nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

2026 LUXEMBOURG GRC SUMMIT
powered by NC3

IS THE PQC TRANSITION A CRITICAL STEP FOR RESILIENCE, OR DOES IT STIR MORE CONCERN THAN ACTUAL DANGER?

OUTCOME PAPER

Key insights and recommendations from the Luxembourg GRC Summit 2026 forum on the PQC transition, outlining how organisations can assess their exposure to quantum threats and prioritise practical steps towards PQC readiness.

Table of contents

3	Summary
4	The Quantum Challenge to Digital Trust
5	Future Quantum Threat, Current Exposure
5	What is Holding Back PQC Readiness?
6	From Technical Awareness to Organisational Readiness
7	Building a Practical PQC Migration Strategy
10	Regulatory Momentum and The Need for Practical Guidance
10	Key Takeaways
11	Recommendations and Action Points

IS THE PQC TRANSITION A CRITICAL STEP FOR RESILIENCE, OR DOES IT STIR MORE CONCERN THAN ACTUAL DANGER?

Summary

This paper summarises the outcomes of the forum “Is the PQC transition a critical step for resilience, or does it stir more concern than actual danger?”, held during the second edition of the Luxembourg GRC Summit on 3rd and 4th of June 2026. The Summit brought together Cybersecurity Governance, Risk and Compliance (GRC) professionals, practitioners and decision-makers to exchange knowledge, examine emerging threats, and explore evolving practices in the field.

The forum focused on the challenge of preparing for post-quantum cryptography (PQC) while the timeline of the quantum threat remains uncertain. Although sufficiently powerful quantum computers are not yet available, the potential impact of such systems on widely used public-key cryptography is already known, and migration will require time, coordination and investment.

The discussion therefore centered on how organisations can assess their current exposure and determine when actions are justified and how they should be prioritised, while avoiding both complacency and overreaction. Discussions explored how organisations can build awareness across all levels of an organisation and, even more importantly, how organisations can turn this awareness into readiness through practical steps and make informed decisions regarding their PQC migration strategy.

The Quantun Challenge to Digital Trust

01

Cryptography is fundamental to a large part of today's digital infrastructure. It protects communications and transactions, supports authentication and digital signatures, and secures stored data. Public-key algorithms such as RSA and ECC (Elliptic-curve cryptography) have been relied upon for decades and are deeply embedded in technologies ranging from Public Key Infrastructure (PKI) and identity management to software signing, cloud services and financial systems.

Quantum computing challenges this long-standing model. Since Shor's algorithm was published in 1994, it has been known that a sufficiently capable quantum computer could break widely used public-key cryptographic schemes such as RSA and ECC. At the same time, substantial work has been undertaken to develop alternatives designed to resist quantum attacks. This has already resulted in the standardisation of the first post-quantum cryptographic algorithms by NIST.

The challenge is therefore no longer to determine whether quantum computing will affect current cryptography, but how and when organisations should prepare for that transition.

The timeline for a cryptographically relevant quantum computer remains uncertain, while replacing cryptographic mechanisms across complex digital environments can take years. This creates a difficult balance between acting early enough to reduce future exposure and avoiding poorly planned or premature migration.

The migration to post-quantum cryptography also goes beyond replacing one algorithm with another. Cryptography is embedded in certificates, identities, software signatures, devices and infrastructure, communications, and applications, often with strong dependencies between them. Moving to PQC therefore affects the wider digital trust infrastructure and raises technical, operational and governance questions. It should ultimately be approached as not only a cryptography challenge, but as a broader issue of digital infrastructure resilience.

Future Quantum Threat, Current Exposure

02

The PQC transition should be approached as a long-term resilience effort rather than as a reaction to an immediate crisis. The central difficulty is that the exact timeline of the quantum threat remains uncertain, while the preparation needed to address it cannot be postponed indefinitely. Organisations therefore need to begin planning before quantum attacks become operational.

A key reason is the *harvest now, decrypt later* scenario. Attackers may collect encrypted information today and retain it until sufficiently capable quantum computers become available. This creates a present exposure for data that needs to remain confidential over long periods, such as state or defense information, health records, intellectual property, sensitive corporate information, and data related to critical infrastructures.

