cambridge consultants
Part of Capgemini Invent

Regulator and industry perspectives on the current plan for PQC transition

Department for Science, Innovation and Technology

March 2025 | Final report

Table of contents

Executive Summary

This is a research paper and does not necessarily reflect HM Government policy.

Quantum computers (QC) are ushering in a new paradigm of computing, with the potential to solve currently intractable mathematical problems and to transform industries and economies. While still in the development stage, quantum hardware and algorithm development are advancing faster than initially predicted. But the speed and capabilities of quantum will bring about new threats, alongside these new opportunities.

Government and commercial organisations worldwide are making significant investments to develop cryptographically-relevant quantum computers. Within the next decade [1], quantum computers could be able to break encryption schemes commonly used for cyber security, compromising the privacy and security of digital communications and impacting individuals, organisations, and nations.

The purpose of this study, conducted by Cambridge Consultants and Capgemini on behalf of the Department for Science, Innovation and Technology (DSIT), was to explore how UK critical national infrastructure (CNI) organisations are engaging with the need to migrate their cyber security schemes to post-quantum cryptography (PQC). For cyber security to remain secure, organisations will need to replace many currently used cryptographic algorithms with 'quantum-safe' algorithms. This is not a trivial task: it will involve significant planning, investment and mobilisation of IT and cyber security teams, and will require buy-in from both senior management and on-the-ground operational teams.

Our study focused on five key CNI sectors in the UK: energy, financial services, healthcare, telecommunications (which in this report includes telecoms operators, IT services and communications infrastructure), and transport.

These five sectors were picked from the thirteen sectors that are recognised as CNI in the UK, as they cover a range of technical architectures and potential challenges for the adoption of PQC. The selected CNI sectors provide examples of different operational technologies, enterprise networks, and legacy systems. They rely on different types of data, require a wide range of data asset lifetimes, are subject to different resourcing constraints and regulatory regimes, and are driven by a range of different security goals (e.g., consumer privacy, confidentiality, data integrity, operational safety).

We conducted primary research to support our analysis, including 21 industry and regulator interviews and a complementary online survey on PQC readiness. We interviewed one UK regulatory body from each of the five focus sectors.

Note: The UK's National Cyber Security Centre (NCSC) released guidance on timelines and a roadmap for PQC migration for critical sectors at the end of March 2025 – just before publication of this report, and after the interview and survey programme were completed. Points that have been highlighted in this report regarding unclear timelines for PQC migration should be considered in this context.

Key takeaways from the research

1. Overall, around 50% of respondents for both interviews and the online survey believe the quantum threat to cybersecurity will become reality in the next 10 years. However, for many, PQC is not yet a high priority, due to other, more immediate cyber security risks. There is a risk that the quantum threat is not being properly assessed by organisations, and also that migration timelines are being underestimated by industry.
2. PQC migration is a complex task, and respondents indicated they were struggling with uncertainty around migration timelines, business justification (Return on Investment, RoI), and technical readiness. While many organisations we interviewed and surveyed have begun planning, a mix of skills shortages, infrastructure complexity and legacy systems, and supply chain immaturity are hindering progress.

3. Some sectors are likely to need more (or different) support than others, on planning for and executing PQC migration. For example, interviewees and survey respondents in the finance and energy sectors were more likely to be taking proactive steps towards PQC migration, and these sectors generally are more cryptographically mature; while telecoms, healthcare and transport respondents were more likely to be taking a 'wait and see' approach, due in part to the greater challenges they face due to infrastructure complexity and reliance on the vendor supply chain.
4. Government support was seen as crucial for driving PQC adoption across CNI sectors, with regulators, academia, and industry stakeholders calling for clearer guidance, structured transition plans, and greater regulatory engagement. Targeted support is needed to help overcome common challenges such as technical expertise shortages, uncertain timelines and RoI, and supply chain readiness. In addition, government can help by setting up more formalised forums or interest groups to facilitate cross-collaboration and technical engagement between vendors, academia, regulators and industry experts, which a number of interviewees suggested would be valuable.
5. Regulators have a critical role to play in their own right, as well as supporting broader government initiatives to drive PQC migration. A number of respondents highlighted the lack of PQC standards as an issue – regulators can assist here by supporting development of standards, by ensuring sector interests are represented.

Summary of main findings

Context for PQC Readiness: Organisations' Cyber security Goals and Maturity

- Continuity of operations and ensuring customer data protection clearly emerged as the most important cyber security goals. There was high consistency across industry sectors in prioritising these two top goals, which appeared in the top 3 ranking of survey respondents in every one of our five CNI focus sectors.
- Based on the responses to our survey, the energy sector appeared to be the most cryptographically mature among the five U.K. CNI sectors. Finance, healthcare, and telecoms rank in the middle. Financial organisations are actively inventorying cryptographic assets – a key precursor step to planning PQC migration. Transport respondents indicated their sector had the most limited cryptographic awareness and maturity, with many respondents unsure of their organisations' cryptographic strategies and implementations (see *Section 2.2.1.2* and *Appendix D: Online survey methodology details* for more detailed discussion)
- Data security requirements varied widely by sector. Energy sector data retention requirements range from 10 years (trading) to 70+ years (nuclear). Finance must keep customer data for up to 120 years in some cases. Transport is responsible for cyber-physical system security for up to 80 years. These timelines are relevant for PQC migration planning for several reasons. One is that organisations need to consider the possibility of quantum-enabled 'harvest-now-decrypt-later' attacks. In such attacks, securely encrypted data could be intercepted now (or in the future), stored, and then made accessible to adversaries at a later date when they have access to quantum computers that could decrypt the data. The long data retention periods for many CNI sectors mean data will likely need to be kept secure well beyond the time when a cryptographically relevant quantum computer first becomes available, so employing PQC to protect data in advance of this will be important. In addition, CNI sectors such as transport manage cyber physical systems that are being deployed today, but will be in the field for decades; such systems must remain resilient to cyber-attack far into the future. CNI organisations may wish to consider deploying PQC now, to avoid having to undertake expensive early replacements of cyber physical systems if quantum attacks become a reality sooner than expected. Considering this as an up-front action, rather than later having to retrofit PQC to systems that are already deployed, will likely reduce the total cost of ownership.

- In terms of overall security planning and strategy, CNI organisations rely heavily on the supply chain to support cyber security activities. This may hinder organisations' visibility of their own cryptographic estates, and means that the supply chain must be a key part of thinking and discussions around PQC migration strategy. Approaches to working with third party security vendors varied significantly between sectors. The healthcare and energy sectors were much more likely to partially or fully outsource cyber security planning, whilst at least half of finance, telecoms and transport respondents reported strategy and planning were kept fully in-house. In contrast, for ongoing cyber security deployment, management and updates, the approach was more uniform across sectors, with few respondents keeping these activities fully in-house; most used at least partial outsourcing.
- Regulators' main cyber security objectives were ensuring safety of people, and privacy. Their secondary objectives included ensuring that firms are following the NCSC guidance, keeping up with emerging threats, and managing stakeholder groups. Regulators noted that many different technologies are used in the five CNI sectors covered in this study, and that a variety of cryptographic approaches and algorithms are being used as a result; so PQC-related guidance and regulation would need to take into account the differences in sector technology strategies and overall concerns.

Awareness, Understanding and Preparedness for PQC migration

- Most respondents had a good grasp of the threat of quantum-enabled attacks on cyber security, although levels of technical expertise differed. The 'harvest-now-decrypt-later' attack threat was highlighted by many interviewees. Asymmetric cryptography was cited as a major concern by more than 3/4 of interviewees, who recognised the significant threat quantum computers pose to their organisations' security. Public Key Infrastructure (PKI) was seen as particularly at risk.
- All interviewees acknowledged the risk of quantum computers to cyber security. Overall, ~50% of respondents for both interviews and the online survey believe the quantum threat to cybersecurity will become reality in the next 10 years. However, for many it, PQC is not yet a high priority, due to other more immediate cyber security risks. Another reason might be that the threat is not being properly assessed by organisations (as acknowledged by some interviewees – notably in the finance, healthcare and telecoms sectors). There is a consensus that regulatory mandates and compliance-driven initiatives will help drive action.
- Some sectors, such as finance and energy, are taking proactive steps towards PQC migration, while telecoms, healthcare and transport face greater challenges due to infrastructure complexity and vendor dependencies. Some academics indicated – and we agree – that there is a risk that migration timelines are being underestimated by industry, highlighting the need for structured planning, clearer guidance, and stronger industry coordination.
- Interviewees and survey respondents consult with a range of sources and organisations for support in understanding PQC. Among survey respondents, news sources were mentioned most frequently as a source of PQC information. Interviewees indicated they look to different national organisations for regulatory guidance such as the National Cyber Security Centre in the UK (NCSC), or the National Institute of Standards and Technology (NIST) and the Cyber security and Infrastructure Security Agency (CISA) both in the US. Some also mentioned following the NCSC's Cyber Assessment Framework (CAF), although this does not yet include PQC. Others look to sector regulators or industry cyber security groups. Also mentioned were standards organisations like the American National Standards Institute (ANSI) or the European Telecommunications Standards Institute (ETSI). Some interviewees are already engaging with experts **-** notably supply chain vendors but also consultants - to stay informed about PQC developments. Universities have significant quantum expertise, but are not engaging significantly with industry. The role of UK

Research and Innovation (UKRI) in facilitating such engagement through the Digital Futures Institute and its quantum networks was also mentioned.

- The regulators we interviewed clearly understood the impact that quantum computers will have on the development of cyber security, and were familiar with both types of potential attacks (including 'harvest-now-decrypt-later'), and the types of cryptography most at risk (e.g., RSA). Most thought that compared to other threats, quantum computers lie in the middle of the stack – in other words, they are not the most pressing concern right now. Regulators' views on the timeline for the quantum threat varied, with one regulator (financial) estimating a timeline of 'less than 5 years', one estimating '5 to 10 years' (energy), and two estimating '10 to 15 years' telecom and transport). All regulator interviewees said they were monitoring technological advances in the quantum field.

Incentives and Drivers for PQC migration

- A key driver is the requirement to manage long-term assets, which entails an ongoing need to evaluate and prepare for future risks. This is particularly the case for the energy and transport sectors. PQC will need to be considered in long-term roadmaps, which are a common requirement in infrastructure-heavy sectors.
- Interviewees noted the importance of creating a cost/benefit case for PQC migration, to ensure that sponsors (regulators and internal) would be able to justify the spend, and to highlight the economic benefits to those who adopt the technology.
- Regulation and standards are critical drivers, with NIST's standardisation and push on quantum security being commonly referred to. Some recognised the push that NIST is providing, in regard to quantum security.
- Survey respondents highlighted the importance of being able to use quantum security as a business differentiator – nearly 60% of respondents cited this as a top 3 driver. However, interviewees were far less likely to mention this as a driver for PQC migration. Availability of sectoral guidance, regulatory and legal requirements, greater evidence of the quantum threat, and improved understanding of PQC in their organisation were also cited by survey respondents cited as important drivers for taking action on PQC migration,
- Regulators themselves highlighted that legislation from government is likely to be the strongest driver for PQC migration. They also viewed building a business case for PQC migration as viewed as essential to keep pushing migration progress forward. One regulator's view was that if the business case focused on the economic impact of *not* adopting PQC (e.g. potential for operational disruption, IP theft, critical data hitting a GDPR stamp), it would make migration compelling enough for companies to invest in.

Challenges and Blockers for PQC migration

- PQC migration is a complex task to consider, and industries are struggling with uncertainty around migration timelines, business justification, and technical readiness. While some sectors have begun planning, a mix of skills shortages, infrastructure complexity, and supply chain immaturity continue to hinder progress.
- Many CNI organisations lack expertise in post-quantum cryptography, which is also slowing progress on PQC migration. Additionally, uncertainty around the longevity and stability of PQC algorithms creates hesitancy in committing to migration; organisations are reluctant to commit to an investment in PQC when such algorithms could eventually prove to be ineffective/breakable, or could introduce new risks inadvertently.
- There is a lack of clear financial impact assessments, making it difficult to justify investment over other and more immediate cyber security concerns. Resistance at the senior management level in

organisations is exacerbated by challenges in communicating the quantum threat to non-technical decision-makers.

- Legacy systems, complex IT/OT (Information/Operational Technology) integration, and a lack of PQC-ready solutions from vendors also create significant barriers to implementation. Many organisations remain dependent on suppliers who are not yet prioritising PQC migration, further delaying progress.
- There is some variance between sectors on the perceived challenges and blockers. Telecoms respondents were the only sector group that did not identify the skills gap as one of their top two challenges, instead highlighting the lack of PQC standardisation as the most critical barrier. Healthcare and finance sector respondents explicitly identified cost concerns as a dominant issue.
- Regulator interviewees identified a number of technical barriers they were concerned about, including legacy systems which will be difficult to upgrade for PQC, and dependence on quantum research results from tech hyperscalers (e.g. Google, Microsoft, Apple, Meta, etc.). Non-technical barriers that regulators saw as critical were largely aligned with what we heard from industry end users: Lack of relevant cryptography knowledge among people working in cyber security and broader cybersecurity and IT skills gaps; lack of board buy-in and related to this, uncertainty around PQC timelines; Cultural barriers: and costs/access to funding.

Government measures to support PQC migration

- Government support is seen as crucial for driving PQC adoption across CNI sectors, with regulators, academia, and industry stakeholders calling for clearer guidance, structured transition plans, and regulatory engagement. Targeted support is needed to help overcome common challenges such as technical expertise shortages, uncertain timelines, and supply chain readiness.
- Some priorities identified by interviewees and survey respondents are sector-specific; for example, finance respondents focused on support for regulation and compliance, healthcare and transport respondents specifically mentioned help with vendor collaboration and small-medium enterprise (SME) support would be valuable, and telecoms respondents stated they would value support on establishing common PQC standards across their industry.

The Regulator View

Regulators have a critical role to play in driving and supporting PQC migration in the UK. They have the power to set technical standards, and to encourage the adoption of risk-reducing technologies (such as PQC).

Regulator guidance on cyber security is not immediately mandatory in all cases, but failure to adhere to it after receiving a direct request from a sector's competent authority (as defined by the UK's interpretation of the NIS Directive, which is typically the relevant sector regulator) can result in significant financial penalties.

Regulators we interviewed for this research recognised the risks of quantum to cryptography, and the scale of the challenge. Based on the interviews, they are currently hesitant to mandate standards for specific PQC algorithms, given the rapid evolution of cryptographic solutions. One respondent pointed out that regulation often struggles to keep up with fast-paced technology development.

Regulators emphasised the need for a coordinated, consistent approach to PQC regulation, ensuring guidance is aligned where possible, while allowing for necessary sector-specific differences.

Regulators' views on their own responsibilities regarding PQC included:

- Regulators have a responsibility to ensure guidance on PQC migration from NCSC and government (e.g. DSIT) is in place and clearly communicated to stakeholders, and that they, as regulators, are engaging consistently.

