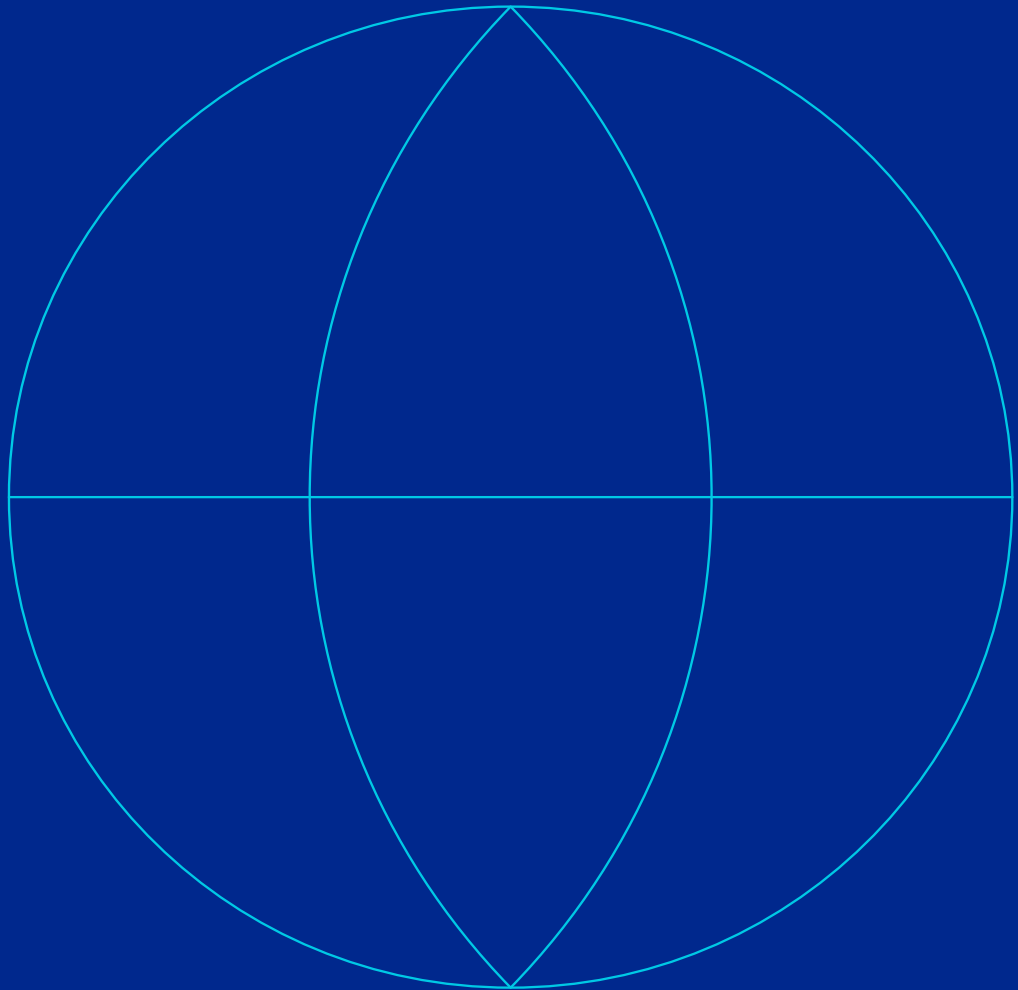
cybersecuritycoalition.be



quantum circle

The Quantum Circle is a community uniting quantum enthusiasts and experts to engage with the market on revolutionary technology, collaborate on distinguished industry use cases and applications, accelerate market adoption, shaping a visionary investment landscape with societal and economic impact.

quantumcircle.eu



Publication Date

October 2026

Contact

Cyber Security Coalition

Henk Dujardin
CEO

+32 (0)475 84 00 42
henk.dujardin@cybersecuritycoalition.be

Quantum Circle

Jan Sonck
Quantum Ecosystem Manager

+32 (0)478 34 53 69
jan.sonck@quantumcircle.eu