nc3
Threat Observatory
Platform

PQC READINESS SURVEY REPORT

NAVIGATING THE QUANTUM TRANSITION IN LUXEMBOURG'S ECOSYSTEM

Published by

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

Table of Contents

2026

Introduction 03

Executive Summary 05

Key Outcomes 08

Practical Steps 09

Detailed Analysis 13

Methodology 35

Introduction

The 2025 Quantum Europe Strategy identifies quantum technologies as a critical domain for Europe's economic security, technological sovereignty, and long-term competitiveness. As the global race to harness quantum capabilities accelerates, the implications extend beyond innovation leadership to the security of Europe's digital infrastructure.

Quantum computing is no longer a theoretical concern for cryptography.The potential emergence of cryptographically relevant quantum computers capable of breaking today's public-key encryption requires Europe to adopt stronger safeguards to protect sensitive communications and the long-term integrity of confidential information. The Commission explicitly acknowledges this threat and reinforces the need to transition to Post-Quantum Cryptography (PQC) as a matter of strategic urgency.

Europol Innovation Lab Observatory Report[1] talks about how Quantum computing is going to have a significant impact on password cracking. Quantum computing changes the notion of what is today considered a strong password, which may lead to longer and more complex passwords becoming widely used in the future in order to counteract quantum-based password guessing, or the wider adoption of biometric identification methods.

The European Commission formally raised the alarm in Recommendation (EU) 2024/1101[2], urging Member States to coordinate a migration to Post-Quantum cryptography (PQC) via hybrid schemes that may combine PQC with existing Cryptographic approaches or with Quantum Key Distribution (QKD). This requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

This guidance was operationalized in June 2025 with the release of the EU Coordinated Implementation Roadmap for PQC[3], which requires full adoption of PQC across European critical infrastructure by December 2030.

1 https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement

2,3 https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Introduction

The urgency reflects accelerating technical forecasts. Gartner[4] predicts that quantum hardware may render RSA, ECC (Elliptic Curve Cryptography) and similar asymmetric schemes unsafe by 2029, exposing sensitive data already being intercepted today for "harvest-now-decrypt-later" attacks. With long-lived assets, health records, financial data, industrial IP already are at risk, regulators see no buffer period left.

The EU PQC Roadmap[5] defines a clear transition path: cryptographic inventories by 2026, hybrid classical Post-Quantum deployments during 2026-2027, and full migration to approved PQC algorithms for high-risk use cases by 2030, for medium-risk use cases by 2035, and for low-risk use cases to the extent feasible.

These expectations are reinforced by broader regulatory frameworks. DORA requires robust and continuously tested cryptographic controls in the financial sector and its ICT supply chain, while NIS2 extends strong security obligations including encryption requirements across 17 critical sectors.

Although many people today do not recognize the risk, it is in fact a systemic one, which becomes critical once exploitation becomes possible.

In this report, PQC readiness refers to an organization's ability to plan, implement, and transition cryptographic systems to quantum-resistant solutions. Delayed action may result in material, financial, operational, and regulatory exposure.

Against this backdrop, the National Cybersecurity Competence Center (NC3), in partnership with LuxQuantum conducted a PQC readiness survey to evaluate Luxembourg's overall Post-Quantum maturity.

The aim was to assess ecosystem-wide awareness, readiness to PQC migration and provide guidance.

4 https://postquantum.com/industry-news/gartner-quantum-pqc/

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

Executive Summary

The objective of this survey is to provide the ecosystem with a clear view of current readiness levels and to propose practical steps organizations can take to future-proof their systems and maintain network security in the quantum era.

Overall, the findings point to an ecosystem that is broadly aware of the challenge, yet slow to translate awareness into concrete action leaving significant gaps ahead of upcoming EU PQC migration deadlines for high-risk use cases i.e. December 2030.

NC3's 2025 PQC Readiness Survey highlights the growing URGENCY of preparing for quantum-resistant cryptography.

Based on responses from over 25 cybersecurity professionals including IT leaders, CISOs, CIOs, and Executives across Luxembourg the survey reveals varied levels of maturity, differing migration timelines, and common challenges in adopting PQC standards.

Executive Summary

Strategy: Leadership Support Without Execution

Although 72% of respondents report leadership support for PQC initiatives, more than half lack a defined strategy or roadmap for migration. Only a small minority have initiated pilots or Proofs of Concept (PoC), indicating that executive awareness has not yet translated into governance structures, budgeting, or execution plans. Most organizations remain at an early stage of PQC maturity.

Inventory & Migration Readiness: Gaps in Visibility and Planning

Cryptographic inventories critical for meeting the EU's 2025 requirements are often incomplete or not yet initiated.
Only 11% of respondents have assessed which systems are most vulnerable to quantum threats, and the same proportion are currently testing or piloting PQC algorithms. Migration timelines vary significantly, with 48% unsure or expecting action only in five to ten years.

Awareness: High-Level Understanding, Limited Practical Insight

While 92% of respondents have heard of PQC and understand the general implications of quantum computing, more than half (56%) have not integrated quantum risk into training programs or risk management processes. Many organizations continue to view the threat as distant, underestimating near-term "harvest-now-decrypt-later" risks.

Regulation & Compliance: Low Readiness for What's Coming

Only a small share of respondents feel prepared for PQC-related regulatory requirements, while 72% are unaware of or uncertain about emerging EU guidance.
Against this backdrop, transitioning to PQC can support compliance efforts, particularly as frameworks such as DORA, NIS2, and the EU PQC Roadmap and National Strategy continue to encourage in this direction.

Challenges: Structural and Technical Barriers

Legacy systems, technical complexity, lack of perceived urgency, and cost are cited as the primary obstacles to PQC adoption. Skills shortages, uncertainty around standards, and limited internal ownership further slow progress, with 40% of respondents reporting no dedicated PQC owner.

Executive Summary

Workforce: Skills and Capacity Gaps

Only 24% of respondents report having in-house PQC expertise, and most organizations do not plan to hire or train staff in this area within the next 12 months. While the value of PQC training is widely acknowledged, budget constraints, skills shortages, and the absence of a clear strategy limit investment. Transition to PQC does not necessarily require hiring dedicated cryptographers organizations may also benefit from engaging experts with practical experience in implementing and managing cryptographic solutions.

Vendors & Supply Chain: Minimal Engagement

Despite heavy reliance on third parties, 52% of respondents have not assessed vendor cryptographic dependencies or engaged suppliers on PQC roadmaps. Procurement processes rarely include PQC requirements, increasing exposure to vendor-driven timelines and future integration challenges.

The survey reveals an ecosystem at the starting line: aware of the quantum threat, but lacking the visibility, structure, and capabilities required to meet upcoming EU PQC milestones.

The full report explores these findings in greater detail and outlines where organizations must act now to mitigate future security, operational, and compliance risks.

Key Outcomes

Overall, the survey indicates that Luxembourg's ecosystem remains at an early stage of PQC readiness. Accelerated action across governance, technical planning, skills development, and vendor engagement will be essential to meet EU timelines and ensure long-term digital resilience.

Practical steps

To improve PQC readiness across sectors and close the gaps, organisations should consider the following recommendations:

Develop a PQC Roadmap and Assign Ownership	Every organization regardless of industry should define a post-quantum strategy/roadmap as soon as possible and assign ownership and outline key steps and timelines. Clear governance ensures accountability, sustained progress, and alignment across security, IT, and compliance functions.
Increase Awareness and Urgency	Leadership teams should be briefed on the quantum threat timeline and the “harvest now, decrypt later” risk. PQC must be integrated into cyber resilience programs and risk management processes to ensure it is treated as a strategic priority rather than a distant technical issue. Broader awareness initiatives supported by workshops must be led by National Competence Centers, Universities, and government agencies, such as Quantum Breakfast organized by University of Luxembourg.
Conduct a Cryptographic Inventory and Risk Assessment	A comprehensive inventory of all cryptographic assets in the organization is the essential first step. Identify algorithms and key lengths used in applications, protocols, and devices and assess which systems and data would be most vulnerable if current encryption were broken. This provides the foundation for planning the migration and will be the key step to manage quantum risks.
Prioritize “High-Risk” Systems and Data	Use a risk-based approach to plan the transition just as any security project. Systems handling high risk data MUST be prioritized for early migration to PQC. By classifying data and systems by sensitivity, organizations can make better use of available limited resources.

Monitor Standards and Align with Best Practices

Compliance team MUST start keeping track of PQC standards development –for instance, the NIST PQC algorithm standards and ENISA guidelines and any industry-specific guidelines. Organizations should plan to adopt widely recommended quantum-resistant algorithms, and ensure their cryptographic libraries and vendors support them.

Engage Vendors and Strengthen Supply Chain Requirements

Proactively reach out to critical vendors (cloud providers, software suppliers, hardware manufacturers) to inquire about their PQC roadmaps and make PQC part of the regular conversations. This will encourage vendors to share their plans for supporting quantum-safe encryption.

Collaboration through industry groups or sectors can also be effective: sharing knowledge on vendor readiness and possibly coordinate requirements to apply pressure on the supply chain collectively.

Address Legacy Systems Early

Start identifying legacy systems that use hard-coded or outdated cryptographic schemes. Because legacy systems are one of the hardest challenges, tackling them sooner will reduce the risk during the transition.

Where possible, work with vendors of legacy products for updates; if they are uncooperative or no longer existent, that would strengthen the case for accelerating upgrade or change of those systems.

Consider TLS Migration as Priority [7]

TLS is the most widely used security protocol on the internet. It can secure any protocol running over TCP and is universally supported by browsers. Therefore, migrating to TLS should lead to a significant reduction in risk.
From version TLS 1.3 onward, the protocol supports Post-Quantum Cryptography (PQC). A common approach is to use a hybrid key exchange combining ML-KEM768 (FIPS 203) with X25519 (a classical elliptic curve). Large-scale implementations already exist, such as those by Cloudflare and Google Chrome. Several other browsers are also known to support PQC-enabled TLS under specific conditions.

7 TLS as a PQC Migration Opportunity- Steve Purser

Foster Cross-Sector Collaboration and Information Sharing

Improving Post-Quantum Cryptography readiness should not be approached in isolation, as inter-dependencies across sectors directly affect organizational risk. In critical sectors such as finance, government, and telecommunications, participation in industry working groups, standards bodies, and public-private partnerships enables early visibility into emerging requirements and best practices. Collaborative information sharing helps accelerate progress, align approaches, and reduce duplicated effort across the ecosystem.

Implement “Crypto-agility” as a Strategic Principle

Organizations should adopt crypto-agility by designing systems that can update cryptographic algorithms over their lifetime, enabling a smooth transition to secure Post-Quantum solutions. This requires planning for future updates through modular cryptographic libraries, avoiding hard-coded algorithms, and using hybrid classical Post-Quantum approaches during the transition.

Hybridation

Hybridation involves combining Post-Quantum asymmetric algorithms with well-established pre-quantum cryptography based on factorization or discrete alogarithms. As emphasized by ANSSI and other authorities, hybrid approaches remain necessary in the short to medium term, as Post-Quantum algorithms alone are not yet sufficiently mature and have previously been subject to classical attacks.
This position is shared by other European agencies, including BSI, which has reaffirmed the need for hybridation in its updated technical guidelines on cryptographic mechanisms.