- Regulators should be driving collaboration across CNI industry players, academia and government to ensure consistency and feasibility of regulatory guidance or mandates.
- One regulator pointed out that any regulation should be developed in close conjunction with industry, to ensure that recommendations and expectations were feasible (and this view was also echoed in several of our industry end user interviews).
- At the sector level, the energy sector regulator opined that PQC is a large-scale problem that will take significant effort to address.

In our view, it will be important for regulators to undertake a concerted program of communicating more specifics and clear guidelines about PQC and the quantum threat, at the sector level as well as more generally, in order for key industries to really engage with planning for migration. This should be done prior to taking any specific regulatory action on PQC.

We are also conscious that regulators may be looking to take a light-touch approach, in order to minimise the legislative burden on organisations they regulate. When combined with the complexity of understanding quantum technology and its likely evolution, this could be holding back regulators from taking timely action on areas such as standardisation and mandating PQC migration timelines. Close engagement with the NCSC, as the UK technical authority in this area, will be absolutely critical to achieving successful outcomes.

Recommendations and Next Steps

Overall, the research undertaken for this report indicates that PQC migration is perceived by UK critical national infrastructure players as significant, but not yet a high priority for investment.

The following recommendations focus on how government and regulators can help to drive awareness of the need for PQC migration, address the most critical barriers to progress, and ensure that UK organisations move forward effectively to address security risks. Please note that recommendations are based on the authors' views, as informed by the outcomes of this research (including - where relevant - specific suggestions from interviewees), and by our understanding of the technology and policy environment. Our recommendations are that government and regulators should:

1. Address uncertainty around PQC timelines, by collating and sharing informed estimates for the Q-Day (timeframe for a likely quantum-enabled attack) for commonly used cryptographic algorithms.
2. Develop and disseminate a clear, single source of guidance for PQC migration – this could be provided at a central level by the NCSC, but also needs a clear sectoral-level overlay to address the specific context and complexities of each CNI sector. This should emphasise the importance of cryptography for achieving organisational goals, the need to invest to protect information from quantum computers, and the business case for PQC migration.
3. Produce guidance and disseminate information specifically targeted at board members and other senior management-level stakeholders.
4. Work with industry and academia to develop training for organisations looking to upskill their staff. Couple this with development of a formal register or certification, to allow industry to recognise quality support.
5. Publish a list of intensive training courses that can help technical employees to get up to speed on PQC and cryptographic migration.
6. Establish a network of PQC working groups, at a cross-sector and sector-specific level. The groups should involve academia, government, regulators, industry and standards bodies. These should share best practice and encourage collaboration on PQC migration.
7. Ensure that the need for quantum-safe products is clearly articulated as an opportunity for technical suppliers, and help to drive development of a vendor ecosystem.

8. Provide guidance and advice on scoping exactly what activities will be required for PQC migration. This should include identifying what skills and resources those activities need, and advising on how to judge the scale of the investment required. Expected migration timelines should be presented alongside the estimated timeframe for a cryptographically relevant quantum computer to emerge. Regulators are in a strong position to contextualise this advice, and to ensure that sector-specific considerations are reflected in their dissemination of this information.
9. Highlight the risks associated with adopting PQC, as well as the risks of not adopting it, so that organisations can make informed choices and manage risks appropriately.
10. Build a communications and dissemination plan to reach out to the wider ecosystem to achieve the above objectives.
11. Consider when and how best to take specific regulatory action to mandate PQC migration (e.g., by a certain date). While this may seem an obvious way to drive migration, the research conducted for this study indicates that most UK CNI organisations are still far from ready to start on the journey. Given the complexities of planning for and deploying PQC, industry interviewees – who contributed several of the above recommendations – indicated that it would be valuable to action some of the suggestions above, prior to taking regulatory action. Several interviewees also emphasised the importance of developing policy and regulation on PQC collaboratively with regulated organisations, to ensure that regulations are practical and achievable. This desire was echoed by regulators themselves, who felt that they were in a good position to translate high-level PQC guidance from the NCSC and government into the language of their stakeholders, and to provide relevant sector-specific context.

Further explanation and guidance on these recommendations can be found in Section 5 Conclusions and recommendations.

1. Market and technology context for PQC

1.1 Why PQC matters – the quantum computing threat

Quantum computers are ushering in a new paradigm of computing. Quantum algorithms and hardware will enable the solution of currently intractable problems, and will open the door to transformation of numerous industries, from biosciences and pharmaceutical R&D to financial analysis and forecasting. While still in the development stage, quantum hardware and algorithm development is advancing significantly faster than initially predicted. This opens up many exciting opportunities, but also introduces significant new threats; in particular through quantum's ability to break cryptography schemes that are widely used for cybersecurity.

Governments and businesses are becoming more aware of the promise and the threat of quantum. A recent Capgemini Research Institute survey [2] reports that 55% of top executives and 44% of Venture Capitalists (VCs) expect quantum computing to be one of the top three technologies in the 'Computing & Networking' sector.

2025 is the United Nations' International Year of Quantum, and the technology will see a significant push in multiple sectors this year [2]. he increased awareness of quantum technologies is intended to drive governments and private sector organisations to fund work exploring potential uses of quantum (see Appendix B: Supporting technical information), and highlight the risks that PQC will need to mitigate.

Governments and commercial organisations worldwide are investing significantly to develop cryptographically relevant quantum computers. Within the next decade [1], we expect that quantum technology will progress to the point where it can compromise the privacy and security of digital communications everywhere, impacting individuals, organisations, and nations.

Quantum computing is a particular threat to public-key cryptography. It will potentially make currently prevalent encryption methods obsolete, and jeopardise the integrity of widely-used digital assets from passwords to digital signatures (see Appendix B: Supporting technical information). Quantum computers could enable threat actors to breach government and enterprise security, disrupt public services and utilities, interfere with financial transactions, and compromise personal data.

According to NIST, the emergence of a credible quantum threat to cryptography is generally thought to be around 10 years away [1]. But with accelerating progress in the development of quantum technologies, this timeline is potentially compressing. As well as direct attacks on future systems, there is also the threat of quantum-enabled 'harvest-now-decrypt-later' attacks that make use of encrypted data captured today. Given the advance planning needed for security strategies – and the complexity of applying those in critical national infrastructure environments with significant operational technology needs and existing (and long-life) infrastructure – businesses and governments need to start planning for the quantum threat well in advance of the technology becoming a reality.

1.2 The Post-Quantum Cryptography solution

The term "post-quantum cryptography" (PQC) refers to an approach that cyber security teams and developers can use to mitigate the risks posed by quantum computers to cyber security schemes. Essentially, the idea is to replace currently used cryptographic algorithms that are likely to be easily broken by quantum computers. This will involve deploying new cryptographic schemes, based on algorithms that are difficult to break for both classical and quantum computers. PQC is a collection of such algorithms, that allow secrets to be exchanged and data to be signed in a way that does not leave systems vulnerable to quantum-enabled cyber attacks.

In 2016 the National Institute of Standards and Technologies (NIST), a US government agency, began standardising quantum-safe algorithms for key agreements and digital signatures. They have released 69 candidate algorithms for expert analysis. In August 2024, NIST [1]introduced three encryption standards designed to resist quantum computer attacks on digital information and systems. The new standards address two primary encryption tasks that are critical for protecting information used in day-to-day communications and transactions: general encryption for protecting information exchanged over public networks, and digital signatures for identity authentication. (see Appendix B: Supporting technical information)

Assessing the threat posed by quantum computers to systems, products, and applications is complex (see *Appendix B:* Supporting technical information for more detailed technical discussion). The introduction of these quantum-resistant encryption standards is an important step, but is not the solution to the quantum threat in and of itself. Testing these standards fully, assessing where they can be applied, and undertaking the process of rolling them out across both new and existing cryptographic estates are all critical parts of the process.

NIST notes – and cyber security managers around the world will certainly agree – that it usually takes a long time for a new algorithm to be fully integrated into information systems, since organisations need time to incorporate such algorithms into everyday products and services. Many essential components of cyber security infrastructure within both government and industry sectors have not been updated for many years. Rolling out PQC will involve significant considerations around cost, disruption to operations or systems, and other challenges (see Section 1.3).

The PQC migration process will therefore be complex, requiring a gradual approach and meticulous planning. Starting the process now can help avoid unexpected issues and facilitate an orderly transition.

1.3 Technical challenges of PQC migration

PQC implementation entails a range of technical challenges. Some are typical of large-scale digital upgrade projects, while others are unique to projects that focus on cryptography and communications. A few are associated with properties of the PQC algorithms themselves.

In the primary research programme conducted for this study, we asked industry, academic and regulatory stakeholders about their most important technical challenges relating to PQC (see Sections 2,3 and 4).

Ahead of the primary research phase, however, we also identified a set of broader PQC technical challenges as initial hypotheses. These technical challenges were selected for their relevance across all sectors, though the interviews and survey findings summarised in Section 2 highlight that their immediate relevance varied between sectors.

The most important PQC technical challenges we see are:

- **Robustness and maturity of PQC solutions and standards**: The real test of any cryptographic algorithm is that it remains secure in the field. However, the new PQC standards selected by NIST are yet to be widely deployed in real-world applications [3]. Security evaluations of post-quantum schemes using classical computers have been led by laboratories around the world, but these only add confidence rather than proof that the algorithms will be robust to wide scale cryptoanalysis by adversaries. Their robustness against quantum computers is less certain still, as without a quantum computer of cryptographic relevance, assurances can only be theoretical. These factors culminate in significant uncertainty about the long-term effectiveness of PQC. This challenge was also identified as a key issue by interviewees and survey respondents in the primary research conducted for this report.
- **Legacy systems**: Legacy systems often run on outdated or proprietary software and hardware that are not compatible with new cryptographic algorithms. Generally, cryptographic algorithms cannot be changed until all parts of a system can handle the new ones [4]. Updating protocols and infrastructures often accompanies the introduction of new algorithms, making replacements lengthy and disruptive, sometimes taking decades. Implementing PQC standards would require costly and time-consuming modifications. When upgrading existing legacy systems [5] is not

feasible, organisations can deploy middleware to connect legacy systems with newer cryptographic standards, isolate systems that cannot be upgraded, and introduce quantum-safe encryption elsewhere to mitigate risk. Additionally, they can plan a phased migration to new platforms that support quantum-safe algorithms, reducing reliance on legacy infrastructure over time. This challenge was also identified as a key issue by interviewees and survey respondents in the primary research conducted for this report.

- **Secure implementations of PQC**: Implementing post-quantum algorithms presents security challenges in itself [5]. One area of concern is the potential vulnerability of PQC algorithms to side-channel attacks [6]. Such attacks would allow an adversary to deduce the private key of a target by monitoring the electromagnetic emissions from an FPGA implementing the target's cryptography. Standard countermeasures against side-channel attacks are difficult to implement in PQC algorithms as the underlying algorithms have multiple decision-points that rely on secret variables that all need to be protected, whereas algorithms such as RSA access secret variables in a more consistent way, meaning one standard fix can protect the entire algorithm [7] . This was also highlighted as a challenge by a subset of our interview and survey respondents.
- **System hardware constraints**: PQC improves security against quantum threats but can result in lower performance due to the increased computational, bandwidth, and storage requirements compared to traditional cryptographic algorithms. This has the potential to reduce performance for systems operating at scale or where latency has to be kept to a minimum. To mitigate these performance issues, cryptography can be implemented using hardware acceleration [5]. However, new hardware, especially new hardware that requires security testing, comes at a greater cost than software implementations.

1.4 Non-technical challenges of PQC implementation

PQC implementation also brings a range of financial, organisational and regulatory challenges. We present our initial view on these challenges in this section; again, in-depth views from industry end-users and regulators are discussed in Sections 2-4 of this report.

The most important PQC financial challenges we see are:

- **Staff costs**: Estimating the exact costs of PQC migration is challenging. Organisations must estimate and allocate requirements for personnel, time, and funds [8].
- **Hardware replacement costs**: Some hardware might need replacement if it cannot support PQC, and current cryptographic hardware may fall short . Additional software complexity may introduce unacceptable latency into the communications process, or some dedicated hardware encryption devices may lack the memory to perform the computation at all.
- **Cost of replacing cryptographic estate**: Organisations often do not realise the extent of their reliance on public-key cryptography [4]. Many cryptographic tools and protocols will need replacement or major changes when migrating to PQC.
- **Prioritisation of funding**: Organisations' lack of impetus to address quantum threats can hinder the PQC transition. Organisations need to allocate appropriate funds, have a clear roadmap, and implement coherent policies to support their teams through this process.
- **Potential downtime** due to operational impact is another cost factor.

The most important PQC organisational challenges we see are:

- **Inflexible IT and OT systems**: Information systems may lack the flexibility to quickly adopt new cryptographic methods without significant infrastructure changes, requiring considerable manual effort. In some organisations the responsibility for securing IT and OT systems is split between IT Security and Engineering departmental silos, requiring inter-departmental collaboration.

- **Maintaining interoperability**: Maintaining connectivity and interoperability among organisational systems will be a significant challenge during the transition to PQC. This is especially challenging in sectors where multiple organisations need to regularly communicate to achieve sector goals (such as grid balancing systems and energy generation systems in the energy sector, or communications infrastructures operated by multiple operators in the telecoms sector) so no one organisation can drive migration without cross-sector collaboration.
- **Planning the migration sequence**: Organisations need to conduct a thorough analysis of the interdependencies among systems to determine the migration sequence. They must also identify and evaluate sources for components, solutions, and services. Failing to plan carefully may result in [9]:
    - Migration projects executed in silos, causing integration issues
    - Broken system functionality due to partial component migration
    - Higher costs than necessary
    - Increased complexity and unpredictable creation of novel risks as PQC and quantum evolve.

The most important PQC regulatory challenges we see are:

- **Lack of global harmonisation**: The lack of harmonisation in PQC preparedness across regions could complicate operations and increase compliance burdens for global entities. Organisations that operate in regions where cryptography skills are rarified could be left behind if they are unable to deploy software that allows them to interface to global systems that are protected by PQC. This is particularly concerning in sectors where international collaboration is essential to the effective and safe operation of services. For example, in aerospace, where The International Civil Aviation Organisation has instituted a "no country left behind" initiative to support countries who find implementing technical guidance that is important to safety and interoperability challenging.
- **Unclear regulation**: when regulation is not adequately supported and falls behind technology, it can create uncertainty, where non-compliance is justified by explaining the regulation does not adequately cover a scenario or technology. This uncertainty creates divergence and failures of interoperability. For example, legacy guidance recommending cryptography that is known to be vulnerable is likely to be ignored by some organisations who are motivated by achieving risk management rather than compliance, or fastidiously followed by organisations who view security as a check box exercise.