The risk may therefore materialise only in the future, while the exposure already exists. This makes PQC relevant today, particularly for organisations holding information with long-term confidentiality requirements. The objective is thus not to replace all existing cryptography immediately, but to understand where exposure is highest and begin reducing it in a controlled and prioritised way.

PQC migration should be integrated into long-term cyber resilience planning. Organisations need to identify which data and systems require earlier protection, assess how long migration is likely to take, and plan the transition progressively rather than waiting for the quantum threat to become immediate.

What Is Holding Back PQC Readiness?

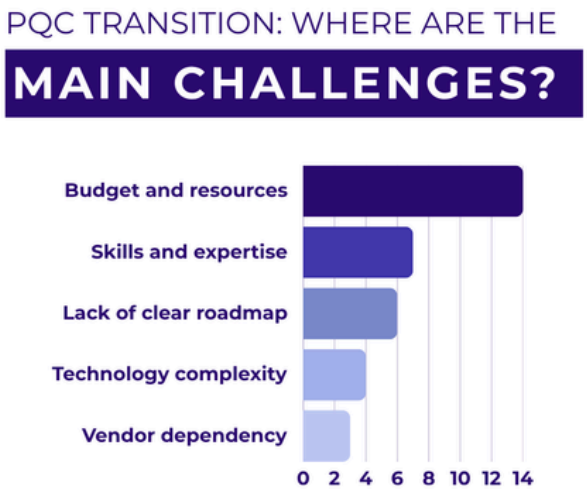
03

Awareness of post-quantum cryptography is increasing, but this has not yet translated into operational readiness. The PQC Readiness Survey[1] conducted by LHC (Luxembourg House of Cybersecurity) and LuxQuantum in 2025 reflects this gap: around 92% of respondents were aware of PQC, while around 56% had not yet integrated quantum-related risks into cybersecurity

[1] https://observatory.nc3.lu/media/reports/PQC_Readiness_Survey_Report_2.pdf

awareness training and their risk management processes. Many organisations therefore still appear to be in a discovery phase, where the issue is recognized but concrete preparation remains limited.

Among the main obstacles to PQC readiness, insufficient budget and resources was identified as a major obstacle by forum participants. Shortages in skills and expertise, as well as unclear roadmaps and migrations strategies were also identified as significant challenges, while technology complexity and vendor dependency were also mentioned by a few participants. Moreover, responses to the PQC Readiness Survey highlighted additional challenges, including namely limited visibility into cryptographic assets and dependencies, incomplete inventories and prioritisation, uncertainty around regulatory expectations and timelines, as well as limited testing capabilities. These challenges provide the starting point for the practical discussion on how organisations can prepare and where action should begin.



Responses from forum participants to the question "What is the biggest obstacle to your organization's PQC readiness today?" (34 respondents).

While awareness of the quantum threat already exists across organisations, these figures highlight that the main challenge might be turning this awareness into action.

PQC migration should be treated as more than a cryptographic upgrade. It is also a governance, operational resilience and change management exercise affecting the overall digital trust infrastructure.

From Technical Awareness to Organisational Readiness

04

One reason the PQC preparation remains limited is that the threat is still perceived as distant. Organisations need to make decisions today about a risk whose exact timeline remains uncertain, while other cybersecurity threats compete for more immediate attention and resources. Regulatory milestones

can help create a clearer sense of direction, but internal awareness is still needed to turn the issue into concrete action.

This awareness needs to exist at different levels of the organisation. Senior management needs to understand the potential business and resilience impact well enough to allocate resources. For CISOs and other security leaders, this means translating quantum risk into business terms rather than presenting PQC only as a technical problem. Potential losses, disruption, long-term data exposure and migration costs can help management understand why preparation is needed before the threat becomes immediate. Meanwhile, other operational functions such as IT, development, procurement and other relevant business units need to understand how the transition may affect their systems and processes. Scenario-based exercises can help make the issue more concrete.