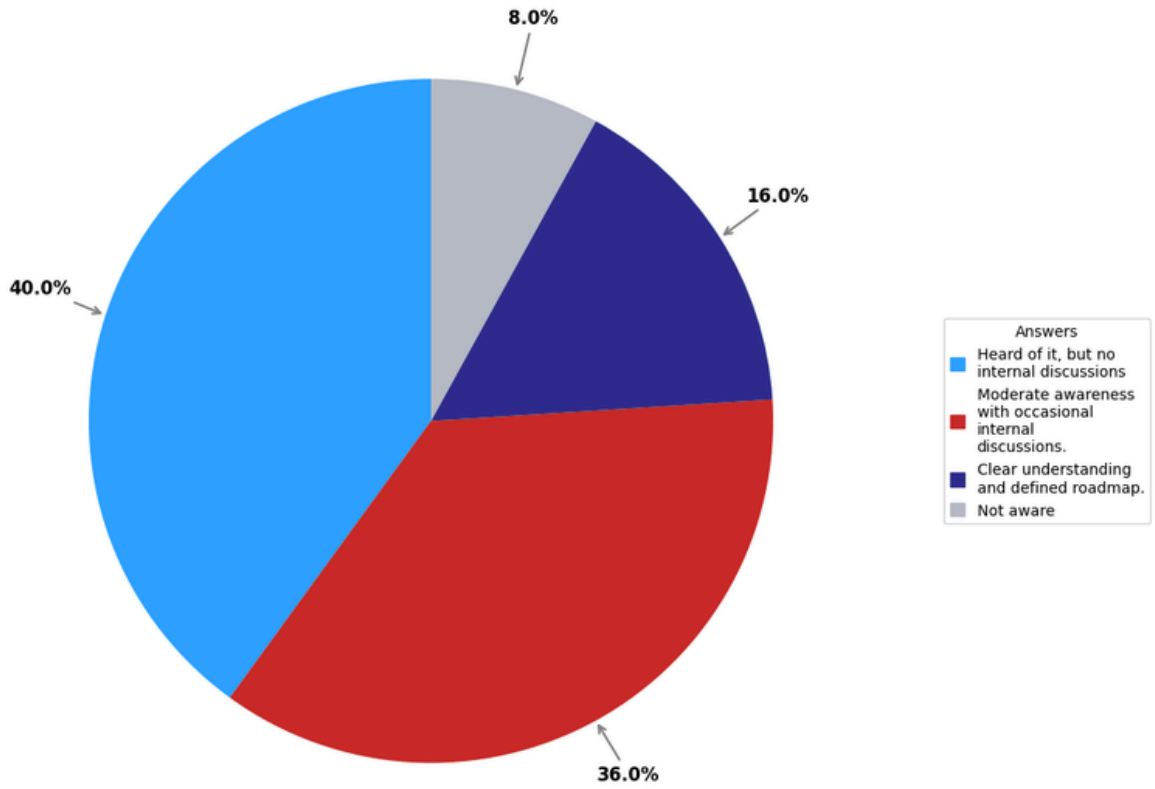
Build Internal PQC Expertise

Organizations should address the Post-Quantum cryptography skills gap by upskilling existing staff, hiring specialized talent, or leveraging external expertise. This includes providing targeted training through vendors or service providers, and where feasible, engaging cryptography experts or specialized consulting firms.
When full-time hiring is not practical, partnerships with external specialists and National Cybersecurity Competence Centers can provide critical guidance, ensuring PQC implementation is well understood and not treated as a “black box” upgrade.

Detailed Analysis

AWARENESS

How familiar is your organization with Post-Quantum Cryptography (PQC)?

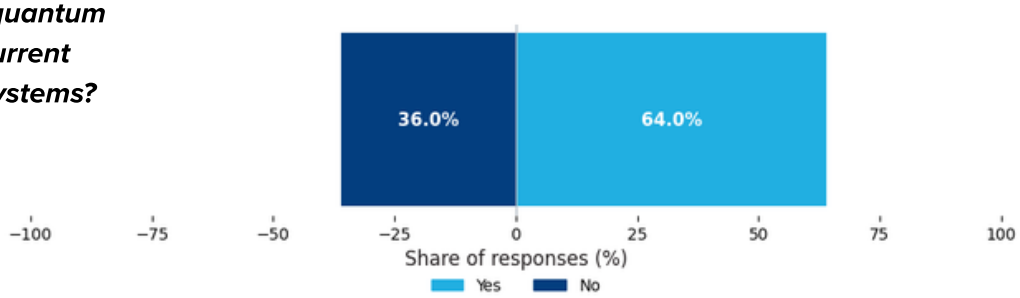


92 %

have heard of PQC, some have internal discussions on the topic and some have more active action plans.

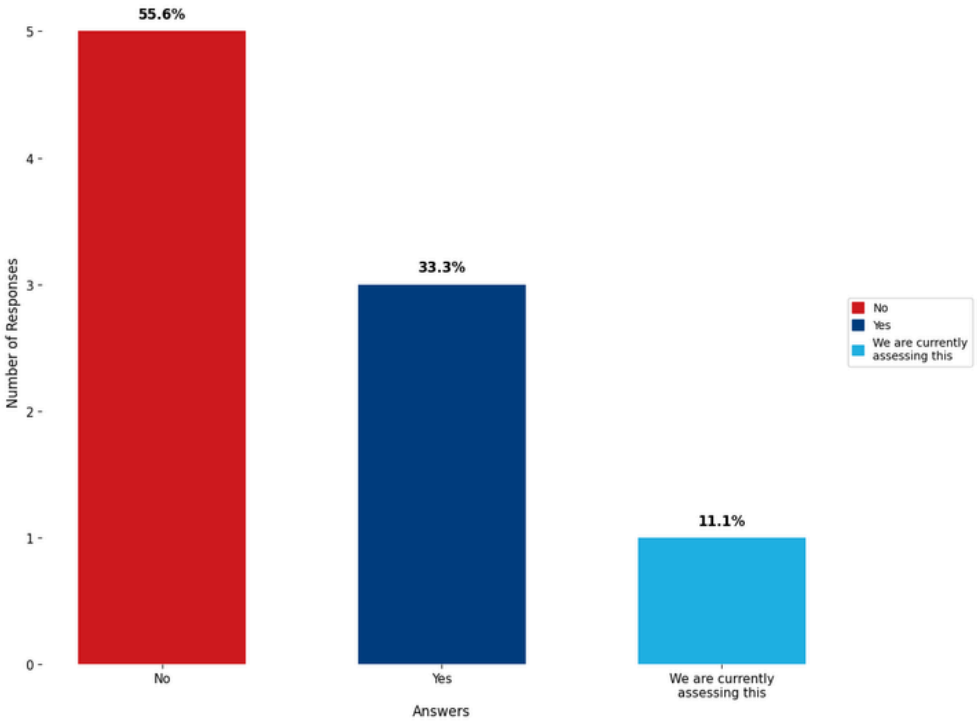
Organizational awareness of post-quantum cryptography varies significantly. While 40% of respondents indicated that they have heard of PQC but have not initiated internal discussions, 36% reported a moderate level of awareness with occasional internal conversations. Only 16% of respondents demonstrated a clear understanding supported by a defined roadmap, whereas 8% reported no awareness of PQC at all.

Are your technical teams aware of the implications of quantum computing on current cryptographic systems?



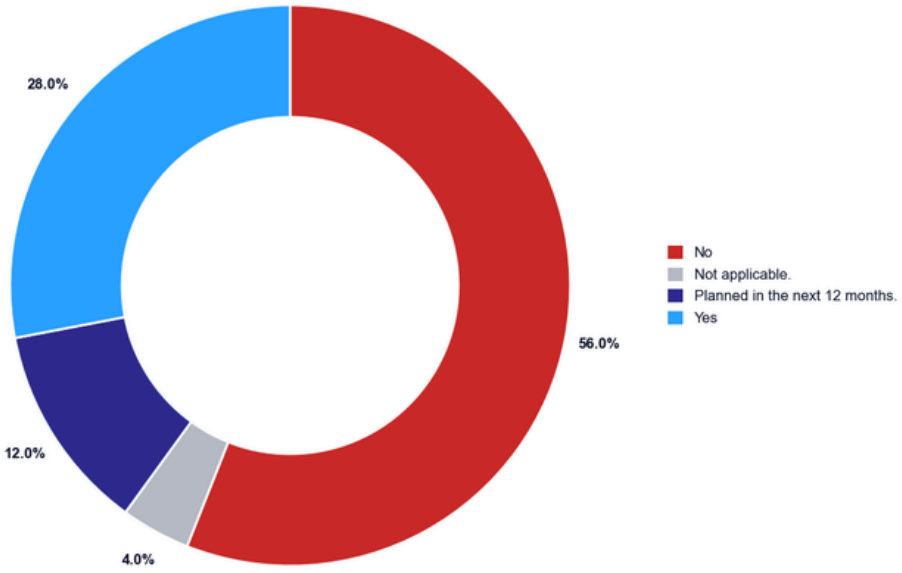
64 % of respondents shared their technical teams are aware of the implications of quantum computing on current cryptographic systems.

Do you know which of your current cryptographic systems (e.g., TLS, VPNs, PKI, blockchain) are vulnerable to quantum attacks?



33 % of respondents are aware of which of their current cryptographic systems (e.g., TLS, VPNs, PKI, blockchain) are vulnerable to quantum attacks. 56% of respondents said No and 11% of respondents are still assessing to identify the cryptographic systems.

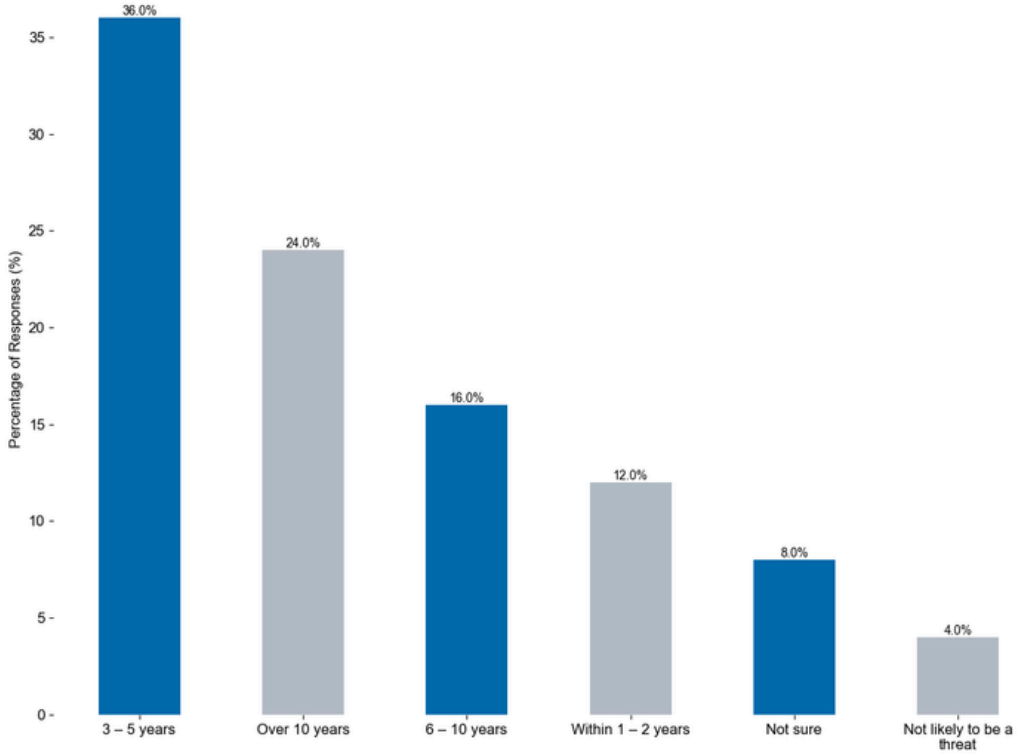
Has PQC or quantum risk been included in your organization's security awareness training or risk management?



56 %

Of respondents have not included Quantum risk in the organizational Training and risk management. 28% have included quantum risk in organizational training and risk management and another 12% have planned in the next 12 months. 4% of respondents think it is not applicable.

When do you believe quantum computers will pose a real-world threat to currently deployed cryptography?