1.5 Timing considerations when planning for PQC deployment

Despite the challenges, there are a few important drivers for organisations to start planning for PQC migration. We explored these drivers with interviewees and survey respondents in the primary research programme discussed in Sections 2-4 of this study.

Alongside these drivers, each organisation must consider how best to judge the priority and effort involved in deploying PQC schemes. These are closely related to the organisation's digital assets and risk profile. Key considerations are:

- **Shelf life of the systems and equipment**: Systems and equipment with a shelf life exceeding 10 years need to be prioritised.
- **Shelf life of data to be protected**: Data valuable for beyond the horizon of cryptographically relevant quantum computers requires prioritisation. 'Harvest-now-decrypt-later' is a significant

threat, especially for data that remains both relevant and sensitive in the time period where quantum computers are expected to become cryptographically relevant.

- **Migration timeframe**: The longer the estimated migration duration, the sooner the process should start.
- **Ability to track and understand impact of the rapid development of quantum systems**: Significant investments are being made to enhance quantum computers' performance across all layers, including hardware, software and algorithms. New techniques aim to accelerate progress, potentially reducing the time available to implement quantum-safe systems before systems could be at risk.

1.6 Relevance of PQC for industry

PQC adoption can help industries prepare for a quantum future by protecting data, ensuring compliance, safeguarding intellectual property, maintaining customer trust, and supporting resilience.

Industries are mostly likely to benefit from PQC if they:

- **Hold sensitive data**, i.e. confidential organisational information such as trade secrets, intellectual property (IP), and confidential information
- **Provide critical infrastructure**, i.e. complex systems critical for the functioning of society and economy, such as healthcare, utilities, and transportation
- **Handle personal data**, including financial services, healthcare, and public sector organisations handling data that needs to be protected for more longer than the expected date of emergence of a cryptographically relevant quantum computer.

Both the public sector and critical national infrastructure industries such as financial services healthcare (which have data and systems with a longer shelf life) face heightened risks as quantum computing evolves. Data like classified government information, financial records, and personal health records will remain valuable when error-corrected quantum computers become available. The growing threat of "harvest now, decrypt later" attacks highlights the need for security measures to protect such data. Critical infrastructure providers, including transportation, utilities, and telecommunications, should prepare by thoroughly understanding potential risks throughout their value chains.

Industry consortia and alliances have been established to address and safeguard against the security threats posed by quantum computers. Some initiatives focus on PQC by developing software for evaluation and prototyping, while others educate their industry communities by discussing the impact of the quantum-safe transition. Organisations across financial services, telecoms and energy (see Table 1.1)are actively engaged in integrating PQC systems and protocols into their existing digital security and communication infrastructures.

Table 1.1. Sector-specific post-quantum cryptography initiatives by industry

Industry	Initiatives
Financial services	Europol's European Cybercrime Centre (EC3) created the Quantum Safe Financial Forum (QSFF) [8], in cooperation with the EC3 Advisory Group on Financial Services to address the transition to PQC across the finance sector. QSFF published its recommendations [9] urging financial institutions and policymakers to prioritise the PQC transition.
	Bank for International Settlements Innovation Hub's Eurosystem Centre, in collaboration with the Bank of France and Deutsche Bundesbank, launched Project Leap [10] to prepare central banks and the global financial system for a transition towards quantum-resistant encryption.

	Emerging Payments Association Asia [11] established a working group with IBM, HSBC, AP+, and PayPal as founding members, to recommend steps towards implementing quantum-safe cryptography.
	HSBC and Quantinuum have successfully tested quantum-secure technology for buying and selling tokenised physical gold [12].
Telecoms	GSMA, IBM, and Vodafone established a Post-Quantum Telco Network Taskforce [13] to help define policy, regulation, and operator business processes for the enhanced protection of the telecommunications industry.
	The Security Enhanced Virtualised Networking for 5G (SEViN-5G) project [14], funded by Innovate UK, leveraged Ampliphae's network security analytics technology and Arqit's Symmetric Key Agreement Platform to deliver a quantum-secure Private 5G testbed that can protect against both current and future cyber threats.
	Vodafone collaborated with SandboxAQ, an Alphabet spin-off, to conduct a proof-of-concept test [15] for a quantum-safe Virtual Private Network (VPN) to access company systems securely via their devices.
Energy	Cambridge Consultants is partnering with National Grid ESO (Electricity system operator), the University of Edinburgh, and the University of Warwick on the "Network Security in a Quantum Future" project [16] funded by UK regulator Ofgem's Strategic Innovation Fund. The project aims to create a framework to identify risks to energy network cyber security, and to generate timeline estimates and readiness frameworks.

1.7 Public sector PQC initiatives and activities

1.7.1 UK public sector activities and initiatives

The UK's National Cyber Security Centre (NCSC) [17] believes that adopting post-quantum cryptography will serve as the most effective defence against the threat posed by quantum computing. The NCSC has advised that public-key cryptography algorithms used for key agreement and digital signatures can be made quantum-safe, and PQC implementations are possible in both software and hardware.

NCSC has issued the following guidelines [18] on how organisations can start preparing for migration to PQC:

- Enterprise IT system owners should discuss their plans for incorporating PQC support in their products with their IT system suppliers.
- Enterprise and custom IT system owners should financially plan to update their IT systems to use PQC. As systems are updated or replaced, new IT should either use PQC or be upgradable to PQC.
- PQC should be used based on robust implementations of final standards.
- Algorithms, such as ML-KEM-768 and ML-DSA-65, should be used for security and efficiency in most use cases.
- Protocol implementations based on RFCs (Request for Comments), rather than Internet Drafts, should be used for operational systems.
- A post-quantum/traditional hybrid scheme should be used as an interim measure within a flexible framework to smooth the transition to a PQC-only scheme in the future.

The transition to PQC is a national technology change programme for the NCSC. Its priority is to ensure that the UK's migration to PQC is seamless and does not introduce cyber risks to central government systems or critical national infrastructure. The focus is on increasing understanding, setting examples of effective practices, and identifying interventions by the NCSC that can have a broad impact. Table 1.2 lists the ways in which the NCSC will help organisations migrate to PQC across four broad initiatives [19].

Table 1.2. NCSC support for organisations migrating to PQC

<table>
<tr><th>NCSC Initiative</th><th>Description</th></tr>
<tr><td>Roadmap for PQC migration</td><td>During the production of this report the NCSC released new guidance [20] that outlines the essential steps for PQC migration. In addition it details how preparatory work may differ across various sectors, and provides recommendations on the timelines for critical activities throughout the transition to PQC.
Three-phase timeline for organisations to transition to quantum-resistant encryption by 2035.
By 2028 – define migration goal, identify cryptographic services that require upgrades and develop a migration plan.
By 2031 – execute highest-priority PQC migration activities and refine plans as PQC evolves.
By 2035 – complete migration to PQC for all systems, services and products.</td></tr>
<tr><td>Supporting PQC integration and policy formulation</td><td>The NCSC will support regulators in establishing appropriate guidelines and policies and offer direct advice to sectors where PQC integration is particularly complex.
Collaborating with the Cabinet Office and DSIT, the NCSC will develop policies for departmental migrations and offer tailored consultancy services.
The NCSC will assess the requirements for creating detailed departmental PQC migration plans.</td></tr>
<tr><td>Building expertise for PQC migration</td><td>The NCSC will provide high-quality consultancy services for post-quantum cryptography, encompassing deep expertise, migration planning, and large-scale system integration.
The NCSC is developing a pilot scheme to accredit specialist cryptography companies and assist them in finding markets in the UK.</td></tr>
<tr><td>Incentivising early adoption of PQC</td><td>NCSC’s market incentives [21] are expected to play a role in encouraging organisations to invest in PQC migration now.
Leveraging drivers such as liability, financial reward, transparency, and consensus to develop policy options would use network effects, the drive for profit, and the desire to maintain reputation to incentivise enterprises to prioritise security.</td></tr>
<tr><td>Identifying good practices</td><td>The NCSC aims to identify best practices and lessons from faster-moving sectors.
The NCSC target dates for PQC migration have now been released, to support decision-makers and risk owners for large organisations and CNI operators. It is noteworthy that the dates are guidance only.
The NCSC will collaborate with regulators to assist them in setting appropriate targets for each sector individually.</td></tr>
</table>

1.7.2 Activities and initiatives outside the UK

Governments and organisations worldwide, including those in the US and Europe, recognise the critical need to address the emerging threats posed by quantum computing. The implementation of PQC standards is being encouraged to safeguard sensitive information and maintain cyber security resilience in the face of advances in quantum technology. Table 1.3 lists public sector PQC-related initiatives for major countries.

Table 1.3. Post-quantum cryptography initiatives by country

Country	PQC initiatives

US	• In Sep 2022, the National Security Agency (NSA) released the "Commercial National Security Algorithm Suite 2.0" (CNSA 2.0) Cyber security Advisory (CSA) [22] that requires all National Security Systems (NSS) to be quantum-resistant by 2035.
	  o **Software and firmware signing**: begin transitioning immediately, support and prefer CNSA 2.0 by 2025, and exclusively use CNSA 2.0 by 2030
	  o **Web browsers/servers and cloud services**: support and prefer CNSA 2.0 by 2025 and exclusively use CNSA 2.0 by 2033
	  o **Traditional networking equipment** (e.g. VPNs, routers): support and prefer CNSA 2.0 by 2026 and exclusively use CNSA 2.0 by 2030
	  o **Operating systems**: support and prefer CNSA 2.0 by 2027 and exclusively use CNSA 2.0 by 2033
	  o **Niche equipment** (e.g. constrained devices, large public-key infrastructure systems): support and prefer CNSA 2.0 by 2030 and exclusively use CNSA 2.0 by 2033
	  o **Custom applications and legacy equipment**: update or replace by 2033
	• Quantum Computing Cyber security Preparedness Act [23] passed in Dec 2022 requiring the Office of Management and Budget (OMB) to release guidance directing agencies to develop a prioritised migration plan within one year of adopting the first set of NIST standards for PQC.
	• In November 2024, NIST published IR 8547 describing NIST's expected approach to PQC migration and transition timelines. NIST supports the goal of widespread PQC adoption by 2035, which was established by National Security Memorandum 10 (NSM-10). There is an acknowledgement that this timeline may vary depending on specific use cases or applications, which may be more complex and may require earlier transitions.

Canada	• The Cyber Centre [24] recommends that organisations switch to standardised PQC for quantum safety.
European Union	• The European Commission's Recommendation of 2024 [25] urged member states to formulate a comprehensive strategy for adopting PQC, ensuring a coordinated and synchronised transition. An implementation roadmap should be available by 2026. • 18 EU member states [26] recommend protecting sensitive data against 'harvest-now-decrypt-later' by 2030, and developing detailed transition plans for public key infrastructure systems within the same timeframe.

Germany	• The Federal Office of Information Security (BSI for its German acronym) [27] notes that PQC is set to be used by default, and it is crucial to advance the migration to PQC.
	• BSI's recommendations on PQC:
	  o **Preparation**: survey the existing situation and develop a migration plan
	  o **Cryptographic agility**: make cryptographic mechanisms adaptable to new advancements and standards and able to replace outdated algorithms
	  o **Hybrid solutions**: PQC should be used in hybrid mode (in combination with classical algorithms), rather than in isolation

France	• French Cyber security Agency (ANSSI for its French acronym) [28] advises all industries to develop a gradual transition strategy towards quantum-resistant cryptography for applicable cryptographic products. • They also advice companies on using hybrid post-quantum mitigation for security products needing long-term protection or use beyond 2030
Netherlands	• Dutch Organization for Applied Scientific Research (TNO for its Dutch acronym) developed the PQChoiceAssistant, an open-source tool that helps organisations choose PQC algorithms for specific use cases [29].

	• The General Intelligence and Security Service (AIVD for its Dutch acronym), the Centrum Wiskunde & Informatica (CWI) and TNO released an updated version of the PQC Migration Handbook [30] for quantum-safe cryptography, in December 2024.
South Korea	• South Korea selected its final four algorithms as part of the Korean Post-Quantum Cryptography (KpqC) competition [31], for creating post-quantum standards for public-key encryption (SMAUG-T) and digital signatures (HAETAE).

Singapore	• The Monetary Authority of Singapore issued an advisory [32] to financial institutions on addressing the cyber security risks associated with quantum:
	  ○ Stay updated on quantum computing developments and related cyber security risks.
	  ○ Manage an inventory of cryptographic assets and prioritise critical ones for migration to quantum-resistant encryption.
	  ○ Develop strategies and capabilities to address quantum-related cyber security risks.

Australia	• The Australian Signals Directorate (ASD) under latest “Guidelines for Cryptography” [33]:
	  ○ Stated that new cryptographic equipment and software intended for use beyond 2030 should aim to support ASD-approved post-quantum cryptographic algorithms by 2030
	  ○ Approved the use of ML-DSA and ML-KEM as PQC algorithms
	  ○ Did not approve the use of RSA beyond 2030

Israel	• The Bank of Israel under Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities:
	  ○ Organisations are required to develop an initial preparedness plan which address:
	    ▪ raising awareness within the banking corporation, continuously monitoring developments and assessing the associated cyber risks
	    ▪ Mapping and managing encrypted information assets
	    ▪ Readiness for skills and capabilities development to address cyber risks related to quantum computing
	  ○ Preparedness plan should be submitted by January 2026

Spain	• The national cryptology centre (CCN for its Spanish acronym) under “CCN-TEC 009 Recommendations for a safe post-quantum transition”:
	  ○ Greater interest in Key Encapsulation algorithms and recommend CRYSTALS-Kyber and FrodoKEM
	  ○ Recommend digital signatures selected by NIST: CRYSTALS-Dilithium, Falcon, SPHINCS+
	  ○ For symmetric algorithms, the recommended minimum length is 256 bits for AES, SHA2 and SHA3
	  ○ Recommend a phased approach to starting with the immediate use of hash-based signatures for firmware updates and ending with the adoption of PQC algorithms
	  ○ The timescales outlined state that the final phase of adopting quantum resistant algorithms will probably not start until 2030

2. Summary of key findings from primary research

The overall objective of this research study was to (1) improve DSIT's understanding of how UK-based organisations view PQC migration, and (2) understand the blockers and incentives to migration.

To gather input and insights, we designed a two-pronged programme of primary research, including a series of expert interviews and an online survey.

Specific focus areas for the primary research were:

- Who the key PQC migration stakeholders are, and their level of awareness and understanding
- How awareness, IT estate upgrade plans, incentives, and security needs may differ between sectors for PQC migration
- What drivers and market incentives exist for PQC migration
- What barriers to PQC migration exist, and which stakeholders might face hurdles when migrating their systems to PQC
- What kind of government interventions industry would like to see in order to facilitate the transition to PQC

This report contains the views of five critical national infrastructure sectors: energy, finance, healthcare, telecoms and transport.

2.1 Primary research methodology overview

The aim of the interview programme was to explore PQC awareness, migration readiness and plans, drivers and blockers, and potentially useful government interventions and support. The online survey provided further quantitative analysis enriching the interview findings.