The forum did not suggest that every security professional needs to become a cryptographer; organisations only need sufficient expertise to understand their exposure, configure solutions correctly, assess trade-offs, challenge suppliers and manage the migration. Where specialized cryptographic knowledge is required, external expertise can complement internal capabilities. ***The main objective is to build enough understanding across the organisation to support informed decisions and sustained preparation.***

Building a Practical PQC Migration Strategy

05

5.1. A Risk-based Approach to PQC Migration

PQC migration should not treat all systems and data as equally urgent. Organisations need to prioritise based on exposure, criticality, data lifetime and the potential impact if the cryptography protecting a system were to fail. ***The objective is not to migrate everything immediately, but to identify where early action will reduce the most risk.***

Priority should therefore be given to systems and data that are long-lived, high-value, highly exposed or business-critical. Dependencies also need to be taken into account. A system that appears relatively low-risk in isolation may support a much more critical service, making its actual importance higher than a simple asset-level assessment would suggest. Organisations should also consider how difficult a system will be to change,

particularly where legacy architecture or vendor dependency limits migration options.

5.2. Cryprographic Inventory as a First Step

A practical first step towards PQC readiness is to build a cryptographic inventory. Organisations cannot plan a migration if they do not know where cryptography is used, which algorithms are in place, which systems depend on them and how critical those systems are.

The inventory should cover the main areas where cryptography is used across the organisation, including business applications, infrastructure components, PKIs, HSMs, key management systems, certificates, digital signatures, encrypted communications, code signing, S/MIME, APIs, cloud services, CI/CD pipelines, supplier-managed systems and legacy environments. It should also identify the algorithms in use and classify systems according to their criticality, exposure and migration constraints.

Mapping dependencies is particularly important. Cryptographic components are often shared across several systems, and a service that appears relatively low-risk on its own may support a much more critical system.

A reliable inventory therefore provides the basis for identifying priorities, understanding migration dependencies, and making informed decisions for building a realistic PQC roadmap.

5.3. Managing PQC Risk Across the Supply Chain

Many organisations depend heavily on vendors for their PQC readiness. They do not directly control the cryptographic implementation used in cloud services, business applications, smartcards, HSMs, managed services or other third-party platforms. This creates both a technical dependency and a procurement challenge.

Organisations should not assume that suppliers will become quantum-safe within the timeframe they require. Procurement decisions made today can also create future migration debt if products are not designed for crypto-agility or if vendors do not provide a transition roadmap. Supplier discussions should therefore address issues such as planned support for PQC or hybrid cryptography, applicable standards, testing and certification, migration timelines, and the respective responsibilities of the vendor and the customer.

PQC readiness should consequently be integrated into third-party risk management and procurement processes. Vendor questionnaires, contractual requirements, certification and evidence of crypto-agility can help organisations assess whether suppliers are prepared for the transition and avoid introducing new dependencies that will be difficult to migrate later.

5.4. Legacy Systems Require Tailored Migration Strategies

Legacy systems are likely to be one of the most difficult parts of the PQC transition. Many were designed around fixed cryptographic choices and may rely on outdated libraries, protocols or vendor-managed components that are difficult to modify. In some cases, cryptography is tightly integrated into the system architecture, making a straightforward algorithm replacement difficult or impossible.

Organisations should therefore identify legacy systems early and assess which ones can be upgraded, which require temporary protection measures, and which may ultimately need to be replaced. Isolating higher-risk systems, placing protective components or proxies in front of them, upgrading individual components gradually or using hybrid cryptographic approaches where appropriate are a few examples of possible temporary measures.

These interim measures can reduce short-term exposure and provide additional time for migration, but they do not remove the underlying problem. Where a legacy system cannot support quantum-resistant cryptography, organisations will eventually need a longer-term modernisation or replacement strategy.

5.5. Crypto-agility as a Design Principle

The PQC transition also provides an opportunity to avoid recreating the same migration difficulties in new systems. New applications and infrastructure should be designed so that cryptographic mechanisms can evolve without requiring major changes to the overall system.