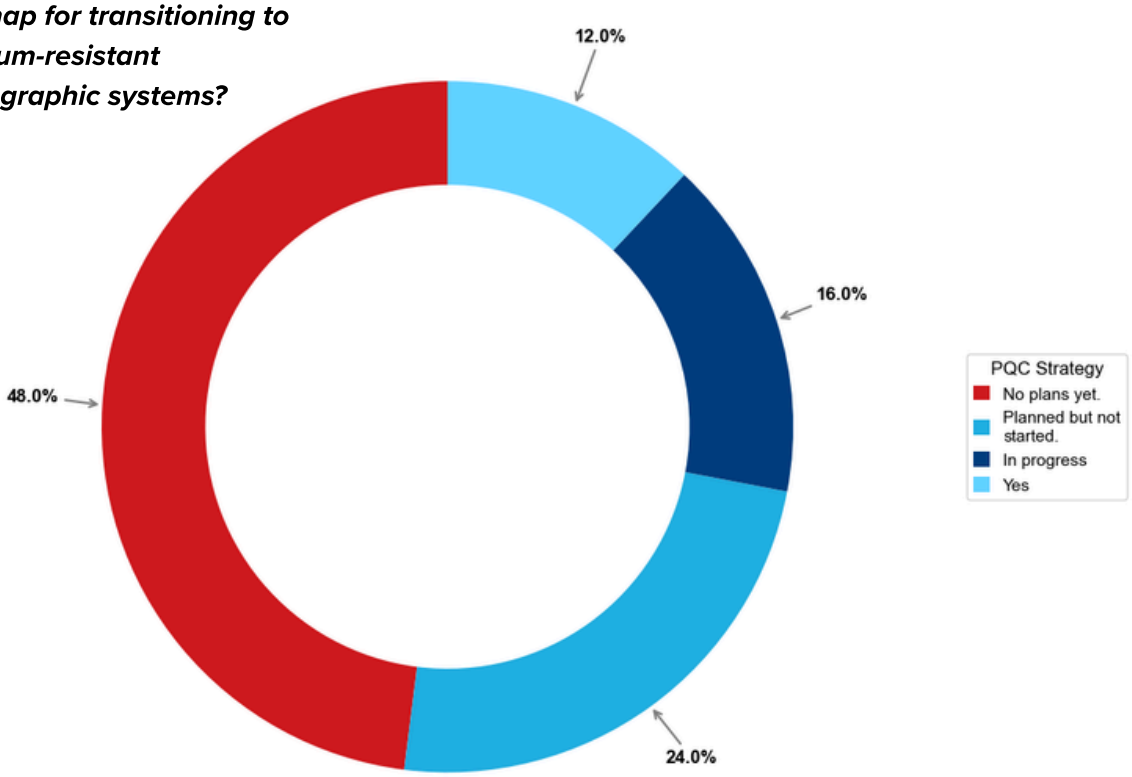
40 %

believe quantum computers will pose a real-world threat to currently deployed cryptography over 5 years.

A minority of respondents foresee quantum attacks on current cryptography as an imminent concern. In contrast majority of the respondents view it as a more distant problem. 16% of respondents have responded 6 to 10 years and 24% of respondents have responded over 10 years. 8% not sure. 4 % of respondents think not likely to be a threat, 12 % of respondents think within 1 to 2 years and 36 % of respondents think 3 to 5 years.

STRATEGY

Has your organization developed a strategy or roadmap for transitioning to quantum-resistant cryptographic systems?



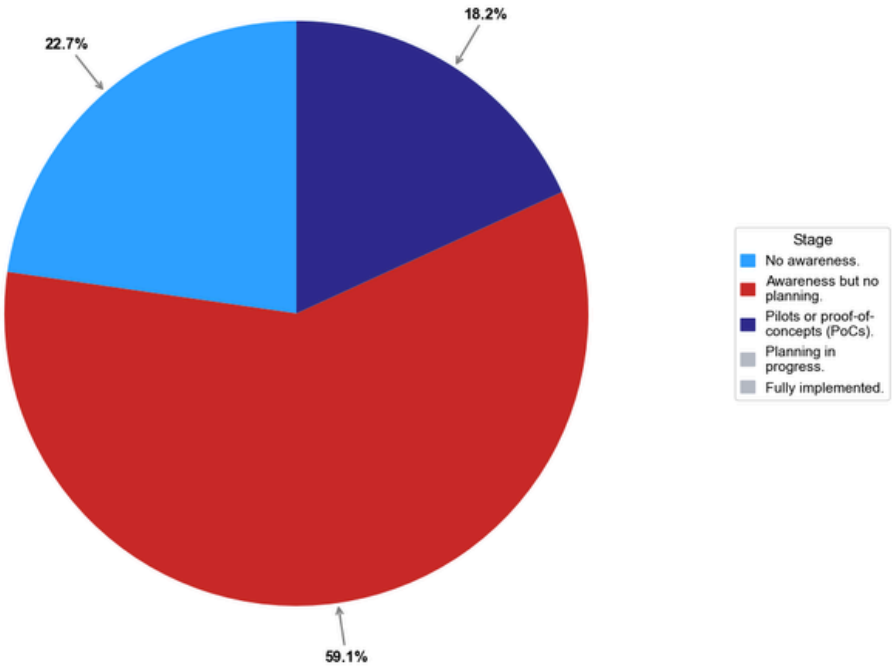
48 %

have not developed a strategy or roadmap for transitioning to quantum resistant cryptographic systems.

12% respondents shared they have a strategy or roadmap for the transitioning to quantum resistant cryptographic system. 24 % have also planned and not started yet. 16% of the respondents are in progress. This is a clear lack of formal PQC strategy or roadmap.

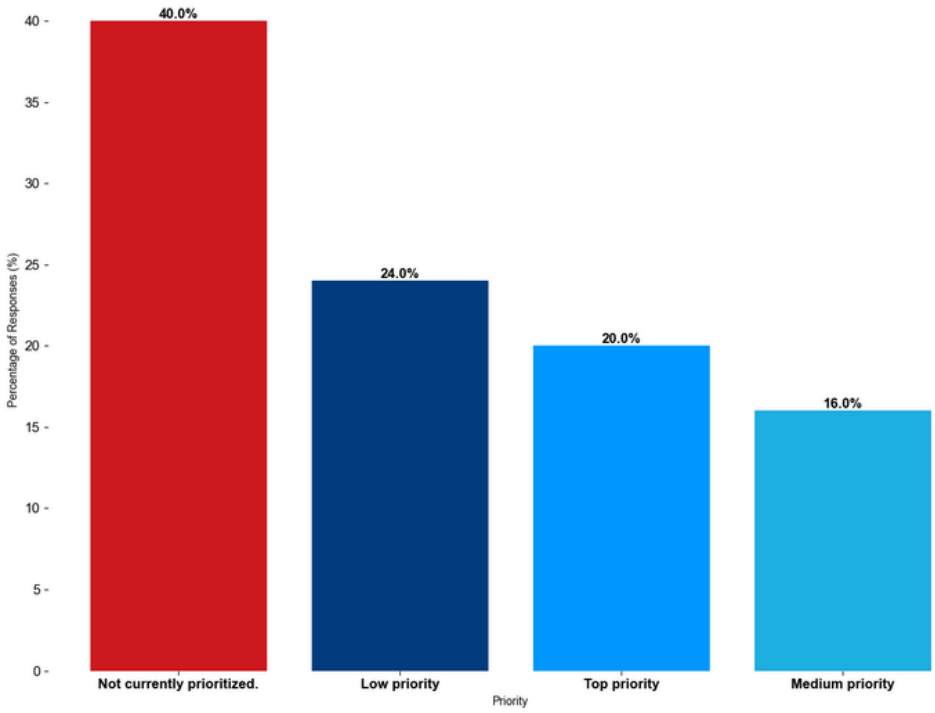
Among the organizations who said Yes, we asked who is driving this initiative internally? The answers were IT security team and CISO/CIO. We also asked do you have your leadership Support? 72% of respondents said they have leadership support. The support has not translated to actions yet.

What stage is your organization at in its post-quantum transition?



The current stage of the organization is still in the **beginning stage**. 23% of respondents said no awareness. 59% of respondents said awareness but no planning. 18% said Pilots or proof of concept stage (PoC) with post quantum solutions. No organizations are in Planning in progress or fully implemented stage.

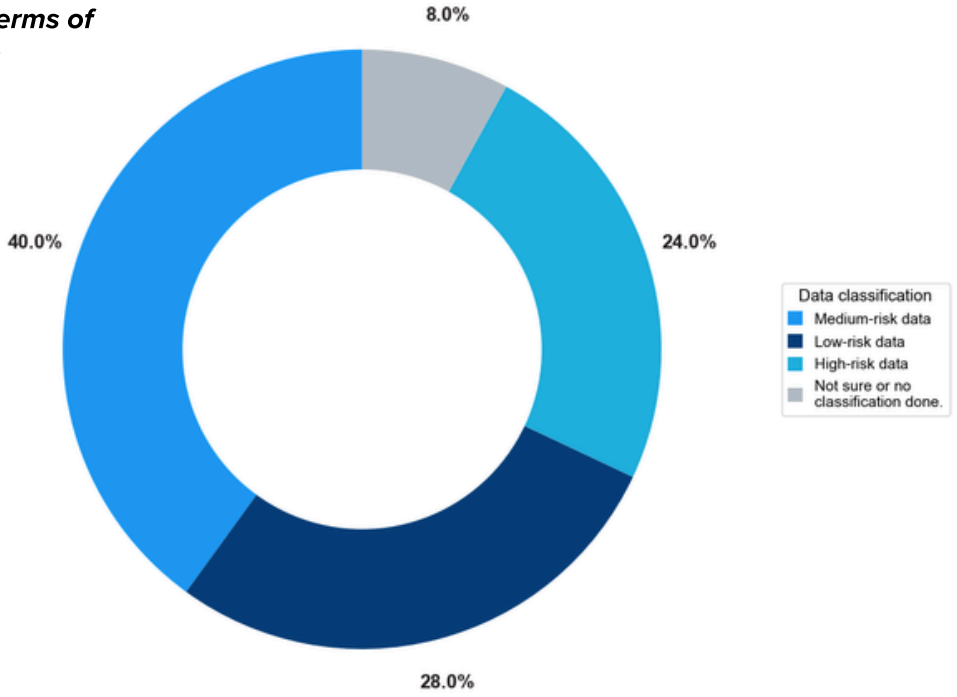
How important is PQC in your overall cybersecurity strategy?



PQC remains a **low priority** for most organizations. While 40% of respondents reported that PQC is not currently prioritized, 24% rated it as a low priority and another 16% as a medium priority. Only 20% consider PQC a top priority primarily those organizations already conducting proofs of concept (PoC) and developing roadmaps. Overall, the results suggest that although leadership awareness exists, concrete planning and integration of PQC into cybersecurity strategies remain limited.

INVENTORY & READINESS

How does your organization classify its data in terms of sensitivity and risk?