One key objective was to understand how views and approaches to PQC migration vary across UK industries, by engaging senior stakeholders from each sector. A second key objective was to understand regulators' views on PQC migration in the sectors they regulate. In addition, we aimed to gain insights from the broader ecosystem, including academia and industry associations, on the critical factors for effectively preparing for PQC migration. Below is a summary view of the methodology; for full details, please see Appendix C: *Interview methodology details* and Appendix D: *Online survey methodology details*

The interview programme

- We conducted 21 semi-structured interviews in Q1 2025.
- These were mainly with senior IT and cyber security managers, including executive leaders. Interviewees were drawn mainly from the five target CNI sectors for this study. Within each sector, we also interviewed one regulator, to get insights into their concerns and point of view on PQC migration. A small number of academics and industry organisation cyber security leads were also interviewed, again to gather their insights on the overall ecosystem's awareness of and readiness for PQC migration. All respondents were UK-based and had some level of familiarity with PQC, ranging from general familiarity to deep expertise.
- Examples of interviewees' job titles included Chief Information Security Officer (CISO), Deputy CISO, Chief Technology Officer (CTO), and Director of Security, Director of Cyber security, Head of Security, Head of Department, Principal Security Architect, Solution Engineer, Cyber Security Advisor, Country-level Vice-President (VP). Within the academic sector, titles of interviewees included Professor, Associate Professor or Reader of Informatics, and Professor of Cyber Security.
- The interview guide included 20 questions designed to prompt discussion and gather insights on PQC awareness, readiness, key drivers, challenges, and potential government interventions. To ensure a comprehensive perspective, slightly different versions of the guide were used for industry

practitioners and ecosystem stakeholders (e.g. academics). Note that not all questions were answered by all interviewees.

- Some interviews focused on the approach to cyber security and PQC migration within the interviewee's specific organisation ('end-user' interviews); others focused primarily on the interviewee's views on the overall approach to PQC and the challenge of migration in their industry overall, or even across the broader CNI sector ('ecosystem interviews'). Breakdowns of interviewees are shown in Table 2.1 and Table 2.2.

Table 2.1. Breakdown of interviewees by role, organisation and interview type (no. of interviewees)

Role type		Organisation type		Interview type	
Technical	11	Industry	11	End user	9
Managerial	7	Regulator	5	Ecosystem	7
Both	3	Academia	5	Both	5
TOTAL	**21**	**TOTAL**	**21**	**TOTAL**	**21**

Table 2.2. Breakdown of interviewees by job title and sector (no. of interviewees)

Job title		Sector	
CISO	7	Energy	3
Head of Department	4	Finance	3
Advisor	4	Healthcare	3
Professor	4	Telecoms	4
Cybersecurity Expert	2	Transport	3
		Other	5
TOTAL	**21**	**TOTAL**	**21**

Note: Definition of each term is included in *Appendix C: Interview methodology details*

The online survey programme

- We conducted the online survey over a 10-day period in February 2025, targeting senior IT and cyber security leaders and practitioners in the five specified CNI sectors.
- The survey included seven screening questions and 12 multiple-choice questions on areas including PQC awareness, goals, barriers and drivers, as well as an open question for respondents to elaborate on the support they would like from government and regulators to help them prepare for PQC migration.
- Survey responses were filtered using automatic screening criteria and a manual quality control process. Figure 2.1 provides a visual summary of the responses used in the survey analysis, and the filtering process.
    - We collected 133 partial and complete responses from pre-qualified candidates. 53 of those survey respondents did not fully meet the screening criteria embedded in the survey. Therefore, instead of being asked to complete the full survey, they were asked only two questions: one about their familiarity with PQC, and one about their estimate of how many years it would take for a quantum computer to pose a cyber security threat to their organisation. Analysis of these 'extra' responses is shown in Section 4.
    - The other 80 respondents passed the screening criteria and completed the full survey. We then conducted a quality assurance review on their responses. 52 of the completed survey responses passed our quality review; the answers of the other 28 respondents (that did not pass our quality criteria) were discarded. The analysis in this report is primarily

based on the 52 completed and qualified responses. More information on the screening and quality criteria can be found in *Appendix D: Online survey methodology details*.

Figure 2.1. Breakdown of all survey respondents by screening group

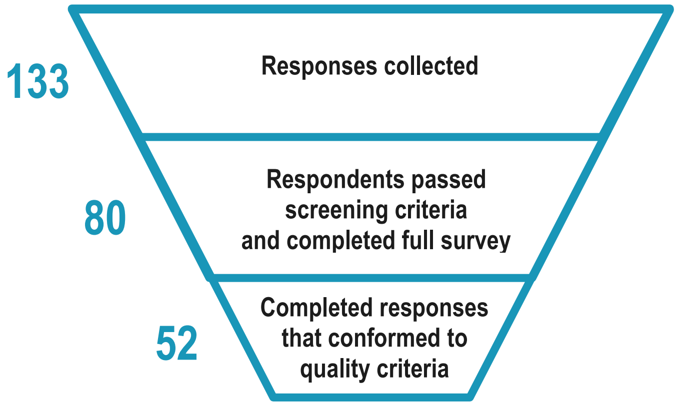


Table 2.3 and Table 2.4 show the distribution of respondents by sector, organisation size, job title, influence on cyber security, and familiarity with PQC.

Table 2.3. Number of survey respondents by sector and organisation size

Sector		Organisation size	
Energy	6	250 – 500 employees	30
Finance	12	500 – 1000 employees	15
Healthcare	11	1000 – 5000 employees	4
Telecoms	16	5000+ employees	3
Transport	7		
TOTAL	**52**	**TOTAL**	**52**

Table 2.4. Number of survey respondents by job title, influence on cybersecurity and familiarity with PQC

Job title		Influence on cybersecurity		Familiarity with PQC	
CISO/CTO	3	Organisation budget holder	15	Slightly familiar	0
Head of Cybersecurity	25	Division budget holder	11	Moderately familiar	16
Head of Data	3	Strategic planner	14	Very familiar	32
Head of IT	18	Influencer	3	Extremely familiar	4
Head of Strategy	2	Implementer	9		
Other	1				
TOTAL	**52**	**TOTAL**	**52**	**TOTAL**	**52**

Note: Definition of each term is included in Appendix D: Online survey methodology details

2.2 Key findings from the research

This section presents a summary of key findings from both interview and surveys across the main areas of research:

- Context for PQC Readiness: Organisations' Cyber security goals and Maturity (Section 2.2.1)
- Awareness, Understanding and Preparedness for PQC migration (Section 2.2.2)
- Incentives and Drivers for PQC migration (Section 2.2.3)
- Challenges and Blockers for PQC migration (Section 2.2.4)
- Government measures to support PQC migration (Section 2.2.5)

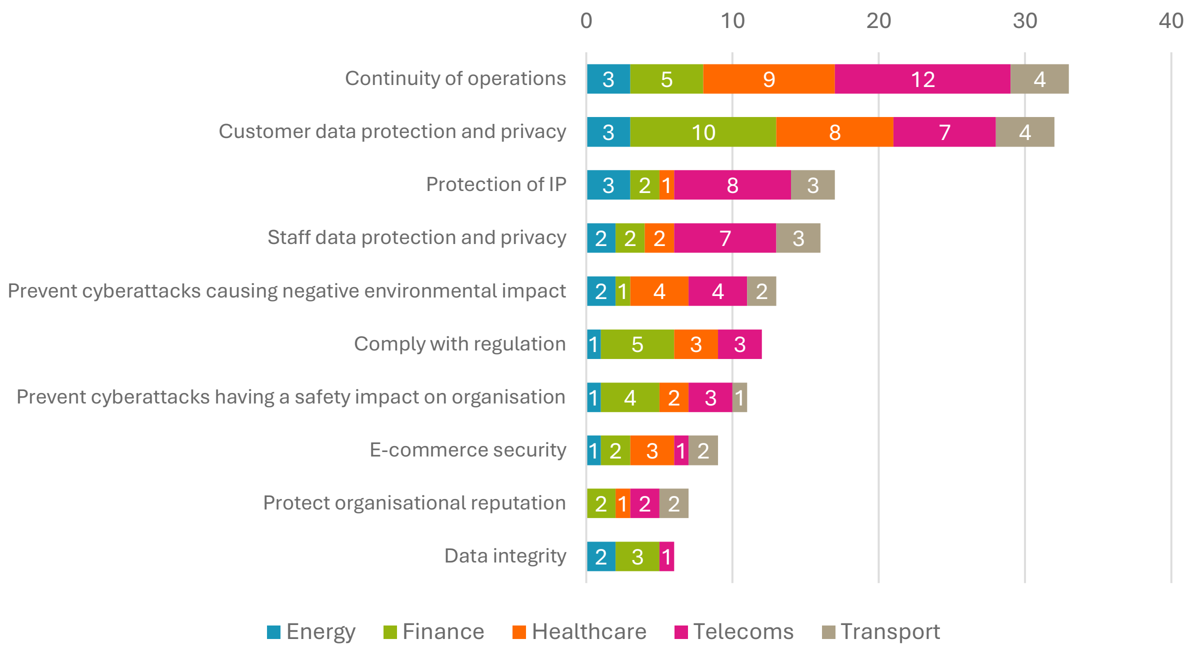
Full details of interview and survey responses can be found in Sections 3 and 4 respectively.

2.2.1 Context for PQC readiness: Organisations' cyber security goals and maturity

2.2.1.1 Organisations' cyber security goals

We asked both interviewees and survey respondents about their organisations' main cyber security goals, to provide context for understanding their approaches to PQC. Figure 2.2 below shows the online survey data only; however, interview responses were very much aligned with the survey results.

Figure 2.2. Main cyber security goals for organisations, top 3 goals (count of respondents per sector)



Note: n = 52 survey respondents (6 energy, 12 finance, 11 healthcare, 16 telecoms and 7 transport). Respondents were asked to select their top 3 cyber security goals. Chart shows number of respondents who selected each option as one of their top 3 priorities, split by sector.

Overall view

Looking across both the interview programme and the online survey, results were consistent: continuity of operations and ensuring customer data protection clearly emerged as the most important cyber security goals. There was high consistency across industry sectors in prioritising these two top goals; they appeared in the top 3 ranking of survey respondents in every one of our five focus CNI sectors.

The industry practitioners we interviewed provided further explanations as to why they chose those two options. Continuity of operations is essential to every business since it allows them to keep offering their products and services, and therefore generating revenue. Ensuring customer data protection is closely tied to customer trust, which is vital for sustaining and growing a business.

Regulator view (interviews only)

Regulators' main cyber security objectives were safety of people and privacy. Their secondary objectives included:

- Ensuring that firms are following the NCSC guidance
- Keeping up with emerging threats
- Managing stakeholder groups

Academic view (interviews only)

Academics suggested replacing outdated cybersecurity systems nearing the end of their lifespan with quantum-safe alternatives to prevent costly future upgrades.

Sector view

This analysis includes both survey and interview results.

Energy sector

Some interviewees from the energy sector expressed their cyber security goals in terms of the CIA triad (Confidentiality, Integrity and Availability). In addition to the two main goals - continuity of operations and ensuring customer data protection – survey interviewees in this sector also highlighted intellectual property (IP) protection.

Finance sector

Both interviewees and survey respondents aligned on the two main goals mentioned by every other sector. Additionally, 42% of respondents reported regulatory compliance also sharing the second position in the priorities ranking.

Healthcare sector

Interviewees in the healthcare sector were concerned not only about ensuring customer data protection, but also about safeguarding R&D findings through IP protection – although only 9% of survey respondents agreed. Unlike other sectors, survey results showed a considerable count difference between the two main goals and the rest, suggesting that the healthcare sector is very strongly aligned on their primary goals. The third cyber security priority mentioned by interviewees in this sector was regulatory compliance, which ranked in fourth position (27%) in the survey responses. Regulatory compliance is needed to ensure healthcare organisations have licence to operate while protecting them from cyber attacks and emerging threats.

Telecoms sector

Each telecoms sector interviewee offered a different view of key cyber security goals. The top 3 organisation goals for survey respondents again included the two main goals of continuity of operations (75%) and customer data protection (44%). However, protection of IP ranked in second position (50%) and staff protection and privacy was also selected by 44% of respondents.

Transport sector

The prevention of security failures that lead to loss of software integrity, or loss of availability of critical systems such as safety monitoring systems or control systems – i.e. ensuring continuity of operations– was the sector's priority among interviewees and for 57% of survey respondents. This implies that quantum-enabled attacks that allow adversaries to forge digital signatures and tamper with software/data integrity with impunity are perceived as a significant risk. Apart from the two main goals, 44% survey respondents also reported protection of IP and staff data protection as the third highest-ranking goals, suggesting that the transport sector is very protective of data.

2.2.1.2 Cryptographic maturity

An organisation's cryptographic maturity is a key indicator of readiness for PQC migration, and the associated level of support that may be required.

We asked questions designed to assess cryptographic maturity in both the interviews and the survey. The survey data provided a more comprehensive view, with seven targeted questions designed to gauge cryptographic maturity levels. These covered understanding of sensitive data storage approaches and requirements for surveyed organisations; knowledge of the organisation's cryptographic strategy; staff technical capabilities; and views on senior management's level of understanding of cryptography. These insights are important when considering what kind of additional support organisations may need to prepare for PQC migration.

Overall view

Based on aggregated and weighted survey responses to the maturity questions, we developed a high-level maturity score out of 10 for each sector. Scores are indicative only, and should not be taken as a formal assessment, particularly given the relatively small survey samples size for each sector. Findings are illustrated in the heat map below (Table 2.5). Scores by sector were:

- Energy: 7.9/10
- Finance: 7.1/10
- Healthcare: 6.6/10
- Telecoms: 6.3/10
- Transport: 5.9/10

See *Appendix D: Online survey methodology details* for an explanation of how scores were calculated.

Our main takeaways are:

- Among the five CNI sectors, survey responses indicated that energy is the most cryptographically mature while transport is the least, with finance, healthcare, and telecoms ranking in between.
- Based on survey responses, financial organisations are actively inventorying cryptographic assets, with larger firms more aware of their cryptographic approach and estate.
- Healthcare practitioners we surveyed and interviewed recognised the importance of PQC, but indicated their organisations lack a strong cryptographically skilled workforce.
- Telecoms interviewees and survey respondents indicated that their organisations rely heavily on public key infrastructure, and also indicated investment in rapidly improving their cryptographic maturity.
- Transport has the lowest cryptographic awareness and maturity, with many survey respondents unsure of their organisations' cryptographic practices.

Regulator view (interviews only)

Regulators we interviewed noted that many different technologies are used in the five CNI sectors covered in this study, with a variety of cryptographic approaches and algorithms used as a result. They also shared some specific concerns:

- The energy sector uses bespoke cryptography algorithms that were developed prior to the establishment of standards.

