Freeform Dynamics in association with CERTES

# The Emerging PQC Imperative

## Insights from early movers

Freeform Dynamics, 2026

*Quantum Computing threatens to break most of the encryption used today to secure data and communications. The timeline is debatable, but regulators aren't waiting - compliance milestones are already being set. The findings from our recent 'Post Quantum Cryptography' (PQC) study will help you work out what this means in practice and how others are approaching the problem.*

## KEY TAKEAWAYS

- **PQC is driven by business risk, not just compliance**
  Regulatory timescales have dominated the urgency aspect of industry discussions, but the primary motivation for acting on PQC is protecting the organization from real-world exposure. This is a business risk conversation first and foremost.

- **The hardest areas to fix are also the most exposed to potential PQC threats**
  Legacy environments, custom applications and edge/IoT equipment present both the highest threat and the greatest difficulty to remediate - a combination that demands careful consideration when prioritizing and setting objectives.

- **Most active organizations are still at the start of their journey, and that's OK**
  Even among the more engaged organizations that qualified into our study, activity remains focused on foundational work. This may be OK for now, as the regulatory timeline still allows for a considered approach, but the window is narrowing.

- **While potential impediments loom large, experience builds confidence**
  A perceived lack of both industry and internal readiness are seen as significant impediments to progress, but experience breeds confidence, which suggests that the challenges can be overcome with an informed and structured approach.

- **The case for acting now is practical, not just precautionary**
  Smart tactics and emerging best practices are reducing costs and complexity, and the PQC ecosystem is maturing faster than you might think. Acting sooner, provides time to build strong foundations that will pay dividends down the line.

Copyright 2026 Freeform Dynamics Ltd

# Introduction

Quantum Computing works on fundamentally different principles to today's systems, enabling it to solve certain types of problem that are effectively impossible using conventional computing models. Among these are the mathematical problems that underpin most current encryption.

When sufficiently powerful quantum systems become available, much of the cryptography protecting your data and communications today will be rendered ineffective. Post Quantum Cryptography - or PQC - is the umbrella term for the standards, techniques and practices being developed to address this.

## Why this conversation, and why now?

Opinions vary on when commercial quantum systems will be powerful enough to pose a real threat. Some put it within the next decade, others see it as further out.

But regulators and standards bodies have decided the risk warrants action now, not later. Compliance milestones targeting critical infrastructure are already set for 2030, with a broader expectation of full transition to quantum-safe systems by 2035. Given the complexity of what's involved - a topic explicitly explored in the research - these dates don't leave as much room as they might first appear to.

**Regulators and standards bodies have decided the risk warrants action now, not later, and compliance milestones have already been set.**

If your organization hasn't started thinking about this yet, the window for a considered, well-planned approach is narrowing. If you have started, you're likely discovering that the practical challenges go well beyond simply upgrading a few encryption libraries.

## About the study

This report is based on input from 200 security and IT leaders and specialists, including CISOs, CSOs, CIOs and other senior professionals. Respondents were equally split across the US and UK, and spanned 6 industry sectors - financial services, manufacturing, energy, telecommunications, healthcare and the public sector. All participants were drawn from larger organizations - 47% in the 1,000 to 5,000 employee band, and the remainder 5,000 and above. Each was individually screened to confirm direct involvement in, and knowledge of, quantum-related security risks.

The study was sponsored by Certes and completed in the second quarter of 2026.

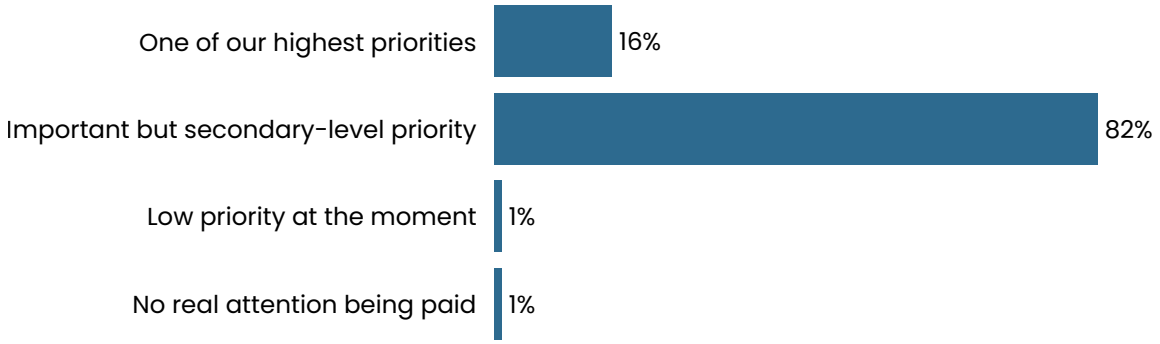
Copyright 2026 Freeform Dynamics Ltd

# Focus on those already engaged

Participants in this study were screened for direct engagement with quantum-related risks, which immediately places them ahead of the curve in this space. While this was by design, to provide the maximum level of informed input on real world practicality, you need to bear the resulting sample skew in mind when looking at specific numbers on charts. Remember that the percentages shown reflect the perceptions and experiences of early movers rather than the IT and security community as a whole.

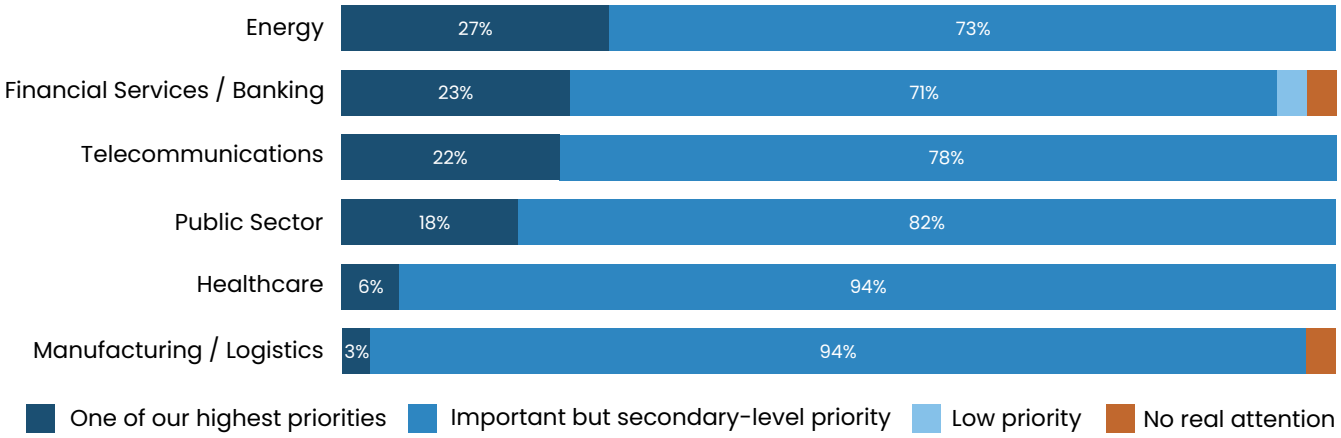
That said, even within this more engaged group, only around one in six treat quantum risk as one of their highest priorities at this early stage in the market.