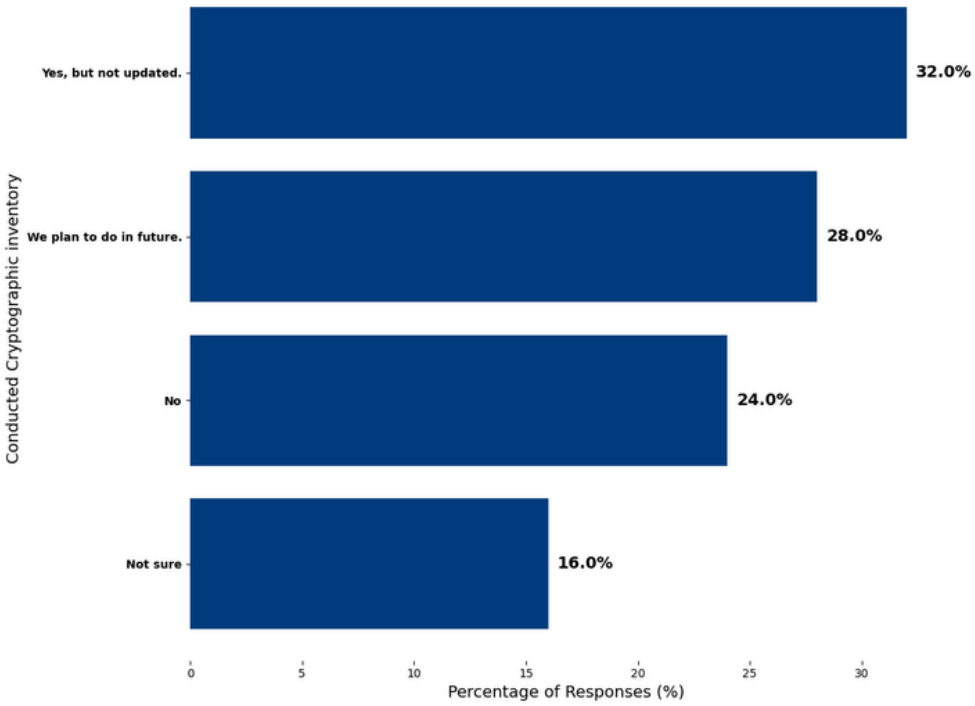


40 %

of organisation data is classified in terms of sensitivity as medium risk data

24% of respondents said the organization data is classified in terms of sensitivity as high-risk data. 28% of respondents said the organization data is classified in terms of sensitivity as Low risk Data and 8% of respondents were either Not sure or no classification of data is done.

Has your organization conducted a cryptographic inventory to identify algorithms and protocols currently in use?



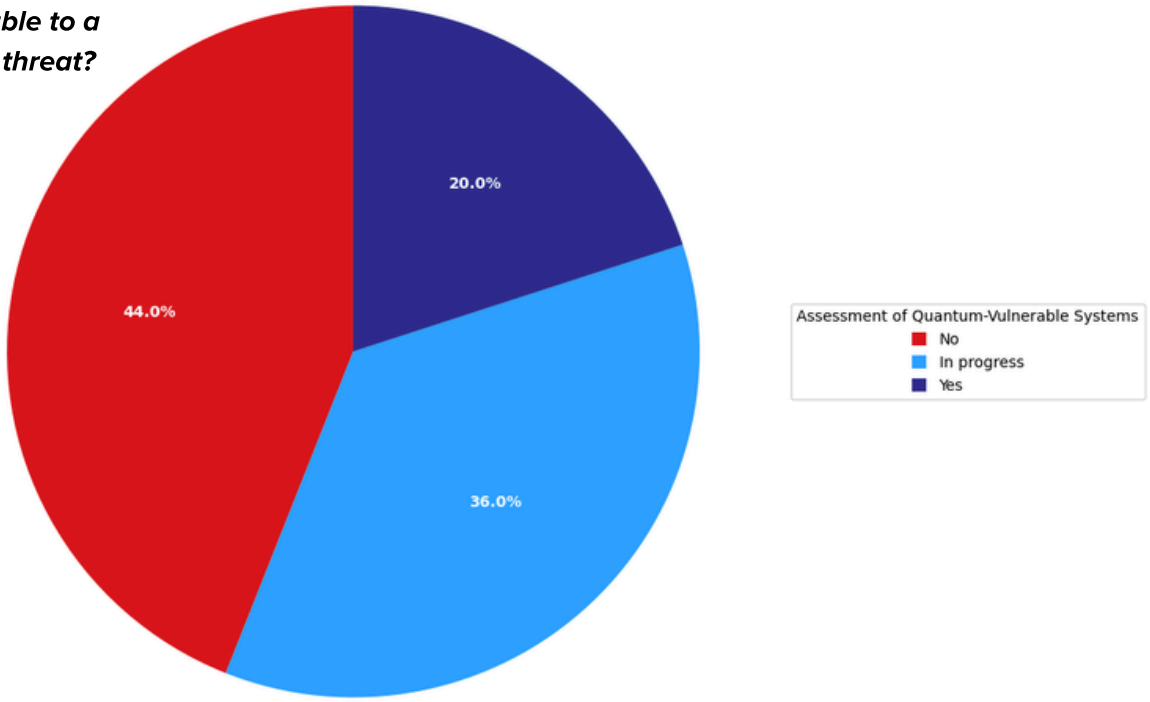
32 %

of organizations have undertaken a cryptographic inventory, but the lack of ongoing updates reduces its value for PQC readiness.

Another 28% acknowledge the need for cryptographic discovery but have postponed execution, indicating intent without follow-through. Meanwhile, 24% of organizations have not conducted an inventory at all, and 16% are unsure whether one exists, pointing to unclear ownership and poor internal visibility.

Having a PQC strategy strongly aligns with having cryptographic visibility. Organizations without a strategy are significantly more likely to lack inventories or be unaware of their cryptographic assets.

Have you assessed which systems would be most vulnerable to a future quantum threat?

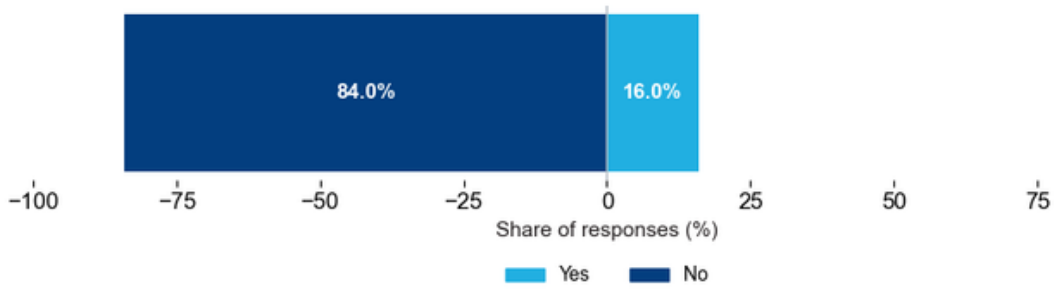


44 %

of respondents have not assessed which systems would be most vulnerable to a future quantum threat.

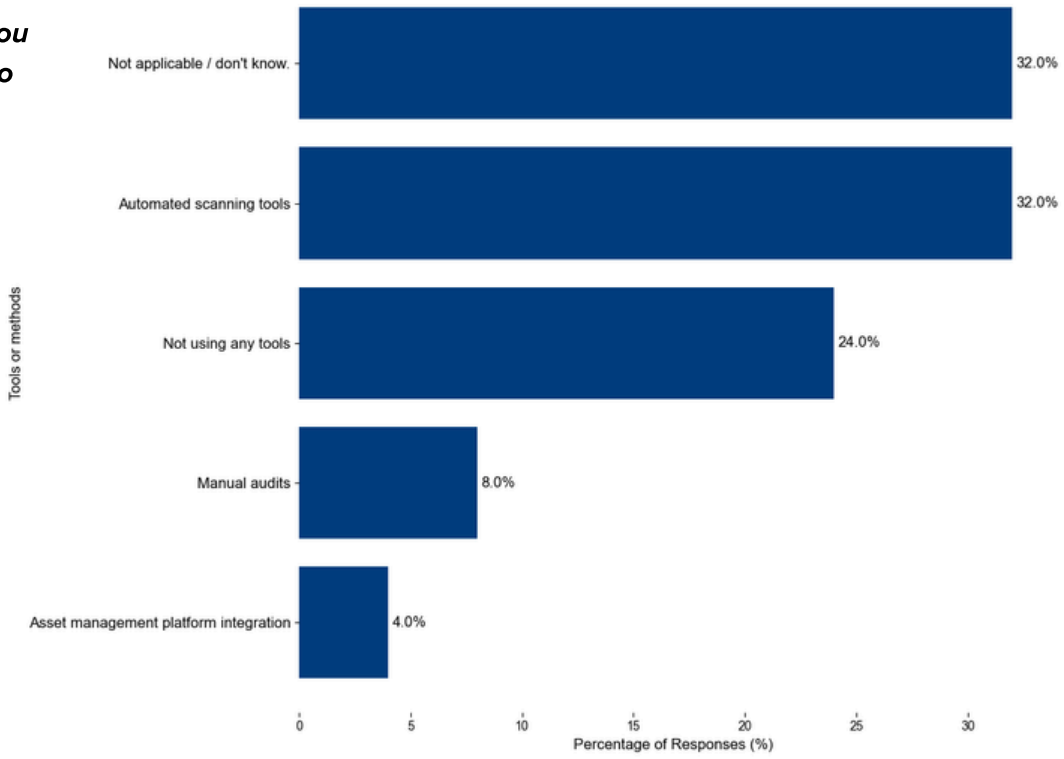
20% of respondents have assessed which systems would be most vulnerable to a future quantum threat. 36% of respondents have begun the assessment. But majority 44% of respondents have not assessed.

Are you currently testing or piloting any PQC algorithms?



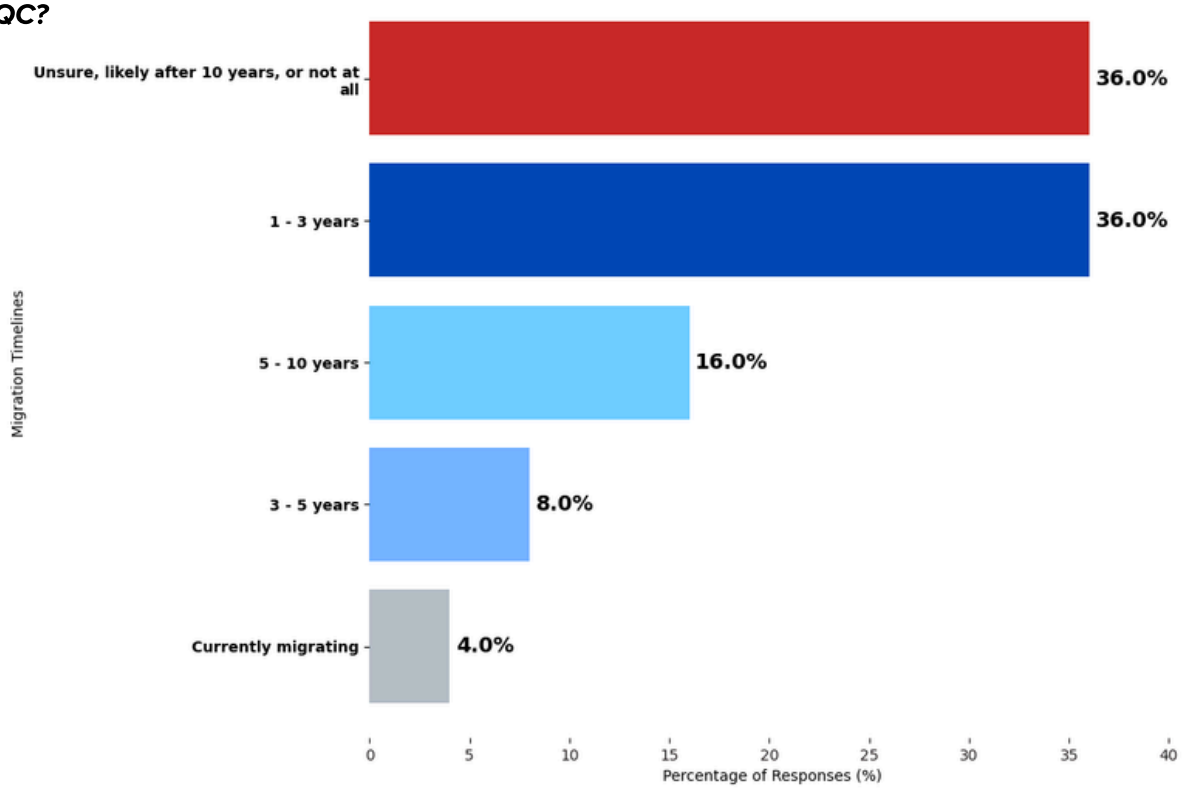
16 % of organizations are currently testing or piloting any PQC algorithms.