- Players in the transport sector are likely to face challenges in upgrading legacy equipment to support new quantum-safe cryptography.
- There is concern about the misuse of encryption for illegal activities in the telecoms sector.
- Use of shorter keys by smaller financial organisations is a concern for the finance regulator.

Academic view (interviews only)

Academia highlighted that they have access to highly skilled experts with a deep understanding of cryptographic libraries and the algorithms that need the most pressing attention.

Sector view

The analysis in this section is based on both survey results (presented in the heat map diagram in Table 2.5) and interview results. As noted above, the sample size for each sector was relatively small, so the heat map analysis should be taken as indicative only.

To understand the level of cryptographic maturity of each of our five CNI sectors, we asked survey respondents to indicate their level of awareness of key information regarding their own organisation's approach to cryptography. We believe it is likely that sectors with higher cryptographic maturity will be 'leaders' in preparing for PQC migration, while those with lower maturity are more likely to be 'followers', and may require additional or different types of government support.

Table 2.5. Comparison of different cryptographic maturity statements, showing sector-level breakdown (based on survey data for the 5 CNI sectors)

	Yes					To some extent				
	E	F	H	Te	Tr	E	F	H	Te	Tr
1. We know where our sensitive data is stored	50%	42%	64%	56%	86%	50%	58%	36%	31%	14%
2. We know how long our data needs to be stored and secured for	83%	75%	82%	31%	29%	17%	17%	9%	38%	57%
3. We have a mostly complete inventory of where our organisation uses cryptography	33%	25%	27%	25%	43%	67%	67%	73%	75%	57%
4. We have a team of internal staff with cryptographic skills	50%	50%	45%	50%	57%	50%	42%	36%	44%	29%
5. We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of "banned" algorithms that cannot be introduced	67%	67%	73%	25%	43%	33%	25%	27%	69%	43%
6. Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations	67%	58%	27%	31%	43%	33%	42%	55%	63%	43%
7. Our senior management understands how cryptography contributes to our organisational goals and business strategy	50%	50%	55%	50%	71%	50%	42%	36%	50%	29%

KEY 0% 50% 100%

(continues on following page)

	No					Unsure				
	E	F	H	Te	Tr	E	F	H	Te	Tr
1. We know where our sensitive data is stored	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%
2. We know how long our data needs to be stored and secured for	0%	0%	0%	0%	0%	0%	8%	9%	31%	14%
3. We have a mostly complete inventory of where our organisation uses cryptography	0%	0%	0%	0%	0%	0%	8%	0%	0%	0%
4. We have a team of internal staff with cryptographic skills	0%	0%	9%	0%	0%	0%	8%	9%	6%	14%
5. We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of "banned" algorithms that cannot be introduced	0%	0%	0%	0%	0%	0%	8%	0%	6%	14%
6. Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations	0%	0%	0%	0%	0%	0%	0%	18%	6%	14%
7. Our senior management understands how cryptography contributes to our organisational goals and business strategy	0%	8%	0%	0%	0%	0%	0%	9%	0%	0%

Note: Sectors are (E) Energy, (F) Finance, (H) Healthcare, (Te) Telecoms, (Tr) Transport. N = 52 survey respondents. Respondents were asked to choose the option (Yes, no, to some extent, unsure) that best represented the reality of their organisation. % and colour indicate the share of respondents in each sector who selected the option indicated, as their response to the specific maturity statement.

Energy sector

Based on both interviews and survey responses, cryptographic maturity varies across the energy sector. Interviewees stated that available investment to maintain cryptography maturity is limited, although one noted that as a regulated sector, energy companies do have an advantage in being able to access government funding for this.

Based on the survey responses, the energy sector is the most cryptographically mature sector. A high percentage of respondents indicated that their organisations:

- Know how long they need to store and secure their data for (83%).
- Maintain a list of acceptable cryptographic algorithms/key lengths (67%).
- Actively assess their cryptographic libraries as part of their vulnerability management (67%).

Finance sector

The financial organisations we interviewed were aware of the types of cryptography they use, and are actively developing inventories. Generally, larger firms such as banks are more aware of their cryptographic strategies than smaller organisations. Based on our survey responses, this sector is the second most cryptographically mature. The survey indicated that most financial sector organisations:

- Know how long they need to store data securely (75%).
- Have an internal team with cryptographic skills (50% 'fully' and 42% 'to some extent').
- Keep a list of acceptable algorithms and key lengths (50% 'fully' and 42% 'to some extent').
- Include an assessment of their cryptographic libraries as part of their vulnerability management approach (67%).

Healthcare sector

Industry healthcare practitioners we interviewed and surveyed were aware of the importance of creating a cryptography inventory and have initiated the process, though progress varies by organisation. According to the regulator we interviewed, healthcare organisations have some knowledge of cryptography and its quantum threats, but lack a strong workforce of experts, with cyber roles often blending IT management, governance, and cyber security tasks. The healthcare sector is the third most mature of the five CNI sectors, based on our high-level assessment of survey responses. Organisations we surveyed in this sector reported that they:

- Know how long they need to store and secure the data for (82% 'yes' and 9% 'to some extent').
- Maintain a list of acceptable cryptographic algorithms/key lengths to use (73% 'yes', 27% 'to some extent').
- Were somewhat less likely than other sectors to have a team with cryptographic skills, with 9% recognising they don't have such a team, and 9% being unsure.
- Ranked low with respect to having a mostly complete cryptographic inventory in their organisation (only 27% of respondents said 'yes' to this, with others stating they were working on it).

> "
> *For our cryptography inventory we will:*
>
> 1. *Create a list of critical suppliers*
> 2. *Work with those suppliers to discover what cryptography is used and which types of cryptography need to be migrated.*
>
> *As part of the migration, we will isolate legacy equipment since such equipment is unable to process 'quantum-safe' algorithms. However, encryption is not the only cyber security measure you can put in place so we will also implement full individual network port isolation to add another layer of security.*
>
> \- ***Healthcare organisation***

Telecoms sector

All interviewees acknowledged that telecoms systems heavily rely on public keys (PKI), and all said their organisations had started developing cryptographic inventories. One interviewee (a certificate authority) is actively migrating PKI; this is important as it relies on SSL cryptography, which is easily breakable by quantum computers.

As the heatmap based on our survey responses illustrates (Table 2.5), the telecoms sector is the second least cryptographically mature of the five CNI sectors, although interviewees indicated the sector is well ahead in some areas. Compared to other sectors, telecoms sector survey respondents were relatively more likely to be uncertain about:

- Their knowledge on longevity of data storage and security (31% were uncertain about this)
- Where their sensitive data is stored (13% were uncertain about this)

Transport sector

A wide variety of technologies are used in the transport sector. Alongside the prevalence of legacy infrastructure, this makes cybersecurity and supporting cryptography strategy challenging to manage. According to one interviewee, regulation (especially from the US) is driving multinational companies in the sector to build a Cryptographic Bill of Materials (CBoM) of their IT assets. Awareness of cryptography strategies is a challenge, with one interviewee acknowledging their uncertainty about where (and whether) cryptography is being used in their products.

Based on our survey data, the transport sector had the lowest level of cryptographic maturity, largely due to uncertainty among respondents regarding key areas, e.g.:

- Only 29% of respondents in this sector said that had a clear view of data storage.
- More respondents in this sector (14%) were uncertain whether their organisation had a team with specific cryptographic skills.
- The same was true of maintaining a list of acceptable cryptographic algorithms/key lengths to use, and of “banned” algorithms that cannot be introduced (14% were uncertain about this); having an approach to vulnerability management which includes assessing their cryptographic libraries to ensure that they are using secure implementations (14% were uncertain); and understanding timespan requirements for ensuring the security of critical assets (14% were uncertain).

2.2.1.3 Understanding how long digital assets need to remain secure

Within the interview programme, we asked interviewees about how long their organisations’ digital assets need to remain secure. Table 2.6 summarises these responses by sector, highlighting the shortest and longest timeframe requirements for ensuring security, along with the specific type of digital assets mentioned.

Overall view

Interviewees indicated a very wide range of different security duration requirements, from as few as 12-18 months (for healthcare R&D data) to as many as 70 or more years (e.g. for nuclear energy-related data and assets in the energy sector). In general, the infrastructure-heavy energy and transport sectors appear to have the longest duration requirements for keeping data and assets secure.

Regulator view

Although regulators did not share very specific views on the timelines for asset longevity and security, they expressed concerns about preserving confidentiality and data integrity.

Sector view

Data security requirements vary widely by sector, as shown in Table 2.6.

Table 2.6. Shortest and longest timeframes for which digital assets need to be stored and secured, by sector

Sector	Shortest timespan Type of asset	Longest timespan Type of asset
Energy	10 years Energy trading and markets	70+ years Nuclear operations
Finance	5 years Customer data	120 years Unspecified engagement
Healthcare	12-18 months R&D confidential data	Company’s lifetime IP data
Telecoms	Unspecified – GDPR* Customer data	30 years Digital assets
Transport	7 years Digital assets	110 years Digital assets

Note: All data above is based on the interview programme; this question was not asked in the online survey.

**GDPR – General Data Protection Regulation*

Energy sector

Energy sector interviewees indicated that regulatory compliance in the energy sector encompasses aspects including legal, safety, environmental, and market integrity. These different areas have different requirements for securing digital assets; e.g. up to 10 years for general energy trading and markets, up to 20 years for renewable energy, up to 30 years for oil and gas, up to 50 years for smart metering, and up to 70+ years for nuclear.

Finance sector

Interviewees indicated that financial institutions must keep customer data secure for five years after the end of the customer relationship. Regulation also mandates a 25-year retention policy in this sector. For some engagements, the lifetime of digital assets could reach 120 years.

Healthcare sector

Interviewees in the healthcare sector classified digital assets as belonging to data or to infrastructure. Timelines for storing and securing data depend on the type of data. Short-term security of 12-18 months is necessary for R&D (Research and Development) data confidentiality. Financial and legal data must be kept for 7-10 years, ensuring confidentiality and integrity. Finally, IP data needs to be protected for the company's lifetime. For infrastructure, some systems need to be secured for their lifetime (20-30 years).

Telecoms sector

Interviewees in this sector highlighted that timelines for customer data confidentiality are governed by GDPR. Infrastructure data must be kept secure for the lifetime of the systems; this is normally around 20 years, although it is common for the lifetime to extend beyond initial plans.

Transport sector

Interviewees indicated that the transport sector has a very long view on assets, with some interviewees stating their organisations could be responsible for cyber physical systems (e.g. vehicles) for up to 80 years. Digital assets in this sector may need to be secure from 7 years up to 30 years beyond the lifetime of the systems they are associated with. This means many organisations are thinking about the impact of quantum computers today.

2.2.1.4 Approaches to in-house vs outsourcing for cyber security

We asked survey respondents about their organisations' approach to cyber security for digital assets (fully in-house, partially outsourced, or fully outsourced) for two key activities:

1. Planning and strategy of cyber security
2. Deployment, management and updates of cyber security

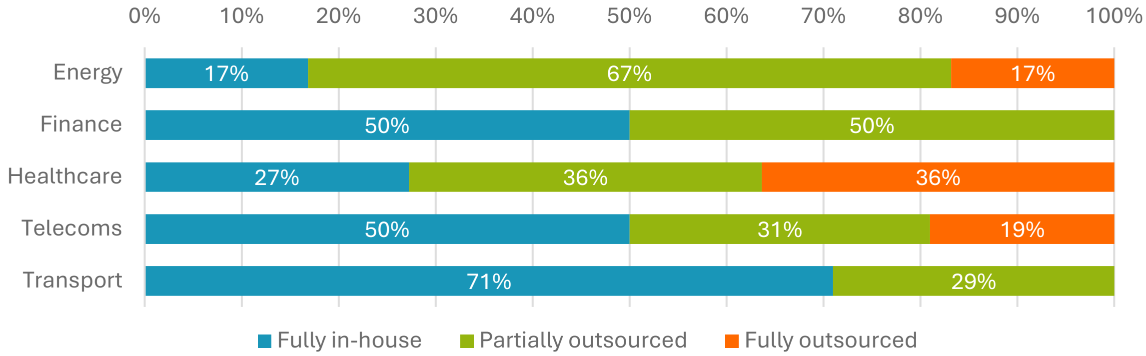
Overall view

For cyber security 'planning and strategy', the share of respondents who chose each approach varied significantly between sectors (see Figure 2.3), although overall most respondents preferred to keep cyber security strategy at least partly or completely in-house. For cyber security 'deployment, management and updates', the approach was more uniform across sectors (see Figure 2.4) with most respondents saying their organisations used partial or full outsourcing. This reliance on third-party vendors may limit organisations' visibility of their own cryptographic estates, and means that the supply chain must be a key part of thinking and discussions around PQC migration strategy.

Regulator and Academic view

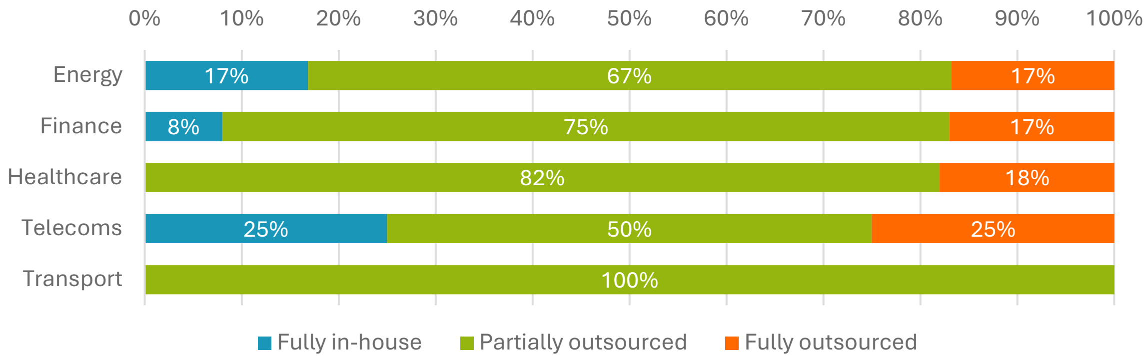
The insights for this area came from the survey responses only (regulators and academics were not included).

Figure 2.3 Organisations' approach to cyber security for digital assets – Planning and strategy, (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to choose how their organisation plans for their cyber security.

Figure 2.4. Organisations' approach to cyber security for digital assets – Deployment, management and updates, (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to choose how their organisation provides cyber security.

Sector view

Energy sector

The energy sector showed strong reliance on outsourcing, with 84% of survey respondents stating that their organisations either partially or fully outsource all aspects of cyber security, including planning and strategy, and deployment, management and updates.

- Partial outsourcing is the most common approach to both cyber security planning and strategy, and ongoing deployment and management.

Finance sector

The finance sector presented a more mixed approach, depending on the stage of cyber security management.