**To what degree is Quantum related risk currently prioritized in your organization?**




The picture shifts when we break things down by industry. Organizations in highly regulated sectors, and particularly those considered part of critical national infrastructure, are noticeably further ahead in terms of prioritization.

**To what degree is Quantum related risk currently prioritized in your organization?**



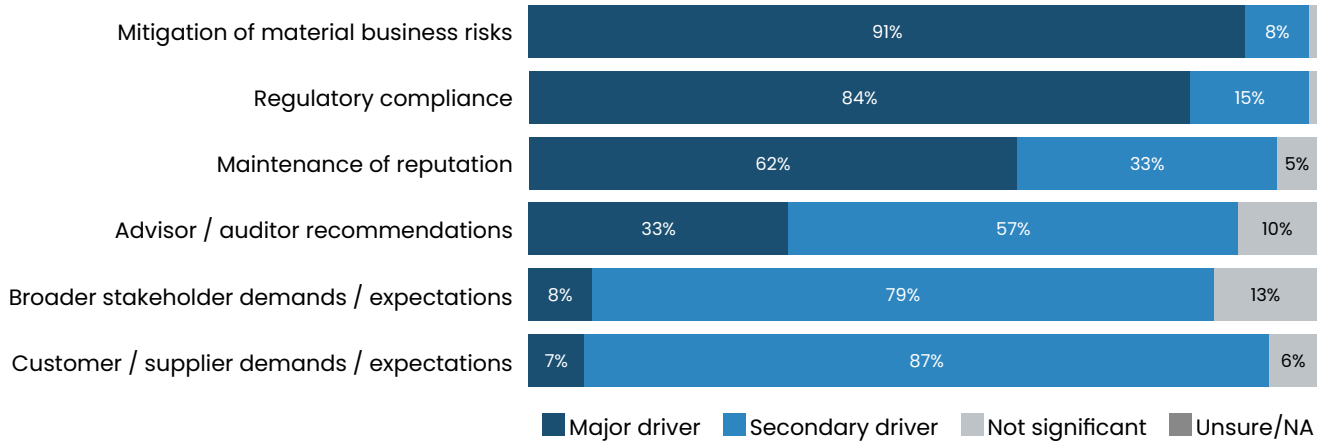

The distribution we see here is consistent with the initial focus of regulatory and standards bodies and deadlines they have already set, but as we'll see on the next page, this doesn't mean that PQC is purely a matter of compliance.

Copyright 2026 Freeform Dynamics Ltd

# Motivations to act

As previously indicated, PQC is definitely not just a matter of compliance, and the research results illustrate this unambiguously. While regulatory pressure is clearly a significant factor, the standout finding here is that mitigation of material business risk tops the list of motivations to act. Compliance provides a timeline, but the underlying concern is protecting the organization from real-world exposure. Reputational risk and advisor recommendations also feature prominently, with broader stakeholder and supply chain expectations playing more of a secondary role for now.

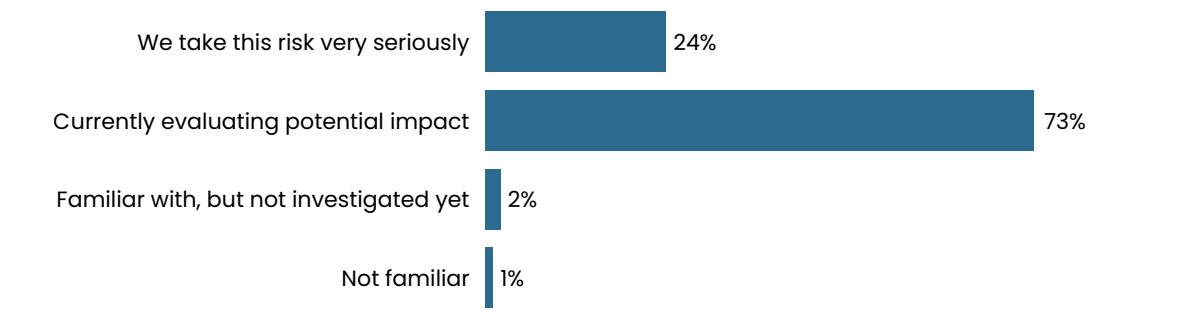
**What's currently motivating (or likely to motivate) action/investment in this area?**




## HNDL - an immediate potential threat

One risk that warrants specific attention is 'Harvest Now, Decrypt Later' (HNDL) - the idea that adversaries may already be intercepting and stockpiling encrypted data with the intention of decrypting it once effective quantum computing arrives. How seriously you take this depends on the nature of the data your organization holds and how long it remains sensitive. If that shelf life is measured in years or decades, the logic of the threat is hard to dismiss. Our respondents are clearly weighing it up, with almost a quarter already taking it very seriously.