What tools or methods are you using for crypto discovery and inventory?



8% of respondent's use Manual audits. 32% of respondents use Automated scanning tools. 4% of respondents use Asset management platform integration.
24% of respondents are Not using any tools. 32% of respondents said Not applicable / don't know.
This indicates that many organizations have an opinion it's not applicable or aren't aware.

When do you plan to start migrating to PQC?

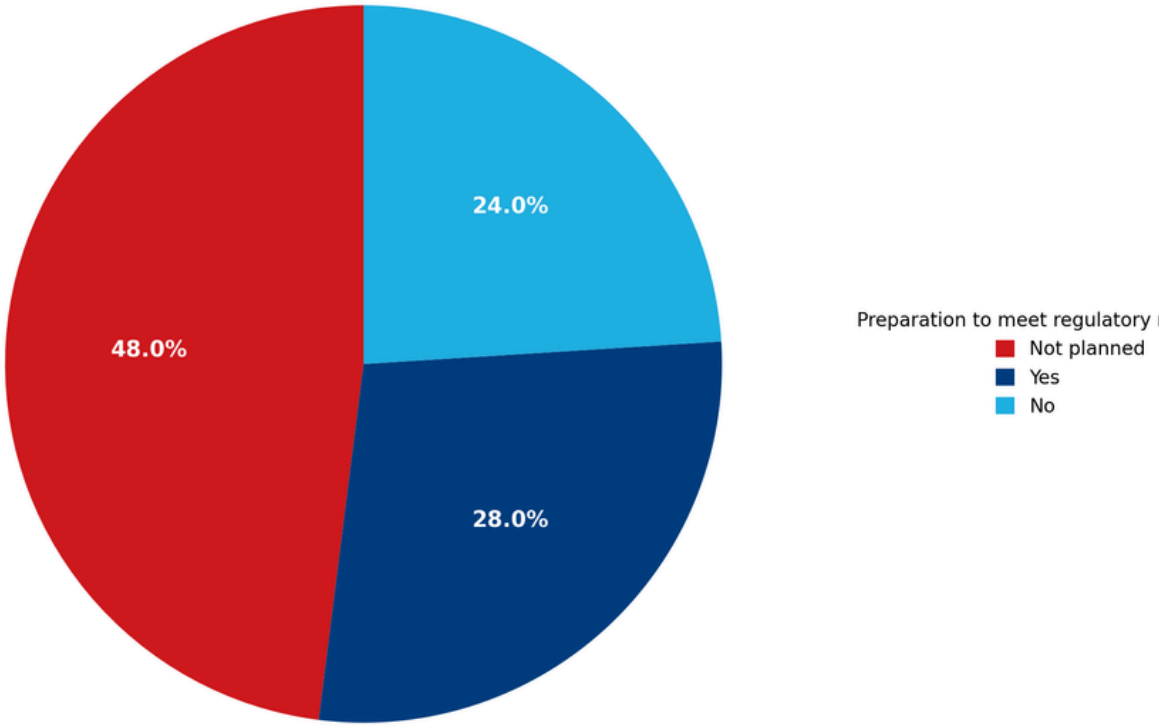


36% of respondents are unsure, likely after 10 years or not at all these are essentially undecided or assume they will not act until far in the future. 36% of respondents think it will be 1-3 years demonstrating a relatively urgent stance and 16% of respondents say 5-10 years. 8% of respondents for 3-5 years and currently migrating. This split reveals that while some forward-leaning companies are preparing to act in the short term, a significant portion have no concrete timeline or foresee waiting a decade or more. Such delay could be risky if standards and regulations push for earlier adoption.

PQC pilots are largely confined to organizations with in-house cryptographic expertise, highlighting workforce capability as a key enabler of early adoption.

REGULATIONS/ COMPLIANCE

Are you prepared to meet impending regulatory requirements around quantum threat resilience?



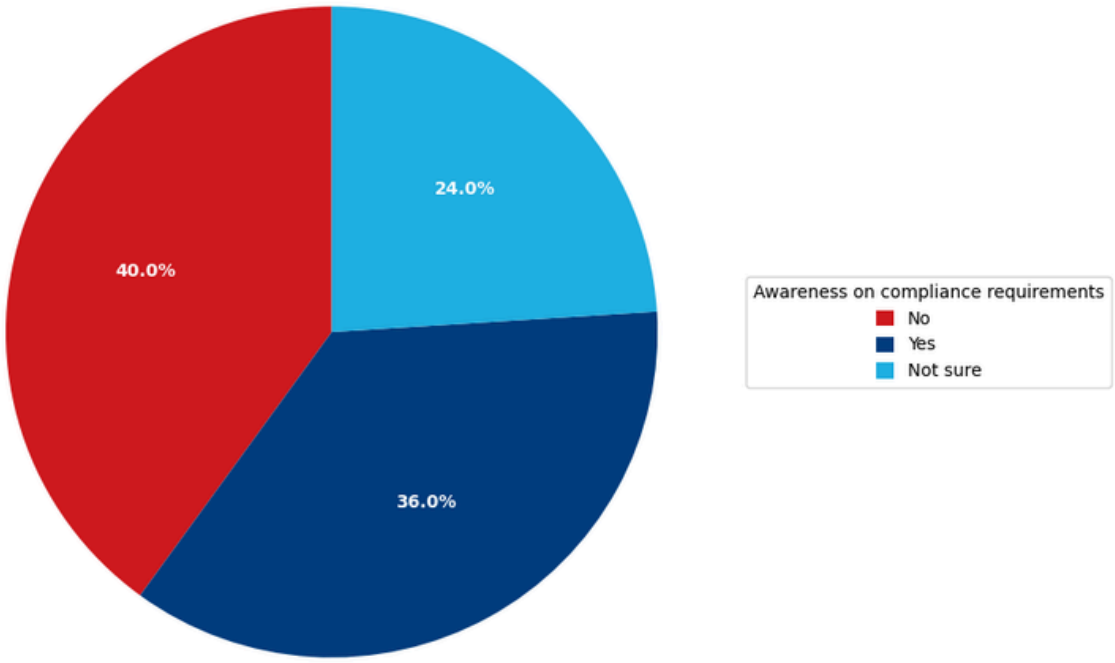
48%

are NOT prepared to meet impending regulatory requirements around quantum threat resilience.

Only 28% of respondents are prepared for regulatory requirements. Majority 48% have not planned and 24% of respondents said no.

This is concerning, given that governments and industry have already shared requirements for quantum-safe encryption in the coming years including roadmaps. It seems two-thirds of companies have not accounted for these upcoming compliance obligations in their plans.

Are you aware of emerging compliance requirements or government guidelines on PQC?



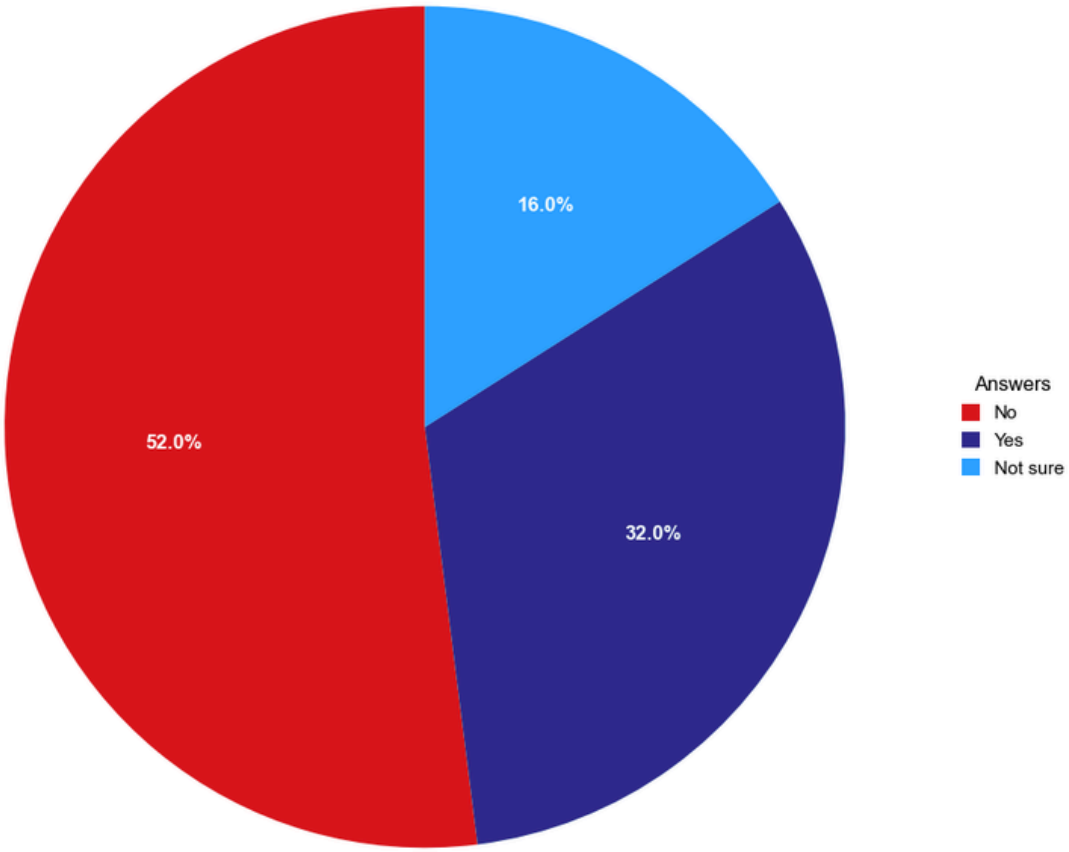
64%

of respondents are not sure or no awareness on the emerging compliance requirements or government guidelines on PQC.

36% of respondents are Yes. Many companies will be under pressure to implement when new regulatory changes are introduced due to the lack of proactiveness. Most organizations have neither planned for compliance nor educated themselves on it. This is a significant risk area: as soon as PQC-related compliance becomes enforceable, these organizations would need to catch up. Proactively improving awareness and making at least basic preparations (like tracking crypto assets and following NIST's PQC standardization progress) would greatly benefit those who currently have "not planned" anything on this front.

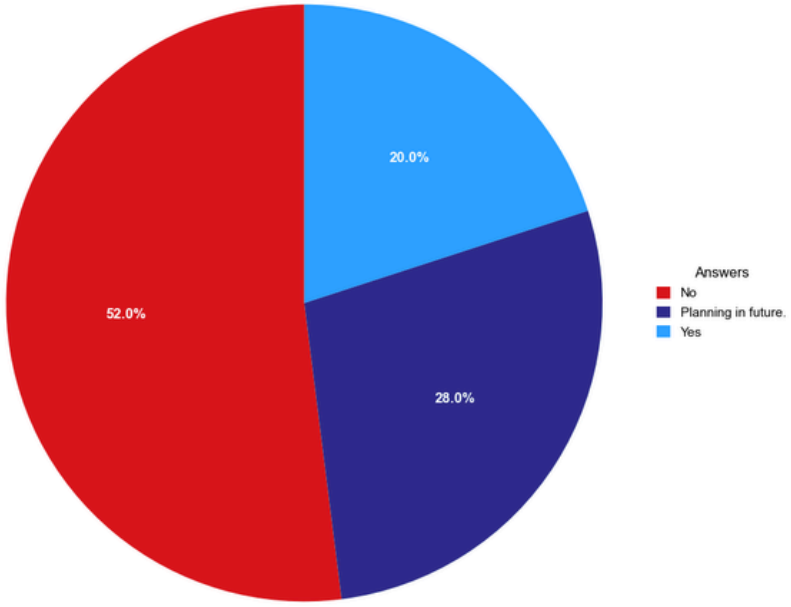
VENDOR & SUPPLY CHAIN

Have you engaged with third-party vendors or service providers about their plans for PQC?