- Cyber security 'planning and strategy' is more balanced, with half of the respondents indicating a fully in-house approach, while the other half reported partial outsourcing.
- 83% of respondents fully or partially outsource cyber security 'deployment, management, and updates'.

Healthcare sector

Healthcare relies more heavily on third parties to support cyber security:

- 72% of healthcare survey respondents relied on or collaborated with third-party organisations for the cyber security strategy and planning of their digital assets.
- No respondents do in-house the deployment, management and update of their cyber security, but 82% partially outsource it.

Telecoms sector

For telecoms sector respondents, cyber security planning and strategy is conducted predominantly in-house, whilst deployment, management and updates shows more variation:

- 50% of respondents preferred to do cyber security strategy and planning in-house, and 19% fully outsourced it.
- 50% partially outsource deploying, managing and updating cyber security, while 25% keep this in-house, and 25% fully outsource.

Transport sector

Within the transport sector, organisations were more inclined to retain cyber security strategy and planning in-house, and to depend on partial outsourcing for ongoing deployment, management and updates.

- 71% of survey respondents keep planning for cyber security fully in-house.
- All survey respondents in this sector reported that they partially outsource their cyber security deployment, management and updating.

2.2.2 Awareness, understanding and preparedness for PQC migration

2.2.2.1 Awareness and prioritisation of quantum risks to cyber security

Awareness of quantum risks to cyber security

We asked interviewees about potential threats quantum computers could pose for CNI, and all demonstrated a strong awareness of the risk.

Overall view

Most respondents had a good grasp of the threat of quantum-enabled attacks on cyber security, although levels of technical expertise varied. They identified and emphasised the following key threats:

- The '**harvest-now-decrypt-later**' attack threat was highlighted by many interviewees. One telecoms sector respondent shared that they are actively conducting a data assessment across their infrastructure to pinpoint the locations of their most valuable data, as part of early efforts to mitigate this risk.
- **Asymmetric cryptography** was cited as a major concern by 76% of interviewees, who recognised the significant threat quantum computers pose to their organisations' security. Two respondents compared Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography and agreed that the former will be compromised before the latter. Diffie-Hellman, which relies on discrete logarithms, was also identified as vulnerable. PKI was seen as particularly at risk, with one interviewee strongly believing that digital certificates will be among the first targets for quantum-enabled attacks.
- Two interviewees also suggested that **symmetric cryptography** could be compromised in the future, specifically mentioning AES-256. Academics expressed differing views on the impact of Grover's algorithm on symmetric encryption—some argued that its speedup is unlikely to pose a significant threat, while others believed it may require the use of longer key lengths for enhanced security.

Regulator view

Regulators we interviewed understand the significant impact quantum computers will have on cybersecurity. Their observations included:

- 'Harvest-now-decrypt-later' attacks will be particularly harmful for IP theft but less so for safety-critical systems.
- The development of quantum computing hardware is crucial: as the quality of qubits improves, the threat to secure cryptography will increase.
- PQC can affect encryption methods and supply chains.
- Old equipment lacks essential cryptographic protections, making it vulnerable to quantum computers.

Academic view

Academics we interviewed understood the link between quantum computing development and cybersecurity. One academic strongly believed that industry end-users are not taking the threat seriously enough and that early action is needed, despite the seemingly long timeline before potential attacks.

Sector view

Energy sector

Industry practitioners were aware of the significant impact of PQC on cyber security, with concerns about long-lived assets like smart meters. The energy regulator highlighted vulnerabilities in old equipment lacking critical cryptographic protections.

Finance sector

Interviewees recognised the substantial threat quantum computing poses to current cryptographic methods, particularly through 'harvest-now-decrypt-later' attacks. There is also awareness of potential quantum-enabled attacks that have not yet been attempted.

Healthcare sector

Interviewees in the sector were aware of the need for PQC migration due to the long lifespan of sensitive data. Concerns included the impact on supply chains and the need for more specific regulatory guidance to navigate the transition.

Telecoms sector

Industry practitioners mentioned proactively raising awareness about the importance of migrating to PQC to protect critical assets.

Transport sector

All respondents (industry practitioners and regulators) mentioned 'harvest-now-decrypt-later' attacks, but attacks to data integrity remain the primary concern.

Quantum risk prioritisation

Interviewees were also asked about the prioritisation of the quantum threat – specifically, where it stands in comparison with other risks.

Overall view

All interviewees acknowledged the risk of quantum computers to cyber security. Key observations included:

- Quantum is not prioritised because of other immediate cyber security risks.
- There is a consensus on how mandates and compliance-driven initiatives will help in driving action, but the criticality of current cyber threats takes priority.
- Some interviewees – notably in the finance, healthcare and telecoms sectors – raised the possibility that the quantum threat is a low priority for organisations because it is not being properly assessed.
- There is a need for quantum-safe options for cyber security.
- Many had concerns around quantum vulnerability of old and legacy systems.

> “*We are exploring the encapsulation of legacy systems. We are collaborating with several start-ups on this. However, our concern is ensuring a certification programme from knowledgeable vendors to certify these start-ups.*
>
> *We are also upgrading our mainframe to support quantum algorithms. However, many applications will need to be migrated and may not initially support quantum. While the mainframe will be ready, encouraging adoption and implementing the necessary upgrades will be challenging.*
>
> *Industry practitioner in the healthcare sector*

Regulator view

Most regulators believed that quantum computers pose a moderate threat compared to other risks. While the impact will be significant, it hasn't materialised yet.

Academic view

Academics were concerned that industry does not fully grasp the threat of quantum computers, which could inevitably break asymmetric cryptography without warning.

Sector view

Energy sector

Industry players relied heavily on regulatory inputs and upstream industries for risk management. Measures suggested include: NCSC mandates, compliance-driven mandates like GDPR, and expressing risks in monetary terms.

One industry practitioner highlighted how the PQC migration could have a significant commercial potential for vendors capable of offering quantum-safe solutions.

Finance sector

Organisations we spoke with found quantum risks to be different from existing risks. Most cyber security risks can be associated to a particular business function, system or technology, but the risk of quantum-enabled attacks is more widespread, making it harder to manage. Respondents indicated they were monitoring quantum threats with the intention of acting on them once they become more pressing. One interviewee also mentioned that there might be quantum-enabled attacks that have not yet been attempted and knowledge is lacking on the impact those could have.

Healthcare sector

Healthcare sector respondents indicated that AI threats are the highest priority right now, although 'harvest-now-decrypt-later' attacks are also a concern. Industry practitioners thought that having the right measures against intruders is essential. They also echoed the need for guidance on quantum threats, since they believe it could help organisations get foundational protection basics right.

Telecoms sector

An interviewee from a telecoms vendor organisation responsible for PQC believed that the sector is focused on more pressing risks, and that the quantum threat is not being properly assessed. The regulator said they were starting to think about quantum threats and has commissioned a horizon scanning study looking at the next 3-5 years.

Transport sector

Responses from this sector varied. Some believed that other sectors are more attractive to adversaries with quantum capabilities, while others felt that immediate action is justified due to 'harvest-now-decrypt-later' attacks. Most agreed the quantum risk will worsen in the near future, but other risks of similar importance currently exist.

2.2.2.2 Understanding of quantum threat timelines

We asked both survey respondents and interviewees questions on their understanding of the quantum threat timeline.

Overall view

Responses varied significantly, highlighting the level of uncertainty about threat timelines within CNI sectors (see Figure 2.5). However, the overall finding was that ~50% of respondents believed the quantum threat to cybersecurity will become a reality in the next 10 years. For survey respondents, the most common prediction was a threat timeline of '5 to 10 years', followed closely by '10 to 20 years'. Among interview respondents, the most common response was 'less than 5 years', followed by '5 to10 years'. We believe this difference between survey and interview responses is due to interviewees being mostly advocates of PQC within their sectors and more acutely aware of the threat in their daily lives.

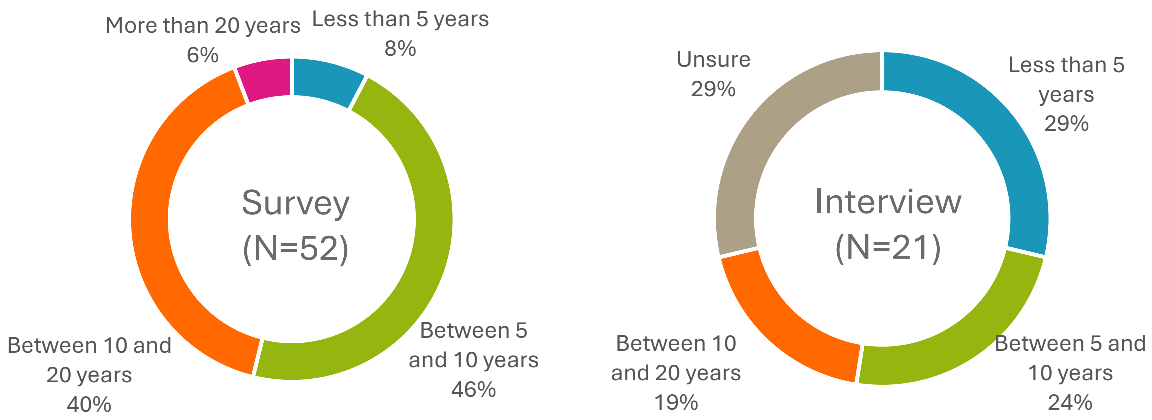
Regulator view

Regulators' views on the timeline for the quantum threat varied, with one regulator (financial) estimating a timeline of 'less than 5 years', one estimating '5 to 10 years', and two estimating '10 to 15 years' (one was unsure). In the survey, the financial sector responses also generally indicated that respondents perceived the timeline for the quantum threat to be shorter, compared to other sectors; the financial regulator's concerns and timeline estimate therefore seem to be well-aligned with its sector.

Academic view

Most academics predicted that quantum computers would become a real threat in '10 to15 years', although one respondent considered 'less than 5 years' as the likeliest timeline.

Figure 2.5. Expected time until a quantum computer enables a cyber attack against organisations (share of survey respondents and interviewees)



Sector view

Expectations about the timeline for quantum computers becoming a threat varied significantly across sectors:

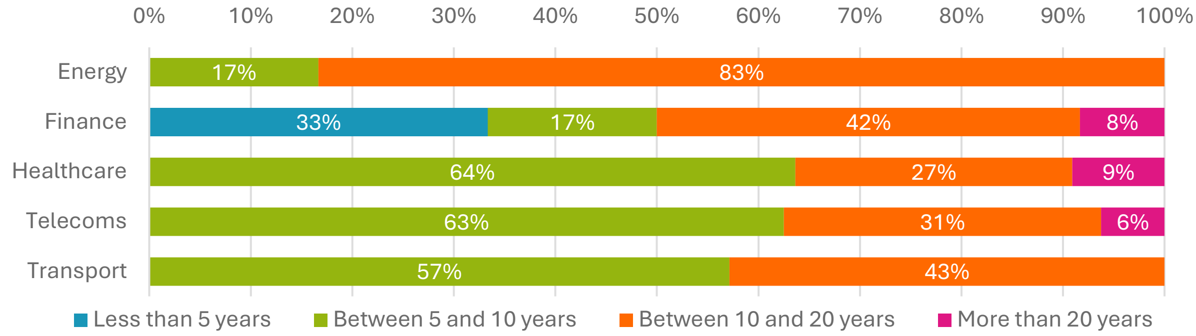
- Estimates ranged from 'less than 5 years' to 'over 20 years'.
- The finance sector saw the threat as more imminent, while some respondents in the healthcare and telecoms sectors expected a longer timeframe.

We believe the finance sector has the earliest expectation for quantum computing, possibly due to the emergence of publicly traded quantum computing companies, which may give the impression that the technology is more advanced than it is. Additionally, the general pace of technological change may also drive the impression across the board that the estimates in newspapers and reports may be conservative.

Energy sector

There were varied opinions among interviewees in the energy sector on when quantum computers will become a real threat. Answers ranged from 3 to 20 years. On the contrary, survey respondents shared a very similar opinion, with 17% thinking the threat timeline will be 5-10 years and 89% selecting 10-20 years.

Figure 2.6. Expected time until a quantum computer enables a cyber-attack against organisations (share of respondents per sector)



Note: N = 52 survey respondents. Respondents were asked to estimate likely number of years until a quantum computer could enable a cyber attack against an organisation's systems.

Finance sector

Interviewees' predictions ranged from 5 to 12 years. However, 33% of survey respondents believed that the threat is closer and will happen in less than 5 years. The finance sector was significantly more likely to believe that the threat timeline was shorter, compared to other sectors covered in the study.

Healthcare sector

Interviewees in healthcare were unclear on the quantum threat timeline. They had heard different theories; some saying 5 years, others sooner, others longer. One interviewee believed that quantum computers are already a threat and cited IBM's breakthrough in error correction and the intention of making QC available to the public market in 2027. Amongst healthcare survey respondents, no one believed that the quantum threat would become real in less than 5 years; all respondents expected longer timeframes, with 5-10 years out being the most common response (64%).

Telecoms sector

Interviewees believed that quantum computers will be a potential threat from anywhere between 5 to 15 years, and a major threat within 20 years. One questioned the Gartner timeline that advances in quantum computing will make asymmetric cryptography unsafe by 2029 [34]. The view among survey respondents in the telecoms sector was very similar to those in the healthcare sector.

Transport sector

Estimated ranges in this sector among interviewees went from 0 to 15 years for the first wave of attacks. The likelihood of 'harvest-now-decrypt-later' attacks was cited as a more immediate threat. Survey respondents believed quantum attacks would happen a bit later, with a very close split of 57-43 between '5-10 years' and '10-20' years respectively.

Analysis including responses from screen-outs

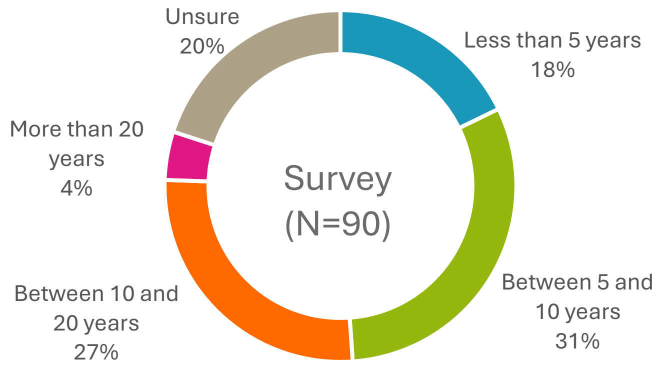
All pre-qualified survey respondents - including those who were screened out due to not meeting criteria such as industry, role or specific cybersecurity responsibility - were asked this question. The idea was to gain a broader view of responses regarding the timeline for the quantum threat, that could be answered even by those without deep technical knowledge or a specific security-related position inside their organisation.

Figure 2.7 shows data from all 90 respondents (note we also removed some respondents who did not meet our quality control criteria). The 'Other' sector was made up entirely of respondents from academic institutions or government.