**To what degree is the 'Harvest Now, Decrypt Later' (HNDL) risk recognized?**

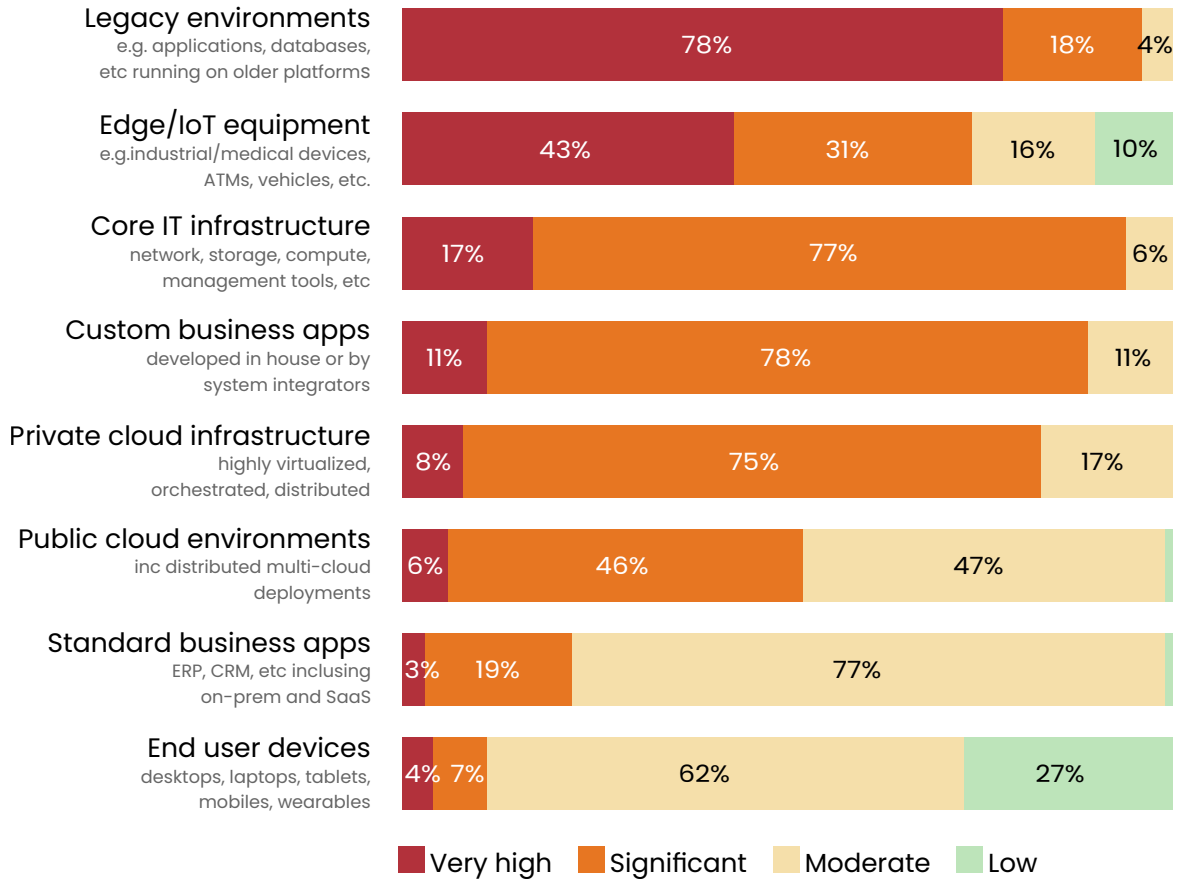



Copyright 2026 Freeform Dynamics Ltd

# Areas of potential exposure

With the broader motivations established, the next step is to consider where the exposure actually sits across your technology landscape. The picture that emerges from the research is one of widely distributed risk, with every environment type registering at least some perceived threat. That said, the pattern is far from uniform, and the variation tells an important story about where the real challenges are likely to be concentrated.

**How would you assess the potential threat to Quantum-enabled cryptography attacks from the following?**



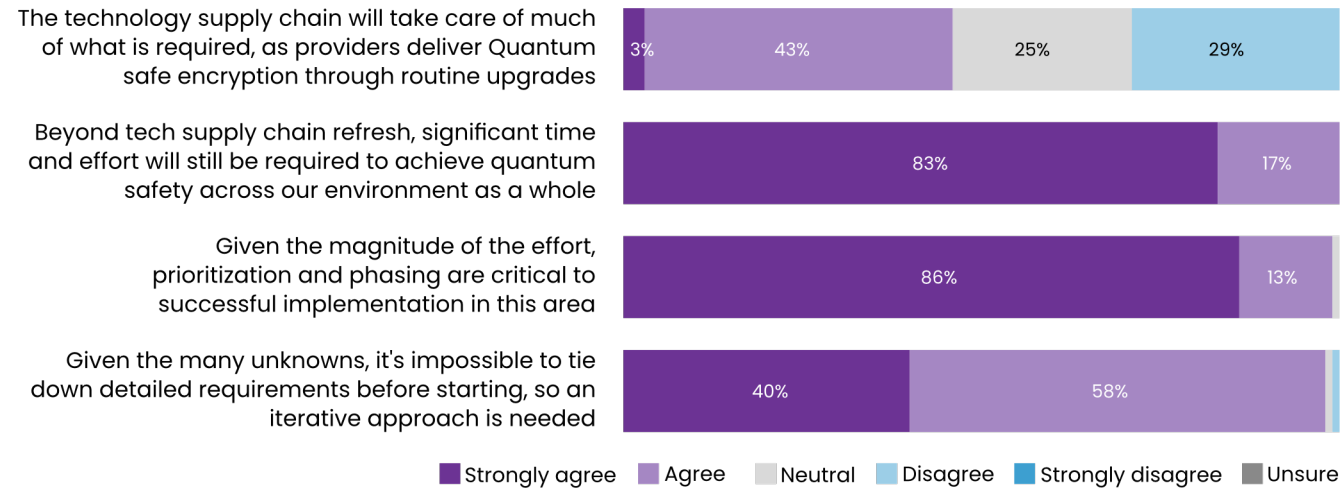

Legacy environments stand out as the area of greatest concern by a significant margin, followed by edge and IoT equipment - both environments where upgrading or replacing cryptographic capabilities is notoriously difficult. Core infrastructure, custom applications and private cloud all sit in a middle band where the threat is seen as broadly significant. At the other end of the scale, standard business applications and end user devices are viewed as lower risk, most likely reflecting an expectation that vendors will address these through routine product updates. The overall picture, though, is that quantum-related cryptographic risk touches practically every part of the technology estate to some degree. So how do you go about formulating and executing a plan to deal with something this pervasive?