Engagement with third-party vendors on PQC remains limited. Only 32% of respondents reported having engaged with external vendors or service providers regarding their PQC plans, while the majority (68%) indicated that they have not engaged or are unsure whether such discussions have taken place.

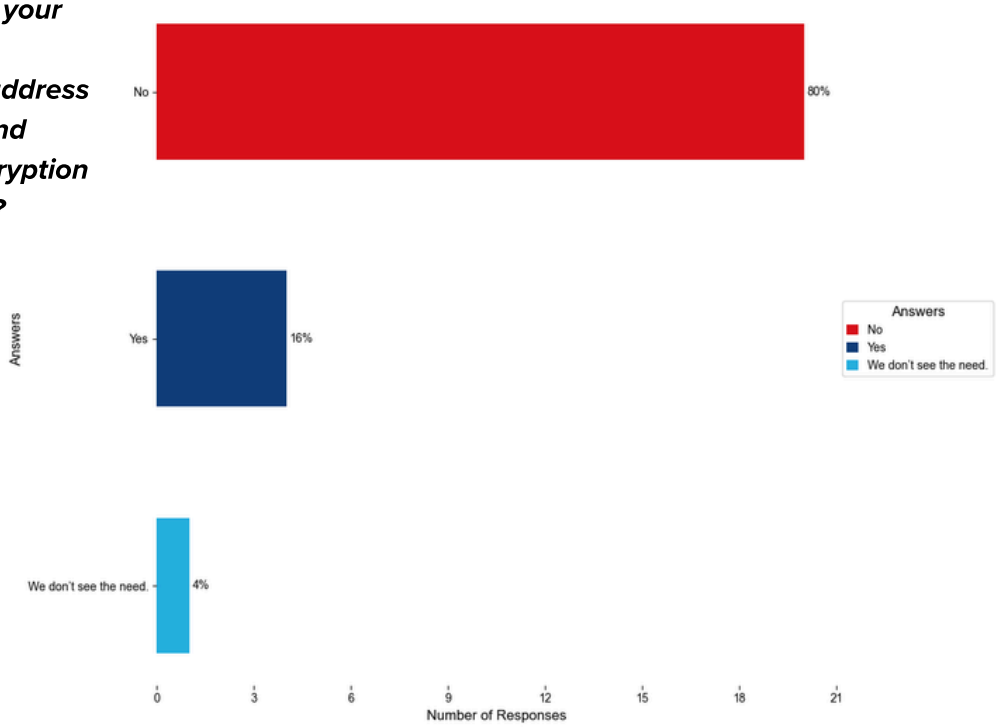
Have you assessed your third-party relationships, their cryptologic standards and any potential impacts on post-quantum?



Most organizations have not yet assessed their third-party relationships for post-quantum readiness. A majority of respondents 52% reported no assessment of vendors' cryptologic standards or potential post-quantum impacts, indicating limited engagement with software suppliers, cloud providers, and other partners on quantum-safe roadmaps.

A further 28% plan to conduct such assessments in the future, while only 20% have already completed an evaluation highlighting a potential supply-chain risk that could directly affect organizational security posture.

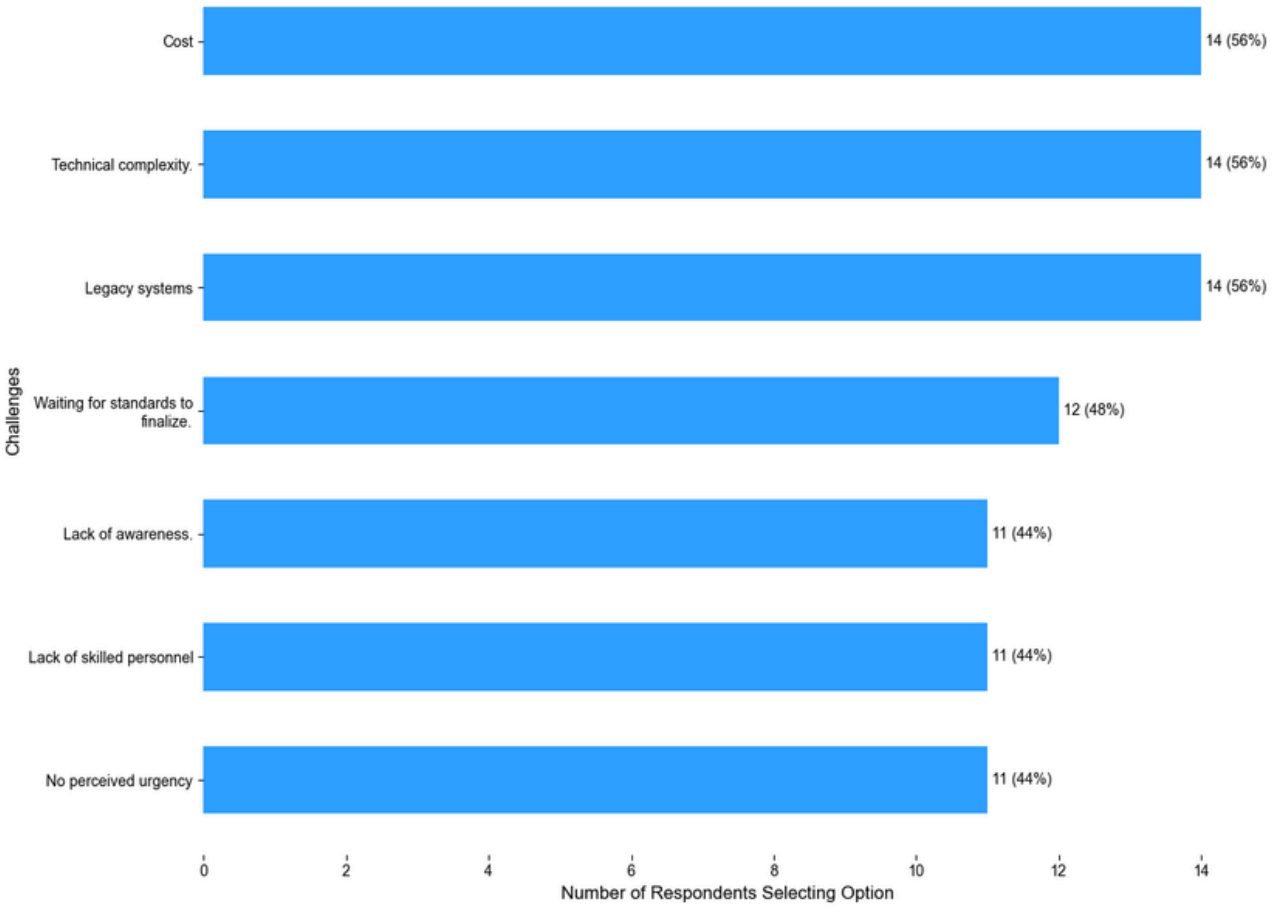
Have you revised your procurement requirements to address PQC standards and documenting encryption for new solutions?



The results indicate that PQC considerations are largely absent from procurement processes. A significant majority of respondents 80% reported that they have not revised procurement requirements to address PQC standards or to document encryption practices for new solutions. Only 16% confirmed that such revisions have been made, while a small minority 4% indicated that they do not see a need to do so.

CHALLENGES

What are the biggest challenges in transitioning to PQC? (Select all that apply)



56 %

of respondents cite legacy systems, cost, and technical complexity as the primary challenges in transitioning to PQC.

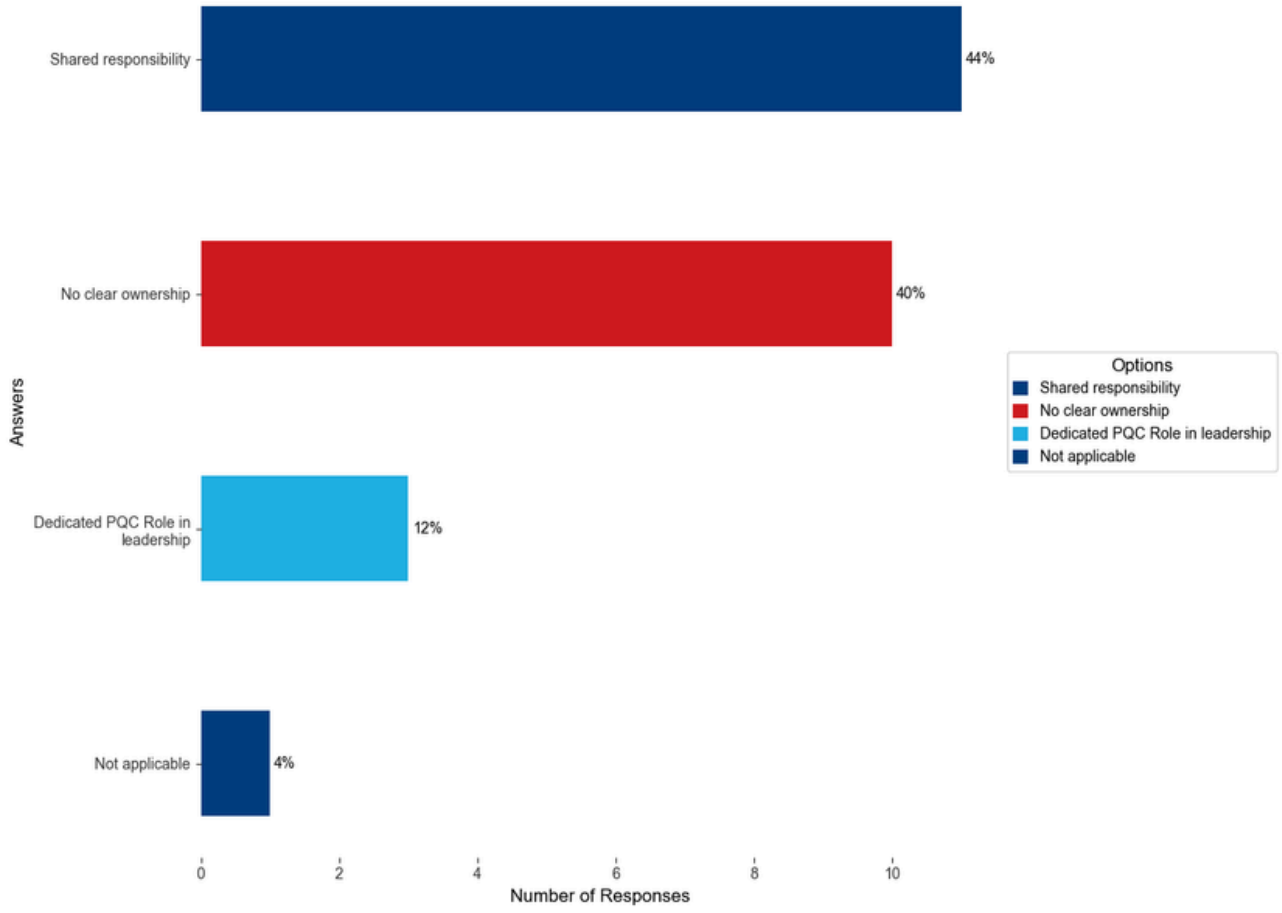
Transitioning to post-quantum cryptography is hindered by a combination of technical and organizational challenges.

The most frequently cited barriers are cost, technical complexity, and legacy systems, each selected by 56% of respondents, indicating that PQC adoption is perceived as both resource-intensive and difficult to integrate into existing environments.

Nearly half of respondents 48% report waiting for standards to be finalized, reflecting uncertainty and a tendency to delay action until clearer guidance emerges.