The pattern of responses from this broader survey group mapped closely to that of our interviewees. Similarly to the interviewees, a significant subset of respondents were unsure about the quantum timeline.

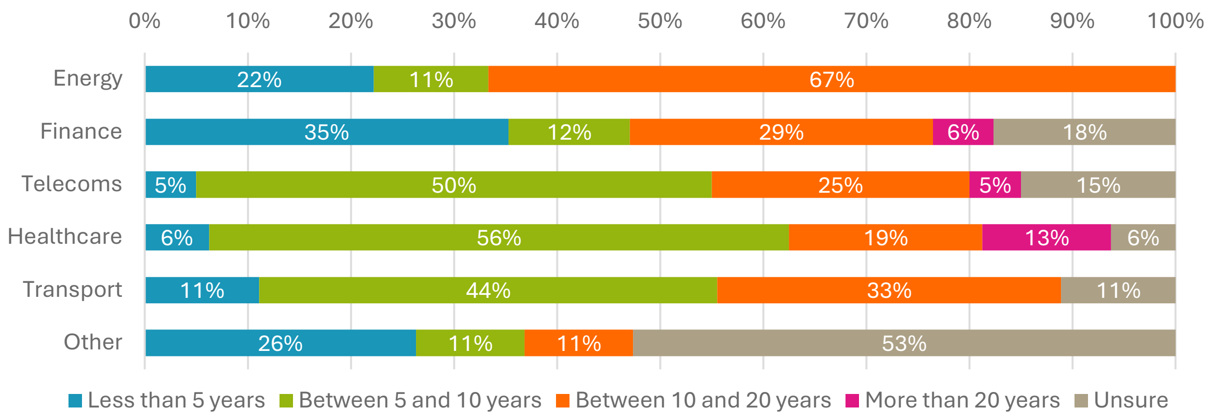
In addition, we saw a relatively higher percentage of survey respondents from this broader group who believed that quantum computers will be a threat in less than 5 years (18%), than we saw in the fully qualified 52-survey respondent group (8%).

Figure 2.7. Expected time until a quantum computer enables a cyber-attack against organisations (share of all survey respondents)



Note: N = 90 survey respondents. Includes responses from both screened-in and screened-out survey groups that met the quality control criteria.

Figure 2.8. Expected time until a quantum computer enables a cyber-attack against organisations (share of all survey respondents per sector)



Note: N = 90 survey respondents. Includes responses from both screened-in and screened-out survey groups.

2.2.2.3 Evolution of the quantum risk over time

We asked interviewees to share their views on how the quantum threat would evolve over time. Specifically, we asked them to consider whether the quantum risk to cyber security would increase or decrease in 5, 10, or 30 years' time. This question was only asked in interviews and was not part of the online survey.

Overall view

Interviewees in most sectors expected quantum computing technology to become more advanced and to increase the likelihood of quantum-enabled attacks. This rise will push quantum-enabled attack risks higher until they require serious mitigation, but most respondents did not expect this to happen until attacks are seen in the wild - which in turn they did not believe would happen within the next five years.

Interviewees generally believed that nation-states are more likely to use a quantum computer first, and to use it against another nation-state. Among industry end-users, this translates into some extra time for them to prepare against the threat, although these interviewees recognised that time won't be enough to accomplish a full PQC migration. Both energy and telecoms sectors believed that after the nation-state-to-nation-state attack, the finance sector will be next, with rogue actors aiming for financial assets.

Regulator view

Regulators across various sectors expected the quantum risk to increase within the next five years. They predicted that the first quantum computers will be available to nation-states in 10 to 15 years, and to the public in 20 years. Continuous monitoring of technological advances was a key strategy cited by regulators to stay ahead of potential threats and ensure preparedness. This is in line with popular sources of quantum risk estimation, such as The Global Risk Institute's Annual "Quantum Threat Timeline Report", which in 2024 speculated that RSA-2048 would be more than 50% likely to be broken in approximately 15 years [35].

Academic view

Academics believed that actions taken now, such as migrating to PQC, would significantly influence future risk levels. The cost of building and operating scalable quantum computers was seen as a critical factor that will affect the feasibility of widespread attacks. Academics emphasised the importance of proactive measures to mitigate future risks.

Sector view

Energy sector

The energy sector's perspective on quantum computing risk evolution differed between regulators and industry practitioners. Regulators believed that the risk would be contingent on the arrival of quantum computers; if they emerge soon, the risk is immediate, but if they appear in 30 years, improved mitigations will enhance preparedness. Industry practitioners, however, did not provide detailed thoughts on the evolving risk. One practitioner anticipated a quantum attack within the next decade, probably targeting defence or finance, while another expected Tier 1 technology suppliers (such as Microsoft, Google, IBM, etc.) to manage the risk effectively.

Finance sector

In the finance sector, predictions about when quantum computing will become a real threat ranged from 7 to 12 years, with some advancements expected even sooner. The primary concern was the vulnerability of encryption methods, particularly AES-based encryption, which could become susceptible within five years. This sector was acutely aware of the potential impact on data security and is closely monitoring technological advancements.

Healthcare sector

Healthcare sector interviewees had mixed views on how the risk posed by quantum computing will evolve over the next five years. Some believed that each technological advancement would heighten the risk, while others thought the risk would not change significantly in the near term. This sector remains vigilant but divided on the immediacy of the threat.

Telecoms sector

The telecoms sector interviewees believed that while quantum computers are not expected to break shared algorithms within the next five years, useful applications may emerge within a decade. The transition to quantum-safe algorithms was identified as the biggest risk, with concerns that governments and defence intelligence might crack encryption before the public is aware, leaving systems vulnerable until quantum-safe algorithms are universally adopted. The regulator in this sector reported they were actively engaged in horizon scanning and monitoring the quantum outlook, in collaboration with the National Quantum Computing Centre (NQCC).

Transport sector

Apart from the statements captured in the overall view, this sector was particularly concerned about the implications of quantum advancements on national security and infrastructure.

2.2.2.4 Migration journey: Status, approach and timing

We asked both interviewees and survey respondents about their progress on the PQC migration journey – specifically planning, approach and expected timelines. Across all sectors, PQC migration is in its early stages, with respondents indicating varying levels of awareness and organisational preparedness. While some industries are actively planning and implementing early measures for PQC migration, others are delaying action due to technical challenges, cost concerns, and reliance on the IT vendor supply chain.

Overall view

The interview analysis suggested that both industry practitioners and regulators acknowledge the importance of monitoring and preparedness in reducing the risk posed by quantum computing. Two distinct approaches could be distilled from the interviewees' responses:

- **Active Preparation**: Organisations that are proactively producing a cryptographic inventory, engaging with experts and vendors, and implementing measures to safeguard against quantum threats
- **Passive Monitoring**: Organisations that are continuously observing the quantum threat landscape, but primarily relying on vendors to develop and provide 'quantum-safe' solutions that can be seamlessly integrated into existing networks

Some sectors, such as finance and energy, are taking proactive steps, while telecoms and healthcare face greater challenges due to infrastructure complexity and vendor dependencies. Further details are provided in Section 3.1.2.5.

In our view, there is a risk that migration timelines are being underestimated, highlighting the need for structured planning, clearer guidance, and stronger industry coordination. Underestimation of the effort required is likely; studies estimate that one in six IT projects suffer a schedule overrun of 70% **[36]**, and PQC migration will be on the more complex end of the IT project spectrum.

> “
> *I think the first steps of the PQC migration journey are:*
>
> 1. *Assign a responsible executive (the owner of the migration journey at a board level).*
> 2. *Build a small team that will own the problem (made up of enterprise architects and security specialists who understand the business, its technology and its people).*
> 3. *Detailed discovery: understand quantum risks, the affected systems and what the industry sector is doing.*
> 4. *Build a business case and plan for PQC migration for board approval*
>
> - ***Telecoms industry interviewee***

Regulator view

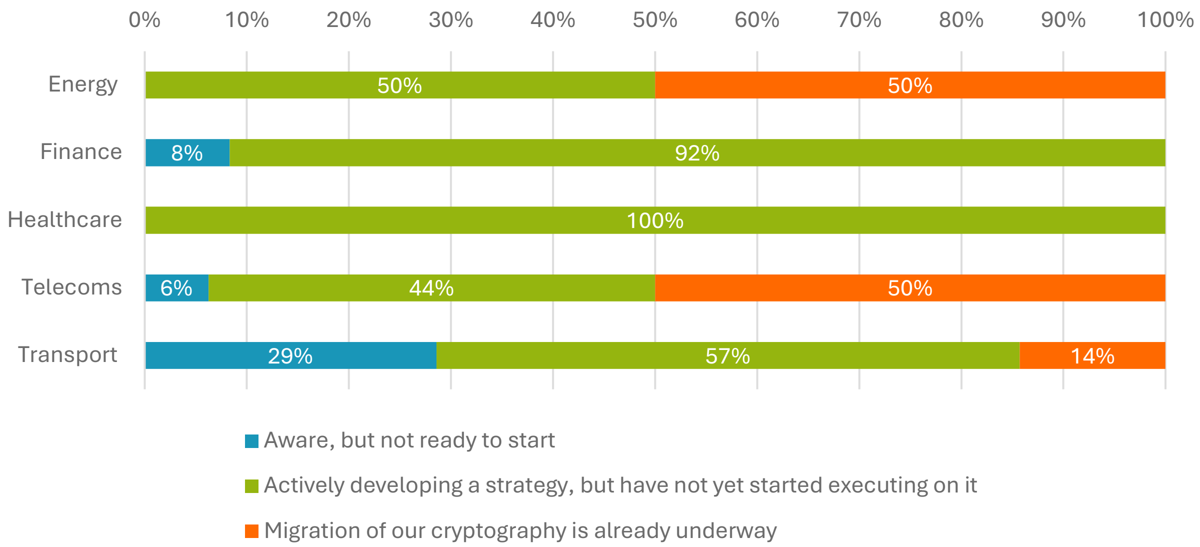
Regulators indicated that they were hesitant to mandate standards for PQC due to the rapid evolution of cryptography, and most were taking a cautious, observational approach. Within the finance sector, regulators acknowledged that larger firms have greater awareness of PQC risks, but concerns remained over the use of shorter (cryptographically weaker) key lengths. Some regulators also perceived lower sector readiness than our research suggests.

Academic view

There was a growing sense of concern among the academics we interviewed, notably that time is running out to complete the migration before systems become vulnerable to quantum-enabled threats. This concern is driving academic research into techniques and approaches to address PQC migration. One academic highlighted the likelihood that some sectors will still be unprepared in 10 to 20 years, similarly to the way that outdated, unsupported operating systems persist in critical systems today.

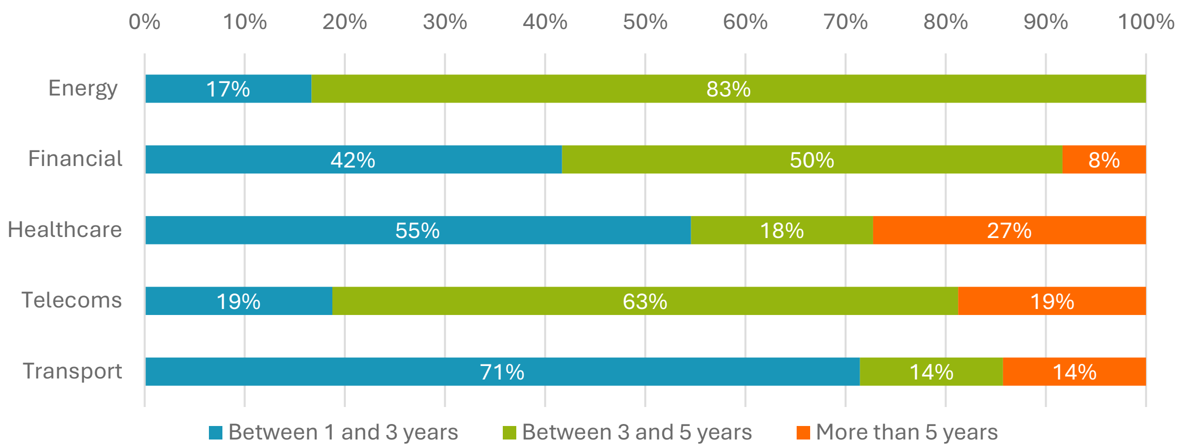
Sector view

Figure 2.9. PQC migration status (share of respondents per sector)



Note: N = 52 survey respondents.

Figure 2.10. Respondents' estimate of time required for PQC migration planning and execution (share of respondents per sector)



Note: N = 52 survey respondents.

Energy sector

Interviews revealed that all respondents had begun planning for PQC migration, with some progressing to proof-of-concept stages. Key challenges included scoping the cryptographic estate, determining what to migrate, and managing vendor dependencies. Meanwhile 50% of survey respondents said they were developing a strategy, and 50% had already begun the migration (see Figure 2.9). This high percentage emphasises the fact that energy seems to be one of the most 'PQC-mature' sectors. A sector regulator highlighted forthcoming requirements for providers to disclose their PQC plans in future business cases.

Most survey respondents anticipated that the PQC migration would require 3–5 years (83%) (see Figure 2.10).

Finance sector

The financial institutions we interviewed were in the early stages of PQC planning, with some formalising strategies and beginning implementation, while others were focusing on initial testing. Interviewees indicated that the sector moves collectively, meaning widespread adoption is likely to accelerate once leading firms take action. A multi-layered migration approach is needed, with strong demand for clear regulatory guidance and standardised frameworks. Survey responses confirmed this outlook, with most organisations (92%) actively developing a strategy but not executing it yet (see Figure 2.9).

There was a divide among survey respondents around PQC migration duration estimate. Half of them estimated the migration will take them between 3-5 years (50%) (see Figure 2.10), followed closely by those who think it will take between 1 -3 years (42%).

> *"*
> *The plan will roughly consist of knowing what we have, knowing who's using it and knowing what technology is consuming it.*
>
> - ***Finance sector organisation***

Healthcare sector

Interviewees from healthcare organisations have begun planning for PQC migration but remain in the early stages, relying heavily on vendors to lead the process. Large organisations will require extensive coordination with external partners, and cost estimates vary widely, from £100k to several million. The vendors to the healthcare sector we interviewed did not see security as a market differentiator.

Additionally, interviewees also reported that whilst regulatory awareness exists, preparation is minimal. This statement contradicted the survey results in which everyone (see Figure 2.9) reported to be actively developing a migration plan but not yet executing it.

Most survey respondents (55%) believed that the migration will take them between 1-3 years (see Figure 2.10), while 27% believed that it would take more than 5 years. Interviewees believed that the migration would last at least a few years.