Copyright 2026 Freeform Dynamics Ltd

# Acknowledging some key realities

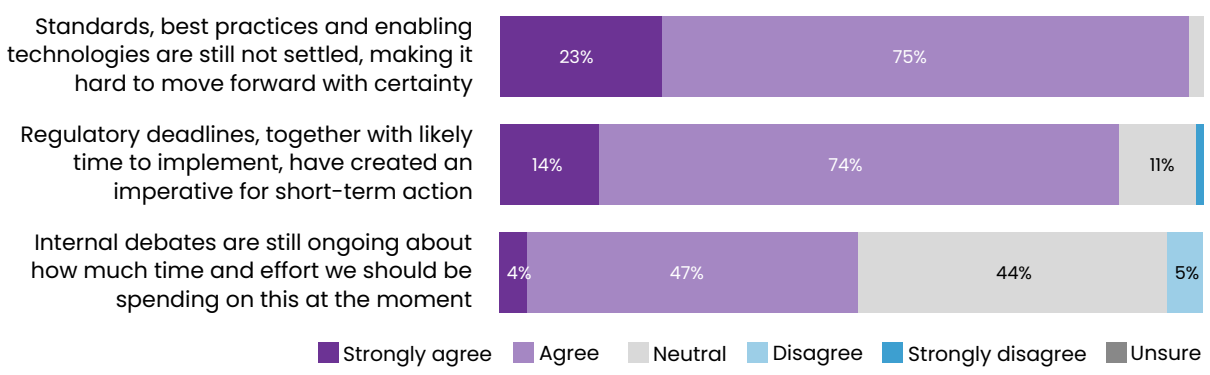
Before looking at specific plans and activities, it's worth stepping back to consider some of the realities that shape the task ahead. A common assumption is that technology providers will take care of quantum safety through routine upgrades - and while that will help in some areas, opinion on how far it will get you is notably divided. What isn't in dispute is that significant work will be required beyond anything the technology supply chain delivers, and that given the scale of what's involved, careful prioritization and a willingness to iterate will be essential.

### Scale of the Challenge (Agree/Disagree)




Against this backdrop, the practical reality of getting traction introduces its own set of challenges. Standards, best practices and enabling technologies are still evolving, which creates genuine uncertainty about how and when to move forward.

### Significant uncertainty (Agree/Disagree)




The tension among our respondents between needing to act and not yet having full clarity on how is reflected in the ongoing internal debates that around half of respondents report. This is arguably the defining characteristic of PQC planning right now - so let's look at how organizations are navigating it.

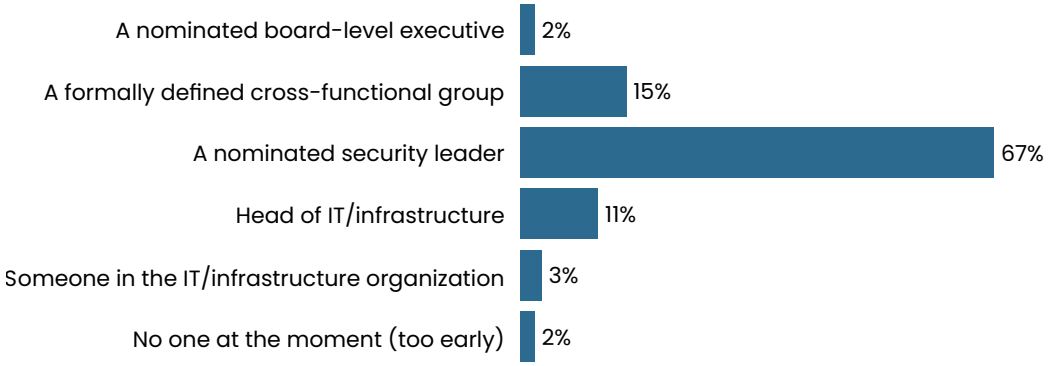
Copyright 2026 Freeform Dynamics Ltd

# Ownership and empowerment

Having acknowledged the scale and complexity of what lies ahead, the question of who owns the problem becomes critical. PQC implementation will cut across technology, operations, compliance and vendor management, so clear leadership and adequate empowerment are prerequisites for any meaningful progress.

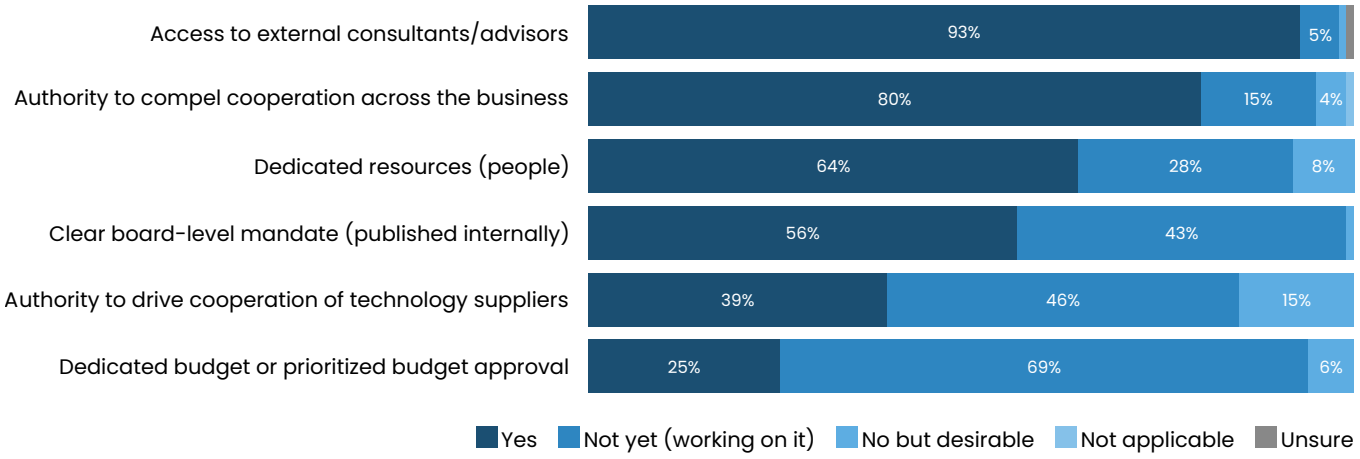
Among our respondents, ownership has largely settled on a named individual, and it's overwhelmingly sitting with security leaders rather than the IT function.