Additionally, 44% cite lack of awareness, shortage of skilled personnel, and no perceived urgency, highlighting persistent readiness and prioritization gaps.

Do you have a dedicated PQC leadership role or is it an additional role with current responsibilities?



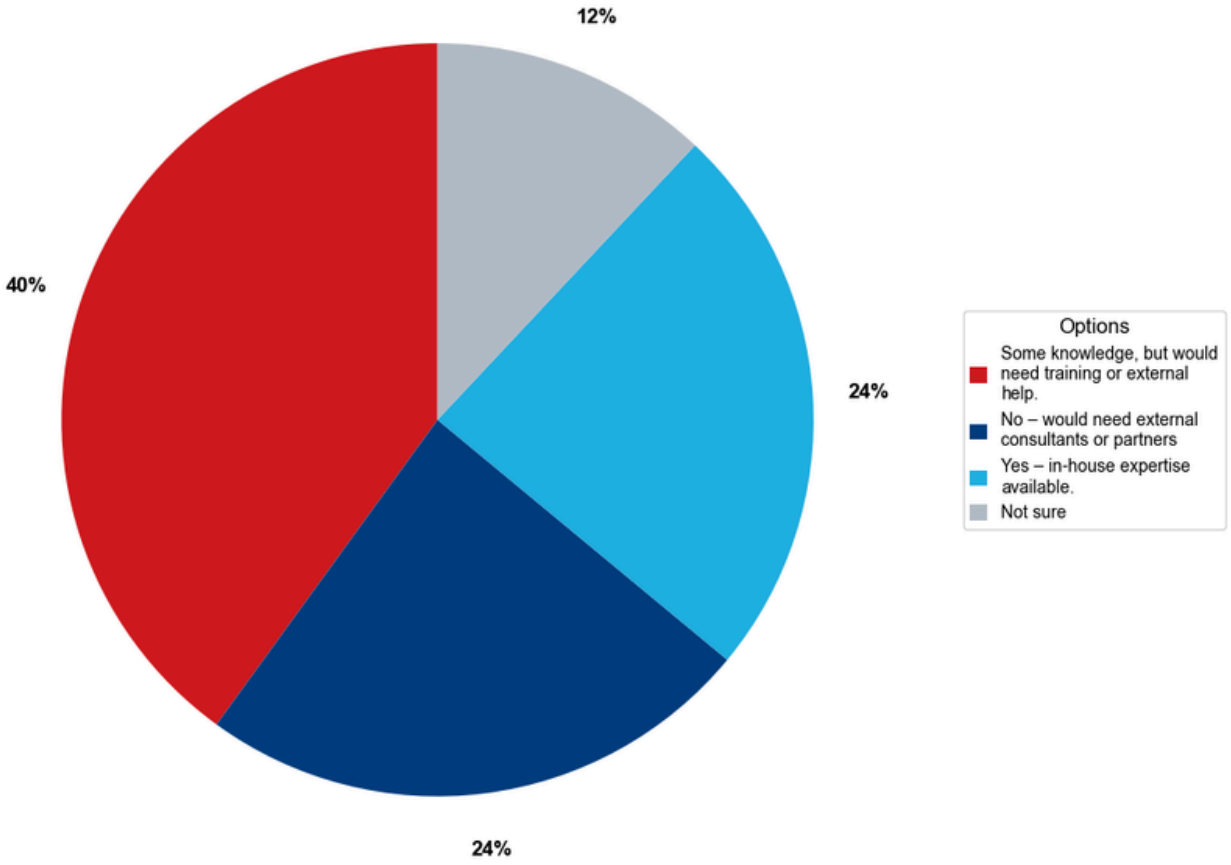
12%

Dedicated PQC Role in leadership

The results show that clear leadership ownership for PQC is largely lacking across organizations. A majority of respondents indicated either no clear ownership 40% or that PQC responsibilities are shared alongside existing roles 44%. Only a small proportion of respondents 12% reported having a dedicated leadership role specifically responsible for PQC, underscoring the early and fragmented nature of governance in this area.

WORKFORCE

Do you have internal staff with sufficient technical knowledge to evaluate and implement PQC solutions?



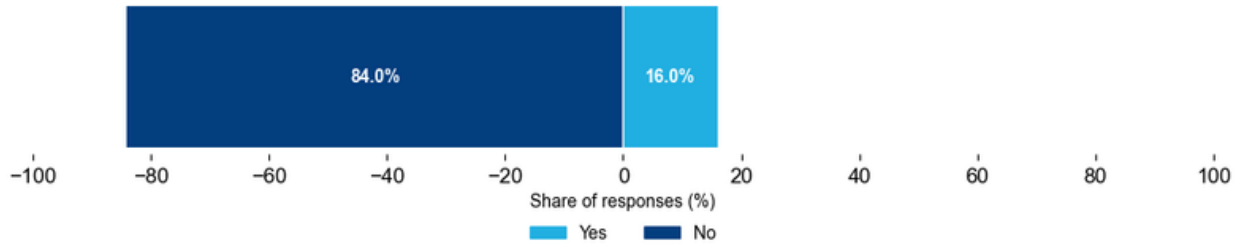
40 %

have internal staff with some technical knowledge to evaluate and implement PQC solutions, but would need training or external help

A further 24% state they lack the necessary expertise altogether and would rely entirely on external consultants or partners, and 12% are unsure of their internal capabilities.

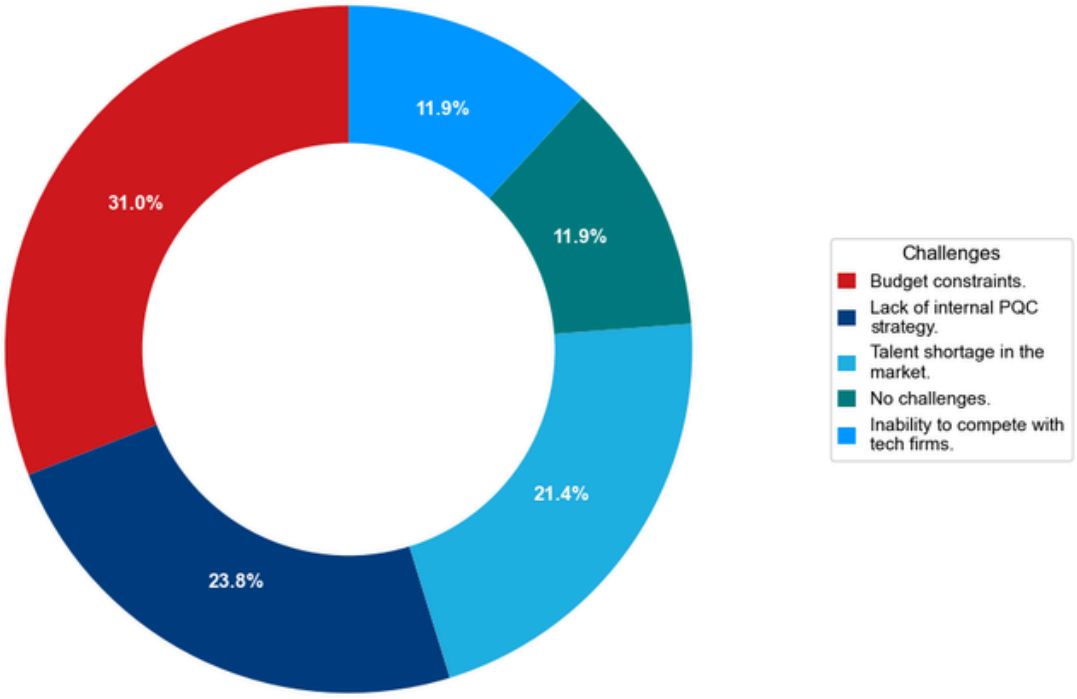
Only 24% of respondents confirm that they have sufficient in-house expertise to independently assess and deploy PQC technologies.

Are there plans to hire or train staff in PQC-related roles in the next 12 months?



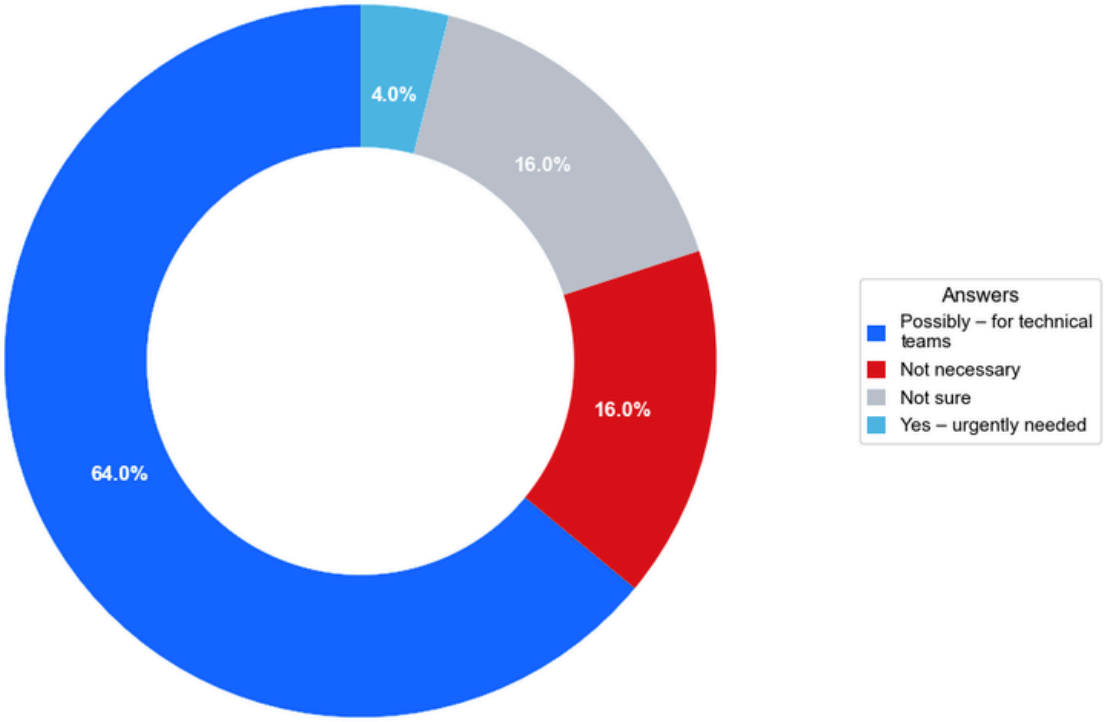
84 % of respondents said no to plans to hire or train staff in PQC related roles in the next 12 months.
Only 16% of respondents said they plan to hire or train staff in PQC related roles.

What challenges do you face in hiring PQC talent?



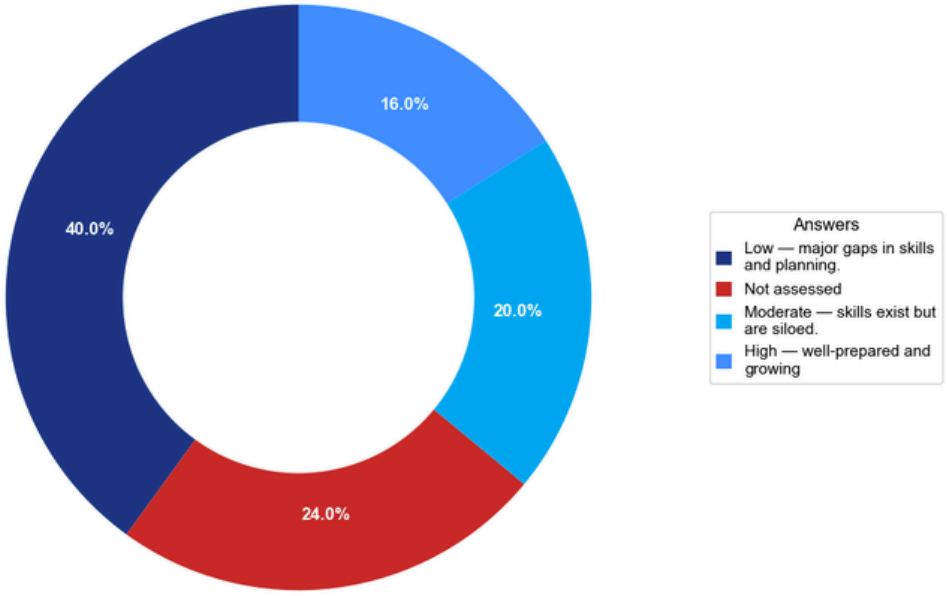
31 % of respondents have budget constraints, 24% of respondents Lack of internal PQC strategy, 21% of respondents talent shortage in the market, 12% of respondents no challenges, 12% of respondents Inability to compete with tech firms.