Crypto-agility refers to the ability to replace or update cryptographic algorithms, parameters, and configurations as security requirements and standards evolve. In practice, solutions providers should avoid hard-coding algorithms, keep cryptographic configurations flexible, separate cryptographic functions from business logic where possible, and anticipate the potential need for hybrid or future cryptographic approaches.

These principles should be reflected in system architecture, secure development practices and procurement requirements. Vendors should also be able to explain how their products support cryptographic updates and provide a clear PQC transition roadmap. ***Crypto-agility should be treated as a long-term resilience capability, not simply as a technique for the current PQC migration.***

Regulatory Momentum and the Need for Practical Guidance

06

European roadmaps are helping move PQC from a future concern to a concrete migration objective. Following the Commission Recommendation of 2024, the NIS Cooperation Group adopted a coordinated EU roadmap in 2025, with milestones for starting the transition by the end of 2026, prioritizing high-risk use cases by 2030, and progressing towards broader migration by 2035.

Standards and certification guidance are also evolving. NIST has standardised the first PQC algorithms, while ENISA and EU certification work continue to refine cryptographic recommendations and implementation expectations. Luxembourg is supporting this transition through its national quantum strategy, MeluXina-Q and wider investments in quantum-safe infrastructure, skills and testing capabilities.

While these milestones and recent evolutions give organisations a clearer basis for planning and can help move PQC discussions towards decisions on resources, responsibilities and priorities, deadlines alone are not enough. Organisations still need technical roadmaps, testing capabilities, budgets, supplier support and practical implementation guidance. ***Regulation can provide direction and urgency, but long-term readiness will depend on sustained governance, coordination between public authorities, industry and academia, and guidance that organisations can translate into concrete actions.***

Key Takeaways

The forum highlighted the idea that while organisations must start considering their PQC transition now, they must not treat it as an emergency migration. While the quantum timeline remains uncertain, the transition itself will take years, and exposure already exists through scenarios such as *harvest now, decrypt later.* Waiting for complete certainty would therefore create its own risk. The appropriate response is a staged and risk-based transition, beginning with prioritisation and planning.

More than a cryptographic upgrade, the PQC transition needs to be treated as a business resilience and change-management programme. CISOs will need to translate quantum exposure into business impact, engage management

and procurement, assess supplier readiness and incorporate PQC into architecture and purchasing decisions. New systems should moreover be designed for crypto-agility and hybrid approaches to avoid future migration debt.

The main gap identified during the Forum is not awareness, but readiness and execution. A practical transition starts with actions that organisations can already take: build awareness at management and operational level, create a cryptographic inventory, identify long-life sensitive data, classify and prioritize systems, assess suppliers, test migration options, update procurement and security policies, and align the roadmap with regulatory milestones.

PQC readiness is ultimately about reducing uncertainty through structured preparation rather than waiting for the quantum threat to become immediate.

Recommendations and Action Points

01. Build and maintain a **cryptographic inventory.** Identify where cryptography is used in your systems. Record the algorithms in use, ownership, dependencies and migration constraints.

02. Classify systems and data by criticality and quantum exposure. Long-life sensitive data and business-critical systems need to be addressed first.

03. Develop a **staged, risk-based PQC migration roadmap.** Avoid treating the transition as a one-time replacement exercise.

04. Assess vendor and supply-chain readiness. Integrate this question into third-party risk management.

05. Include PQC readiness in procurement decisions now. Avoid aquiring systems that will create additonal migration debt.

06. Identify and address **legacy system constraints** early. Where immediate migration is not possible, consider **isolation, protective gateways, gradual component upgrades** or other interim controls.

07. Design **crypto-agility** into new systems. Treat crypto-agility as a long-term resilience capability.

08. Translate quantum risk into **business and resilience terms**. PQC should be presented as an organizational resilience isue rather than only a cryptographic problem to build **awareness.**

09. Establish **clear PQC governance** and ownership.

Thank you for reading. We hope these insights inform your work and encourage further dialogue on cybersecurity governance.

Thank you to our participants, Advisory Board and partners for sharing their expertise, **and to you for taking these discussions forward.**

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

IN COLLABORATION WITH

Luxembourg House of Cybersecurity

LUXEMBOURG CYBERSECURITY FACTORY