**Who is leading your efforts to understand and prepare for Quantum Computing related security risks?**




Assigning ownership is one thing, but equipping that individual or group to be effective is another, and the picture here is more mixed.

**Is this individual or group empowered in the following ways?**



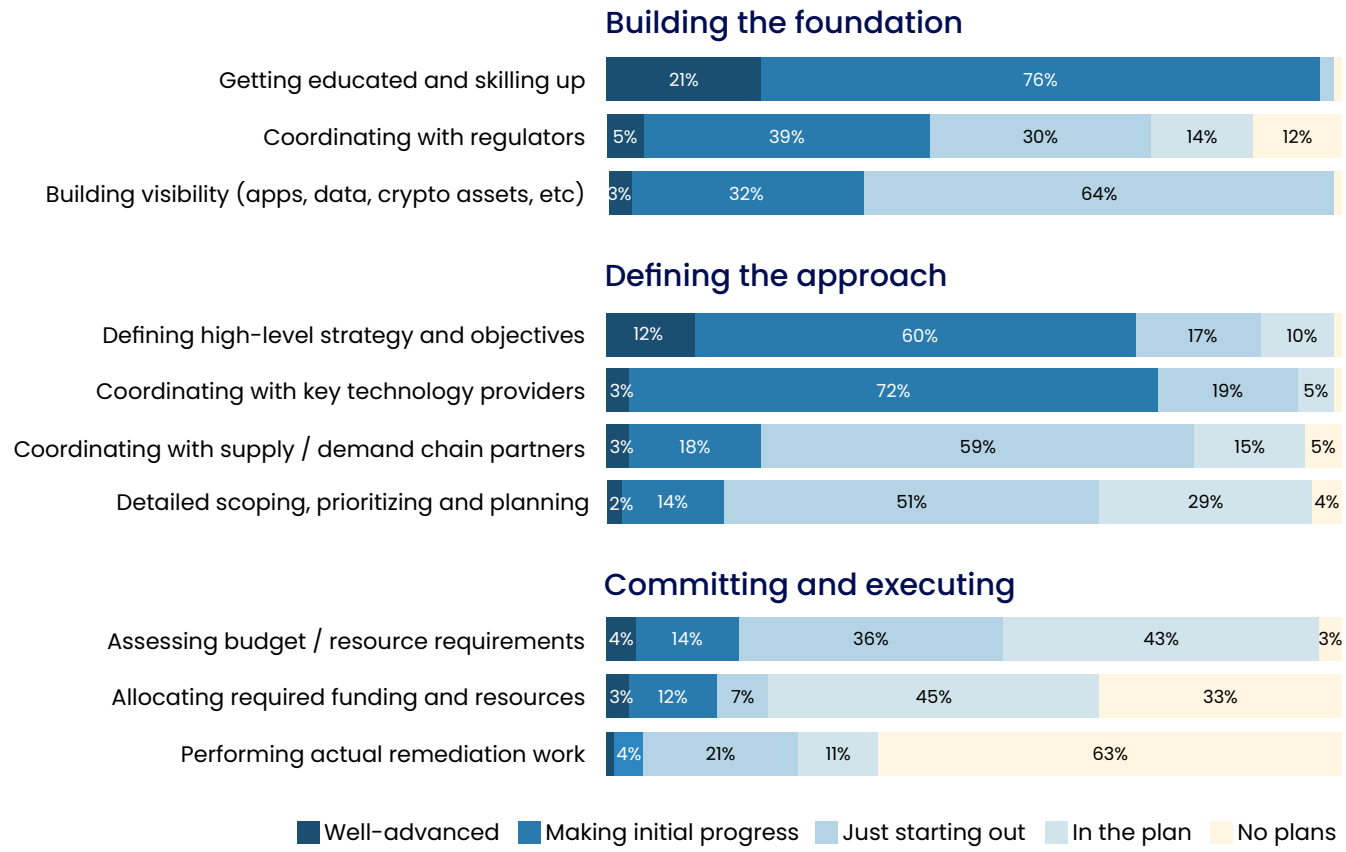

Most of what appears on this chart will ultimately cost money in one way or another, yet despite over half already having a clear board mandate, only a quarter are on a firm footing with regard to budgets at the moment. That gap likely reflects the fact that organizations don't yet know enough about the detail of what's required to make a credible ask. This is borne out when we look at levels of progress.

Copyright 2026 Freeform Dynamics Ltd

# A lot of ground to cover

A PQC program involves a broad set of activities, from building foundational level knowledge and understanding, through defining your approach, to committing resources and executing. And despite our study sample being more advanced than the general population, most are clearly still quite early in their overall PQC journey.

**How would you sum up your progress to date in relation to Post Quantum Cryptography (PQC) implementation in the following areas?**




The other thing that leaps out from this chart is the magnitude of the challenge. While we couldn't be exhaustive in capturing absolutely everything that needs to be done, even this high-level view shows how a PQC program can be a significant undertaking.

Looking more closely at the data, we can see that the bulk of activity to date has been concentrated in the first two phases, and it's interesting to note parallel activity across these. This reflects the iterative approach that our earlier finding told us most see as necessary. For example, you may have decided to initially focus on standard commercial applications - such as ERP or CRM - and might be currently working with vendors and stakeholders on defining your approach in this area. In other areas - e.g. cloud platforms and services - you might still be doing basic groundwork such as building visibility. This brings us onto the topic of objective setting and planning.