Would your organization benefit from external PQC training or workshops?



64 % benefit from external PQC training or workshops for technical teams.

How would you rate your workforce's overall PQC readiness?



40 %

workforce's overall PQC readiness as low.

While 16% of respondents show high preparedness for PQC readiness and growing, 20% of respondents show moderate level of preparedness skills exist but are siloed, 40% of respondents low preparedness major gaps in skills and planning, 24% of respondents not assessed their preparedness.

PQC familiarity emerges as a key enabler of readiness. Strong correlations show that organizations with higher awareness are significantly more likely to have defined strategies, be in advanced transition stages, and conduct PQC pilots.

Methodology

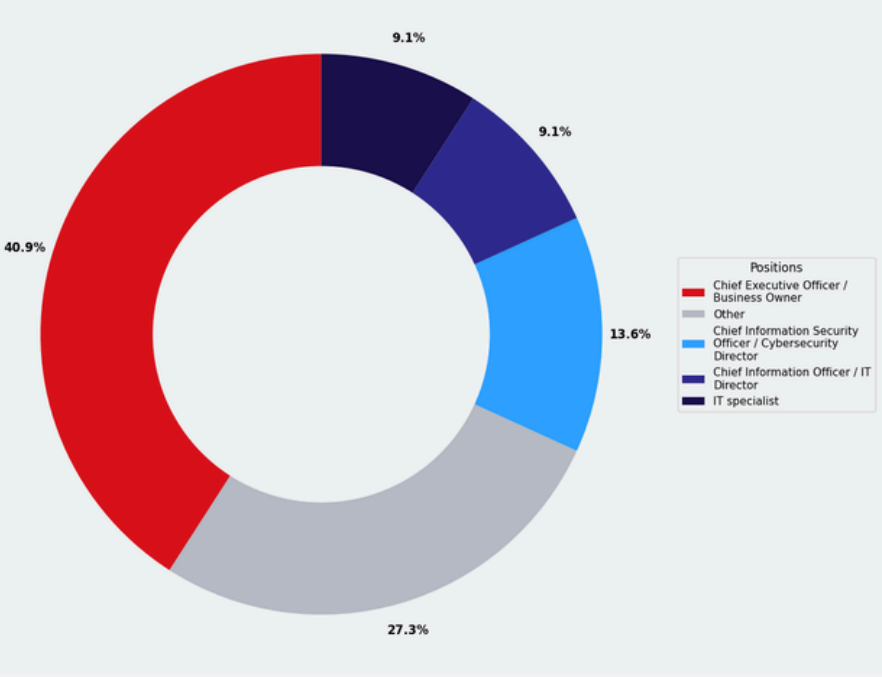
The survey questionnaire was prepared in collaboration with LuxQuantum. The survey focused on 5 key areas

- PQC AWARENESS
- PQC STRATEGY
- PQC INVENTORY & READINESS
- PQC GOVERNANCE
- WORKFORCE

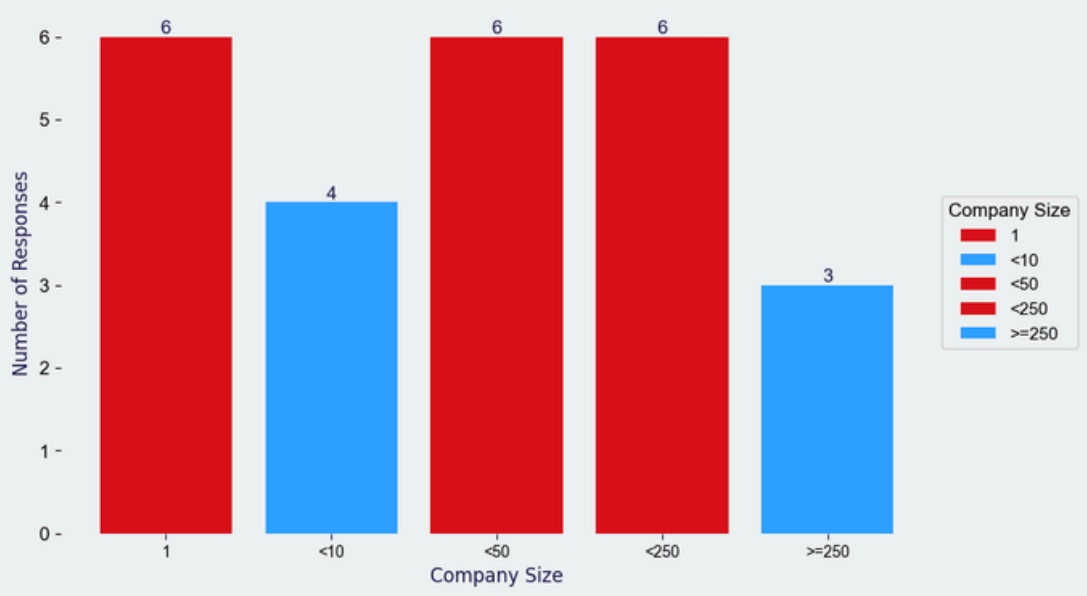
The survey was circulated to the Luxembourg ecosystem through our partners and intensive campaign on our social media channels and newsletter.

25 respondents completed the survey.

Survey participants primarily represent senior leadership and technical decision-makers. 41% of respondents are Chief Executive Officers or Business Owners, while 27% fall into other senior or cross-functional roles. Technical leadership is represented by 14% Chief Information Security Officer (CISO) / Cybersecurity Directors and 9% Chief Information Officer (CIO) / IT Directors, with an additional 9% identifying as IT specialists. This mix ensures the findings reflect both strategic and technical perspectives on PQC readiness.

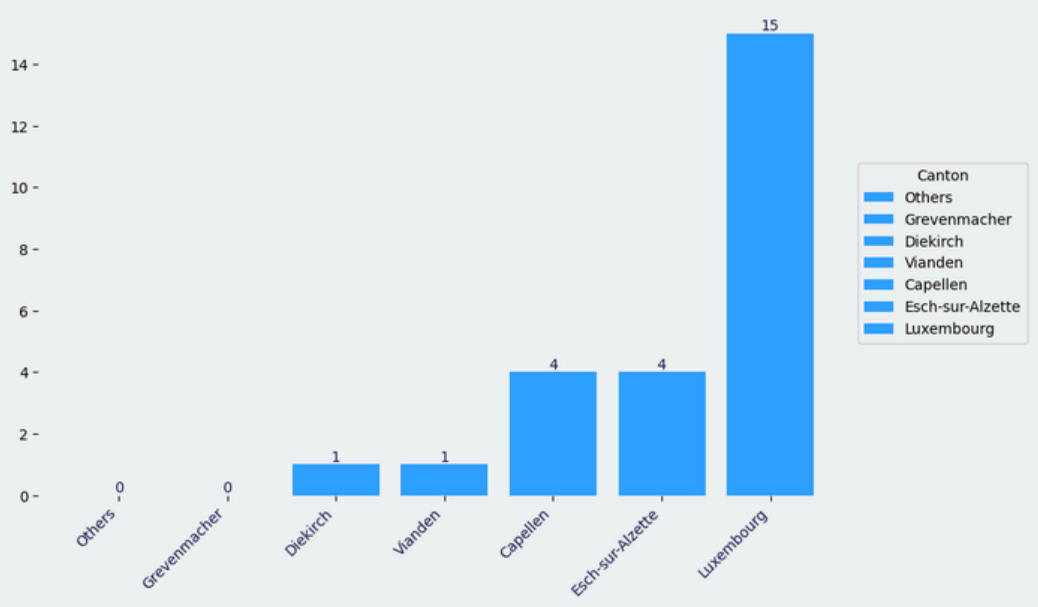


Company size



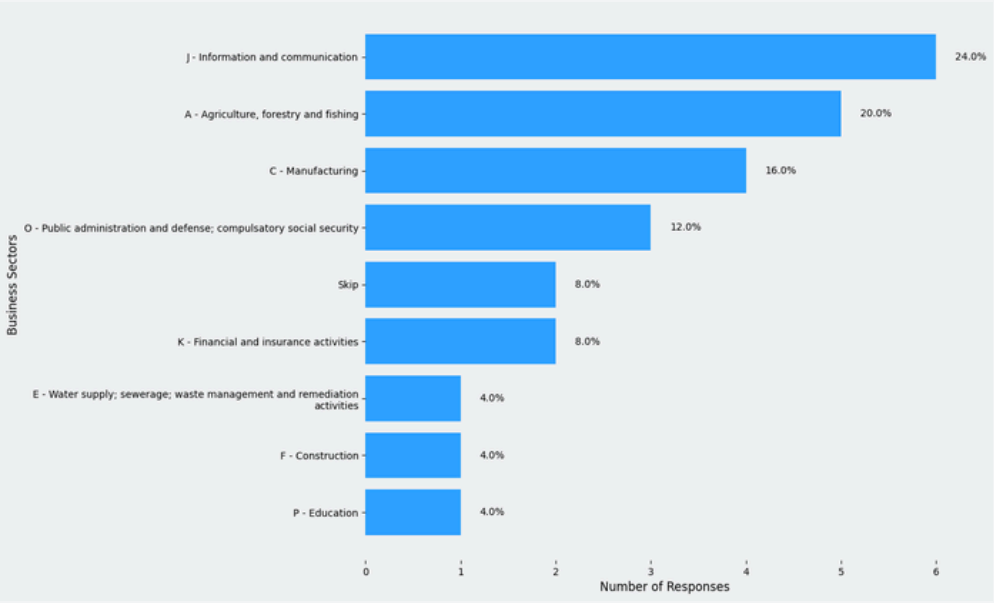
The respondent base is dominated by very small and small organizations. Solopreneurs and companies with fewer than 50 employees and fewer than 250 employees each account for six respondents, while four respondents represent organizations with fewer than 10 employees.
In contrast, only three respondents come from large enterprises ≥250 employees. Overall, the dataset shows strong representation from small businesses, while medium-sized and large enterprises are comparatively underrepresented.

Localisation



15 respondents from Luxembourg, 4 Esch-sur-alzette, 4 capellen, 1 Vianden, 1 Dierkich.

Sectors



Respondents span multiple business sectors, with the highest representation from Information and Communication 24%, followed by Agriculture, Forestry and Fishing 20% and Manufacturing 16%. Public Administration and Defense accounts for 12% of responses, while Financial and Insurance activities represent 8%. Other sectors, including Water and Waste Management, Construction, and Education, each account for 4%, indicating broad but uneven sector coverage.

Special thanks:

We would like to thank Steve Purser,Independent cybersecurity Consultant CSPRO Services for his insightful feedback on the draft report and for helping to add additional practical use case.
We would like to thank Samira Chaychi, Co-founder LuxQuantum for her insightful feedback on the draft report and for helping us clarify the PQC migration timeline.

nc3
Threat Observatory
Platform

Report edited and published by:

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

Luxembourg House
of Cybersecurity