Copyright 2026 Freeform Dynamics Ltd

# Crystallizing the core challenge

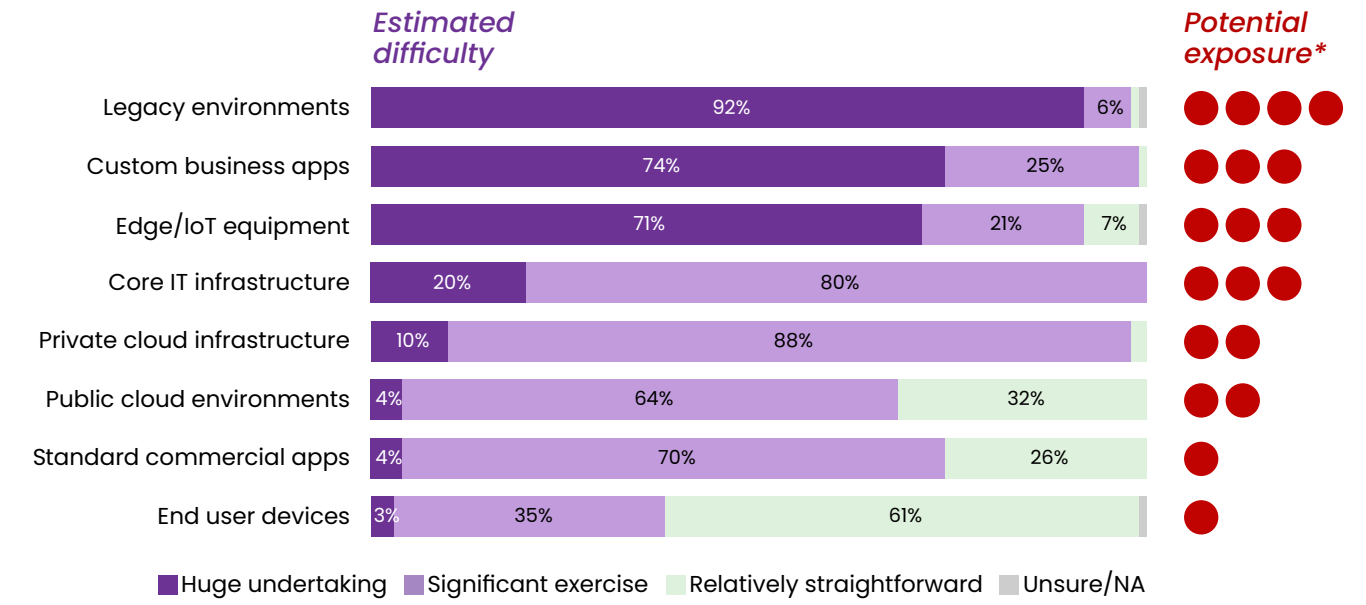
Defining appropriate objectives is clearly an important part of any PQC initiative, bearing in mind your goals may vary depending on which part of the business and/or which aspects of your systems you're targeting.

In some areas, you might simply focus on doing the minimum necessary to address shorter term risks and compliance requirements, i.e. look to achieve a state of 'crypto safety' with the minimum of cost, distraction and disruption. At the other extreme, you might aim for full 'Crypto Agility'. The idea here is to ensure that new or updated security architectures will allow future cryptographic changes to be made rapidly and efficiently. This is an approach that regulators and standards bodies currently advocate, and may well mandate down the line for some scenarios.

**The big challenge is that the areas perceived to represent the highest risk are also seen as the most difficult to address.**

The trouble is that implementing full crypto agility can be hard in areas like legacy environments, custom applications and edge/IoT deployments. And unfortunately, such areas also tend to represent the highest risk.

**How would you characterize the job of implementing full Crypto Agility in relation to the following? (with corresponding exposure indicators*)**




* *Exposure indicators derived from the weighted averages of responses shown on page 5*

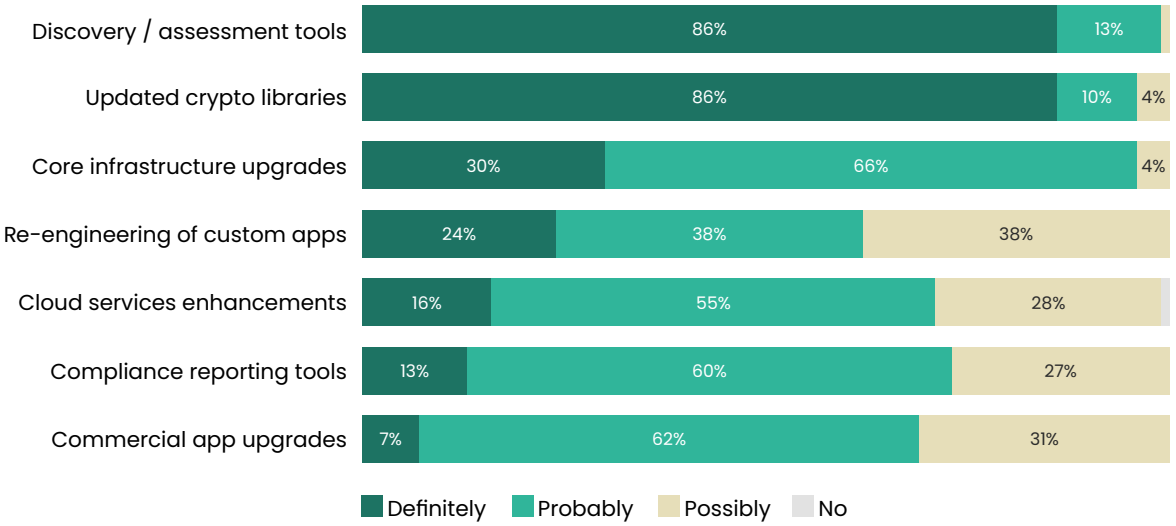
This chart sums up the PQC challenge in a nutshell, and underlines the need to act sooner rather than later. But what does this mean in terms of investments?

Copyright 2026 Freeform Dynamics Ltd

# Enabling the transition

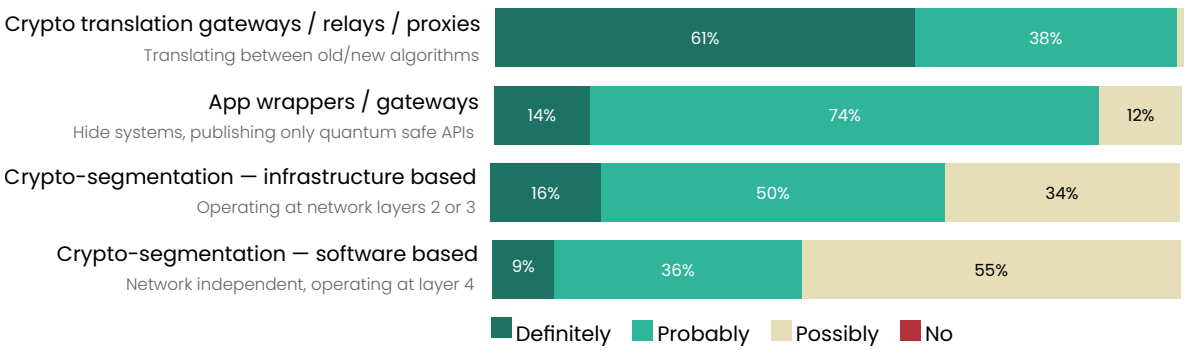
When we drill into some of the investments required to execute a PQC initiative, there's broad agreement on the need for discovery and assessment tools, and the deployment of updated crypto libraries. Beyond these, however, we see a lot less certainty, which again corroborates that it's still early days when it comes to assessment and planning.

**Do you see or anticipate a need to invest in any of these to support your PQC efforts?**




Something worth noting, however, is the potential use of what we might call 'shielding solutions'. If you have a legacy or custom application that's difficult to remediate natively, for example, one option is to intermediate traffic to/from it via a layer that translates back and forth between traditional and quantum safe encryption.

**Do you see a role for solutions such as the following that can shield hard-to-remediate assets from Quantum threats?**




Solutions like these can be implemented as a stop-gap until native remediation is possible, but in many situations can be used as a long term solution as they tend to be crypto agile by design. This can drastically lower overall remediation cost and effort.

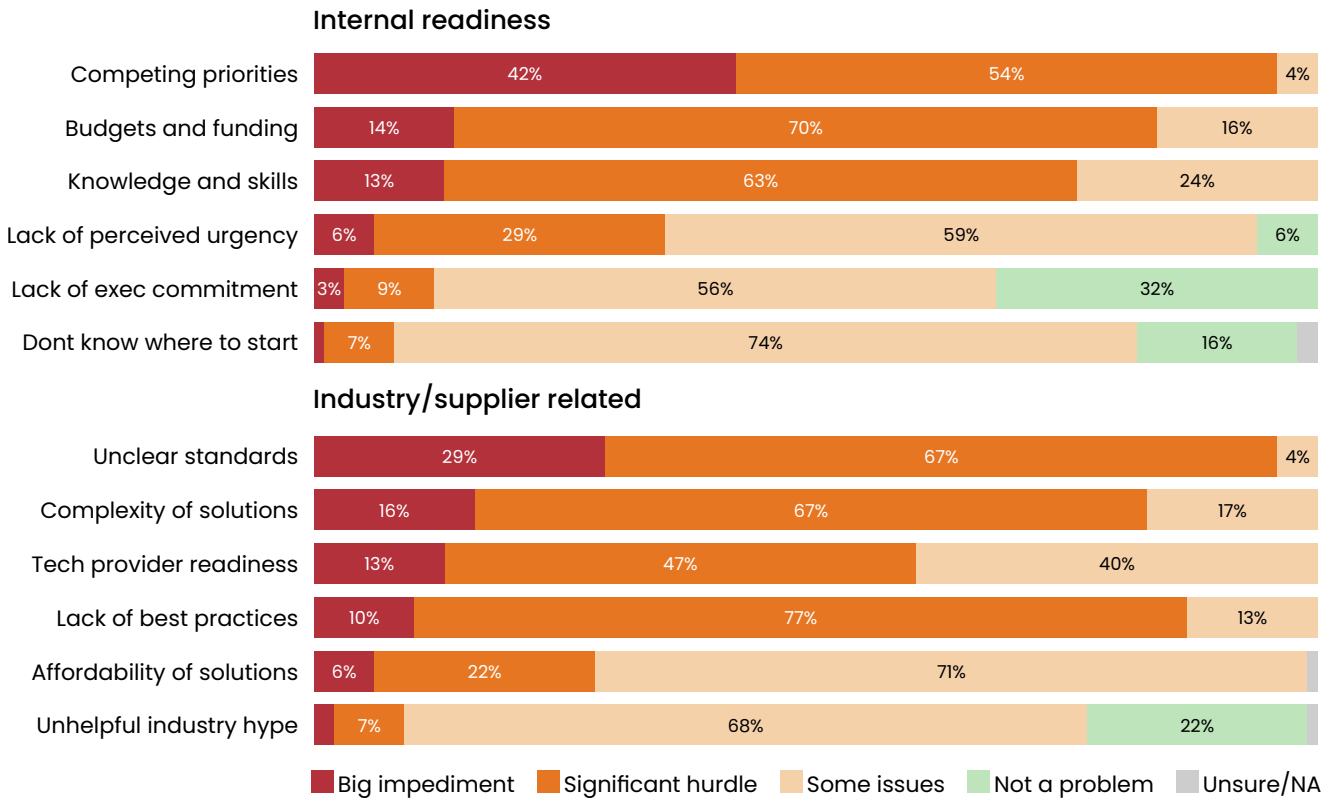
Copyright 2026 Freeform Dynamics Ltd

# Impediments to progress

Every transformational program faces hurdles and challenges, and PQC initiatives are no exception, with a mix of internal and external factors impeding progress.

From an internal perspective, competing priorities dominate the picture, which is unsurprising given that PQC is relatively new on the overall agenda, contending for attention and budget alongside AI, cyber resilience, cloud modernization and a host of other strategic demands. At the other extreme, lack of executive commitment is near the bottom of the internal issues list, suggesting that with PQC, it's more a question of 'when', rather than 'if', initiatives pick up momentum.

**To what degree are the following likely to impede your progress with implementation of PQC?**




Turning to external factors, the data signals a general perception that the industry lacks maturity at the moment. Unclear standards, solution complexity, lack of best practices, and questions about supplier readiness are all consistent with most players operating at the early part of the learning curve. However, this will clearly change as experience is gathered - solutions will become more refined and implementation patterns will crystallize, in turn boosting repeatability and predictability, while lowering overall cost, risk and uncertainty.

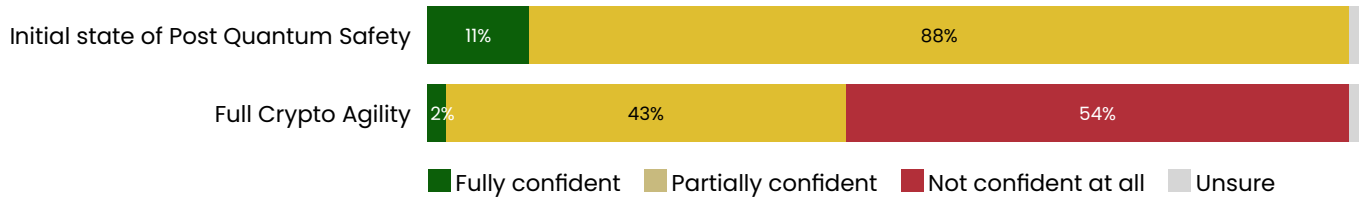
In the meantime, though, where does this leave people in terms of confidence to deliver on PQC requirements?

Copyright 2026 Freeform Dynamics Ltd

# Confidence and the value of experience

During the study, we asked respondents how confident they were in their ability to achieve both an initial state of post-quantum safety and full crypto agility within the timescales regulators are expecting.

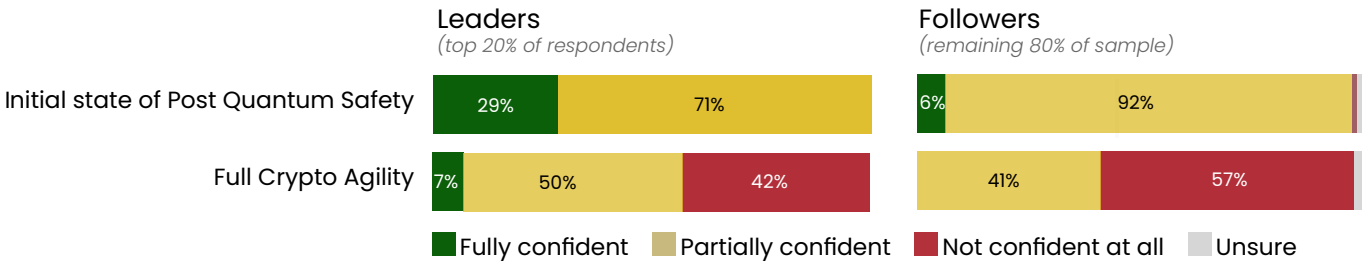
**How confident are you in your ability to achieve the following in the timescales that regulators are expecting?**




While arguably quite predictable, these responses underline the balancing act required when thinking through approaches to PQC remediation. As we said earlier, whether you aim for Quantum Safety, Crypto Agility, or use the former as a stepping stone to the latter, is a judgement call that will vary across different parts of your environment. In practical terms this is about balancing potential exposure, the effort and cost involved, and the resources available to you, always making decisions consciously and objectively.

Encouragingly, however, when we segment study participants based on their overall progress score (weighted average of responses shown on page 8), we see indications that confidence rises as you gain more experience.

**Impact of progress/experience on confidence**




This doesn't mean the challenges shrink in absolute terms, it's more that progress and experience breed greater levels of understanding and insight, which in turn means assessments become easier and more accurate. To put it another way, the earlier you can build a foundation of experience, the quicker your planning moves from educated guesswork to something genuinely suitable for detailed budgeting, resource planning and roadmap development - a strong argument for focusing on PQC earlier rather than later.

Copyright 2026 Freeform Dynamics Ltd

# Acting on the research insights

The picture that emerges from this research is one of an agenda that is still finding its feet, but is undeniably real. Regulatory timescales are set, the nature of the threat is broadly understood, and most of the organizations we spoke to have begun building awareness and defining their approach. Progress beyond these foundational stages remains limited for now, with the practical work of scoping, budgeting and executing still ahead for the majority.

However, none of this is cause for alarm. PQC is a significant undertaking, but a manageable one if approached with the kind of structured thinking and phased execution that organizations routinely apply to other complex programs. And as the data suggests, confidence rises as practical experience builds, which is encouraging.

## On the question of timing...

For organizations holding data with long-term sensitivity, the HNDL threat potentially creates a short-term reason to act. Either way, we recommend starting to engage with the PQC ecosystem soon if you haven't done so already. This will allow you to go beyond the generic guidance available from regulators and standards bodies, and gain more real-world perspective on requirements and solutions. As you do this, you are likely to find the industry is actually further ahead than you previously thought.

**The PQC ecosystem is maturing faster than you might think. Early engagement with key technology providers is one of the most productive steps you can take right now.**

Discovery and assessment tooling provides a good example here, where investing early often reduces the need to spend on expensive consultants. Shielding solutions - API gateways, proxies, and micro-segmentation solutions - represent another example, in this case aimed at protecting legacy and other systems for which native remediation would be prohibitively hard or expensive. The right solution(s) in this space can enable both near-term compliance and longer-term crypto agility.

## Final thought

The organizations in our study that are furthest ahead didn't get there by waiting for perfect clarity. They accepted the uncertainty, started where they could, and refined their approach as they learned. That's a pattern worth considering - not because the sky is falling, but because the window for a measured, well-planned response is at its widest right now.

Copyright 2026 Freeform Dynamics Ltd

# About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information, please visit: https://www.freeformdynamics.com.

# About Certes

Certes provides Data Protection and Risk Mitigation (DPRM) solutions that deliver PQC for any application, over any infrastructure, anywhere. By protecting the target of cyber-attacks, the data itself rather than relying solely on perimeter and infrastructure defenses, Certes helps organizations secure what matters most, reduce financial and operational risk, and retain sovereign control of their most valuable data.

Headquartered in the United States, for more than 20 years Certes has been innovating data protection and cryptography solutions and boast more than 1,000 global customers. With more than a dozen patents, its solutions are designed to protect sensitive data wherever it moves, helping organizations strengthen resilience and safeguard critical information against unauthorized access and data loss.

Website: https://certes.ai/

LinkedIn: https://www.linkedin.com/company/certes-ai/

**Terms of use**
This document is Copyright 2026 Freeform Dynamics Ltd. It may be freely duplicated and distributed in its entirety on an individual one to one basis, either electronically or in hard copy form. It may not, however, be disassembled or modified in any way as part of the duplication process. Hosting of the entire paper for download and/or mass distribution by any means is prohibited unless express permission is obtained from Freeform Dynamics Ltd or Certes. The contents contained herein are provided for your general information and use only, and neither Freeform Dynamics Ltd nor any third party provide any warranty or guarantee as to its suitability for any particular purpose.