> *"*
> *Doing a big bang migration is not an option for us. Instead, we will migrate progressively, because some legacy systems will be incompatible with the new 'quantum-safe' algorithms*
>
> - ***Healthcare industry interviewee***

Telecoms sector

Telecoms progress varies, with some organisations updating frameworks while others remain cautious due to concerns over key management, financial impact, and protocol compatibility. Service providers are technically prepared to issue post-quantum certificates (see *Appendix A: Terms and definitions* for definition). However, broader software ecosystem readiness remains a barrier. 50% survey respondents reported to have already started their migration journey, followed very closely (44%) by those who are developing a strategy, but have not yet started. This is a surprising result if we compare it with their cryptographic maturity score, where they fell into the least mature of the 5 CNI sectors (see Section 2.2.2.1).

Most survey respondents (63%) believed that the migration will take them between 3-5 years (see Figure 2.10). Meanwhile, interviewees believed that the migration could take between 2 and 5 years to complete, recognising it will be a gradual task.

> "
> *We have divided the journey into three work streams:*
>
> 1. *Supply chain: this is our primary focus; we have started by updating our ITT (Invitation to tender) frameworks to ensure all suppliers provide cryptographic support for quantum-safe computing.*
> 2. *'Harvest-now-decrypt-later' scenario: We are working to understand the data flows that need protection, both for our benefit and potentially for our customers'. We aim to transition to quantum-safe computing sooner rather than later. This includes moving away from asymmetric cryptography and using stronger symmetric cryptography in some areas, such as backups. Although pre-shared secrets have drawbacks, we are also considering basic link encryption e.g. between our data centres using pre-shared secrets.*
> 3. *Internal Infrastructure: We are evaluating internal PKIs, which are used by some customers, to determine how and when to transition from RSA-based systems to quantum-safe algorithms. This transition is complex, and we must plan for the future impact on performance and security.*
>
> \- ***Telecoms industry interviewee***

Transport sector

Interviewees believed that different organisations within this sector are at different migration levels, but that some have already built roadmaps for the PQC migration. This statement is echoed by the survey responses, with 29% of respondents who are aware but have not yet started; most (57%) are actively planning for the migration, but have not started executing it; and the rest (14%) stated that they have started their migration journey (see Figure 2.9).

Interviewees reported that the sector's reliance on a complex supply chain makes it challenging for technical professionals to effectively communicate the gravity of the threat to decision-makers. International transport faces additional difficulties, as standard setting cannot happen in isolation and requires coordination with global partners, complicating timelines and expectations.

Survey respondents projected the fastest migration pace among all sectors, with 71% expecting completion within 1–3 years (see Figure 2.10), 14% anticipating the threat to emerge within the next 3–5 years, and 14% believing it would take more than 5 years. Migration timelines for PQC varied among transport sector interviewees, ranging from 12 months to more than 3 years.

2.2.2.5 PQC resources

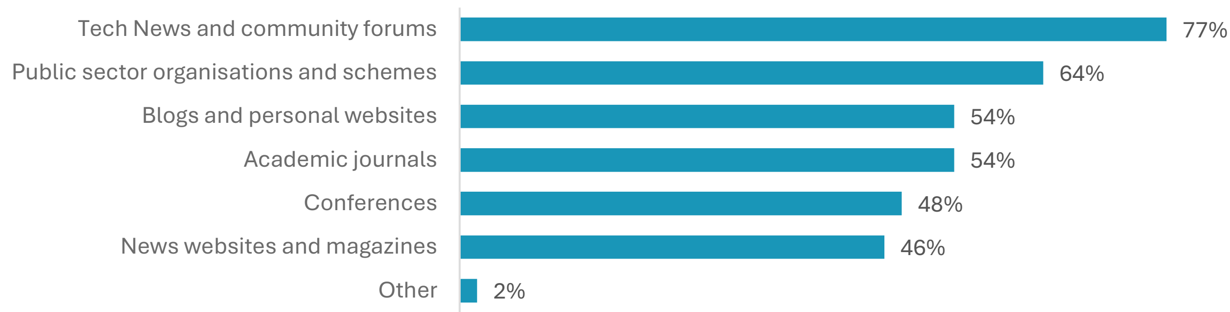
Understanding where organisations seek guidance on PQC is essential for shaping supportive resource development and outreach work. Both interviews and survey responses explored how CNI practitioners, regulators and academia access PQC information, highlighting the key sources of advice and the gaps that remain.

Overall view

The following were identified as the sources that industry practitioners and regulators use when seeking guidance and knowledge about PQC:

- Government and regulators such as NCSC, NIST or CISA - mentioned by interviewees in all the sectors. Some interviewees also mentioned following the CAF (framework provided by NIST) and the guidance provided by their sector's regulators. 64% of survey respondents also seek PQC advice from public sector organisations and schemes. Interviewees from the energy sector noted how fragmented this guidance is, with multiple organisations providing advice but no single authoritative framework to follow. Interviewees from the financial sector deemed these sources as often too dense for non-technical stakeholders. They suggested making insights more digestible for business leaders to bridge the gap between researchers and decision-makers.
- Standards organisations such as ANSI or ETSI
- Industry-specific forums - such as the Certification Authority Browser Forum - were mentioned by interviewees, while 48% of survey respondents mentioned attending conferences.
- Industry experts - generally supply chain vendors (hardware and software) or consultants - to stay informed of developments on PQC. Interviewees from the energy, healthcare and telecoms sector noted that service providers and supply chain vendors are emerging as sources of insight and implementation support. Specific companies mentioned included Google and IBM.
- Academia - although to a lesser extent. UKRI is facilitating these engagements through the Digital Futures Institutes and quantum networks. 54% of survey respondents also consult academic journals for PQC knowledge.
- Tech news and community forums were not mentioned by interviewees, but are the main source used by survey respondents (77%).

Figure 2.11. Sources consulted and followed by survey respondents for quantum cyber security information (share of respondents)



Note: N = 52 survey respondents. Respondents were asked to select all that applied.

Regulator view

Regulatory bodies are a primary source of guidance for organisations navigating PQC migration, and are actively engaged in promoting resources, forums and partnerships. Interviewees referenced NCSC, NIST and CISA as their main sources of advice. However, it was noted that there is a lack of a single, comprehensive regulatory framework, which makes it difficult for organisations to align on best practices. One interviewee acknowledged their reliance on government guidance (e.g. NCSC, NIST and CISA) for updates on PQC best practices. However, they are not providing a joined-up approach and instead are taking different approaches to the problem. Others pointed to the Cyber Assessment Framework (CAF) as a useful tool but suggested that a dedicated quantum-focused regulatory initiative is still missing. Regulators, especially from the transport and telecoms sector, highlighted several partnerships and engagements with industry and academia and acknowledged their participation in expert forums.

Academic view

Many interviewees noted that universities are at the forefront of research, with Manchester, Edinburgh, Bristol, Cambridge, Southampton, and Bath mentioned as leading institutions part of the UKRI's Digital Futures initiatives, which aim to connect academic research with real-world applications, though some noted that more structured collaboration is needed. While academic conferences are seen as valuable spaces for sharing new research, some interviewees expressed concern that much of this information does not translate into practical, industry-ready guidance. One interviewee highlighted the existence of dedicated academic conferences on the topic of PQC, but the detailed research shared in those venues has not yet made its way to industry.

2.2.3 Incentives and drivers for PQC migration

The CNI organisations we interviewed cited a variety of drivers and incentives that are influencing their approach to PQC migration.

Overall view

Among interviewees, the top drivers to act now on PQC migration included:

- Requirements to manage long-term assets, meaning there is an ongoing need to evaluate future risks and prepare for them (especially in the energy sector and transport sectors). PQC will need to be considered in long-term roadmaps, which are a common requirement in infrastructure-heavy sectors.
- Importance of creating a cost/benefit case for PQC migration, to ensure that sponsors (regulators and internal) can justify the spend, and to highlight the economic benefits to those who adopt the technology.
- Regulation and standards are critical drivers, with NIST's standardisation and push on quantum security being commonly mentioned. Some recognised the push that NIST is giving on quantum security. Other regulations driving behaviours include CNI organisations operating in the US subject to Cyber security Maturity Model Certification (CMMC).

In comparison, the main organisational driver overall in survey responses was the ability to use PQC-secure capabilities as a business differentiator – nearly 60% of respondents cited this as a top 3 driver.

The availability of sectoral guidance (50%), regulatory and legal requirements (47%), greater evidence of the quantum threat (46%), and an improved understanding of PQC in their organisation (44%) also appeared among the top drivers for taking action.

Relatively few respondents cited customer demand or availability of a clear business case for PQC as important drivers (see Section 4.1.1 for details).

From the energy sector, there was a clear view that PQC is a large-scale problem that will take significant effort to address. Key drivers include a push from employees and engagement with the NCSC and DSIT. Regulators are going to need to make more noise about this and prioritise it for people to grasp its importance. One respondent pointed out that regulation often struggles to keep up with fast-paced technology development. Another interviewee pointed out that any regulation should be developed in conjunction with industry, to ensure that recommendations and expectations were feasible.

Regulator view

Some industry practitioners in sectors like energy, transport, healthcare and finance have carried out some preparation for PQC. Most regulators recognised that guidance and regulation are necessary to push PQC forward. However, one regulator is waiting to see what the market demands or what other regulators in their sector will do.

Academic view

Academics echoed the drivers mentioned by respondents in the different sectors. There was variance between interviewees on which sectors should be early adopters and which would benefit from a fast-follower model. However, academics believed that industry is under-estimating the amount of time that the PQC migration will take.

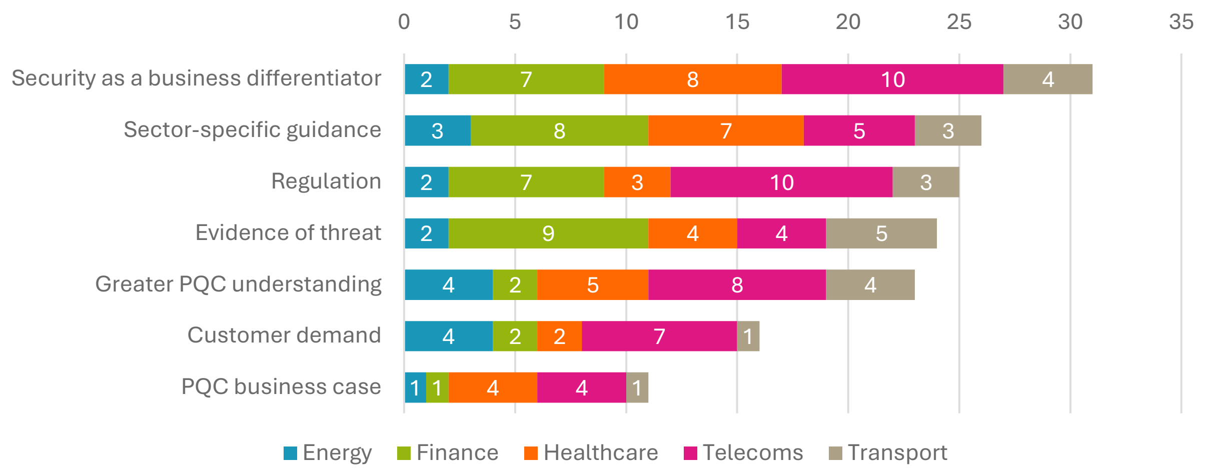
Sector view

Energy sector

Energy sector interviewees highlighted that long asset lifecycles are driving organisations towards a more strategic and long-term approach. NIST's drive and access to government innovation funding are key drivers for PQC planning.

For 4 out of 6 (67%) of energy survey respondents, improved organisational understanding and customer demand were primary motivators for migrating to PQC.

Figure 2.12. Main PQC migration drivers for organisations, top 3 (count of respondents per sector)



Note: n = 52 survey respondents (6 energy, 12 finance, 11 healthcare, 16 telecoms and 7 transport). Respondents were asked to select their top 3 drivers. Numbers indicate the count of respondents who chose the option as one of their top 3 drivers.

Finance sector

The significant threat posed by quantum computers and the complexity of migration were identified as the main drivers for interviewees in the finance sector.

Survey results supported this, with 9 out of 12 (75%) finance respondents citing quantum-enabled cyber threats as the primary driver. This was closely followed by sector-specific guidance for 8 out of 12 respondents (67%).

Healthcare sector

In healthcare the protection of patient data was cited as a key driver for PQC adoption among interviewees, with some viewing it as part of their long-term strategy. However, most reported other risks as more immediate and expected to follow rather than lead in PQC adoption.

Survey responses highlighted an alternative view, with 8 out of 11 (73%) healthcare respondents citing security as a business differentiator as the main driver.

Telecoms sector

In the telecoms sector, there was a strong focus on customer and competitive demand, with the business opportunity of selling quantum-safe equipment cited as a key driver. This, in turn, led to increased knowledge-building in the field to ensure a clear understanding of the associated threats.

Survey results supported this, with 10 out of 16 telecoms (63%) respondents reporting security as a business differentiator as a key driver, alongside regulation.

Transport sector

Interviewees in the transport sector had different drivers for migrating to PQC. One industry practitioner recognised that they will likely wait and see until a quantum computer becomes operational, although they also realised that it might be too late to react by then. This aligns with 5 of 7 (71%) transport survey respondents highlighting evidence of threat as the key driver. For another interviewee, the drivers for migration were aligned with their organisational goals: ensuring customer trust and IP protection.

2.2.4 Challenges and blockers for PQC migration

This section examines the key blockers identified through interviews and surveys. The survey focused on identifying barriers and key factors affecting PQC migration, offering a broad industry-wide perspective. By contrast, the interviews provided deeper insights, exploring both technical and non-technical challenges (further details on Section 3.1.4), including difficulties in conducting cryptographic inventories and broader discussions on migration obstacles.

Overall view

While some sectors have begun planning, a mix of skills shortages, infrastructure complexity, and supply chain immaturity continue to slow progress.

Many CNI organisations lack post-quantum cryptography expertise, leading to slow adoption, particularly due to difficulties in engaging supply chains. Uncertainty about PQC algorithm stability and longevity is leading to a reluctancy from organisations to act pre-emptively, as they weigh the risks of early adoption against the evolving cryptographic landscape.

The lack of clear financial impact assessments makes it difficult to justify PQC investment over other and more immediate cyber security concerns. Resistance at the senior level is exacerbated by challenges in communicating the quantum threat to non-technical decision-makers.

Legacy systems, complex IT/OT integration, and a lack of PQC-ready vendor solutions are significant barriers. Many organisations remain dependent on suppliers who are not yet prioritising PQC migration, further delaying progress.

Academic view

Academic interviewees acknowledged that a significant skills gap persists, with academia far ahead of industry in understanding PQC algorithms and hardware. Academic experts noted that both action and inaction carry risks, as the evolving nature of PQC algorithms makes early implementation uncertain, leading many organisations to delay migration until broader industry movement occurs.

Regulator view

Looking at the industries they serve, the skills gaps came up as a common concern, as did the supply chain. Many regulators now have small teams looking at PQC themselves, but this area is competing for attention and resources with other, more concrete threats.

Sector view

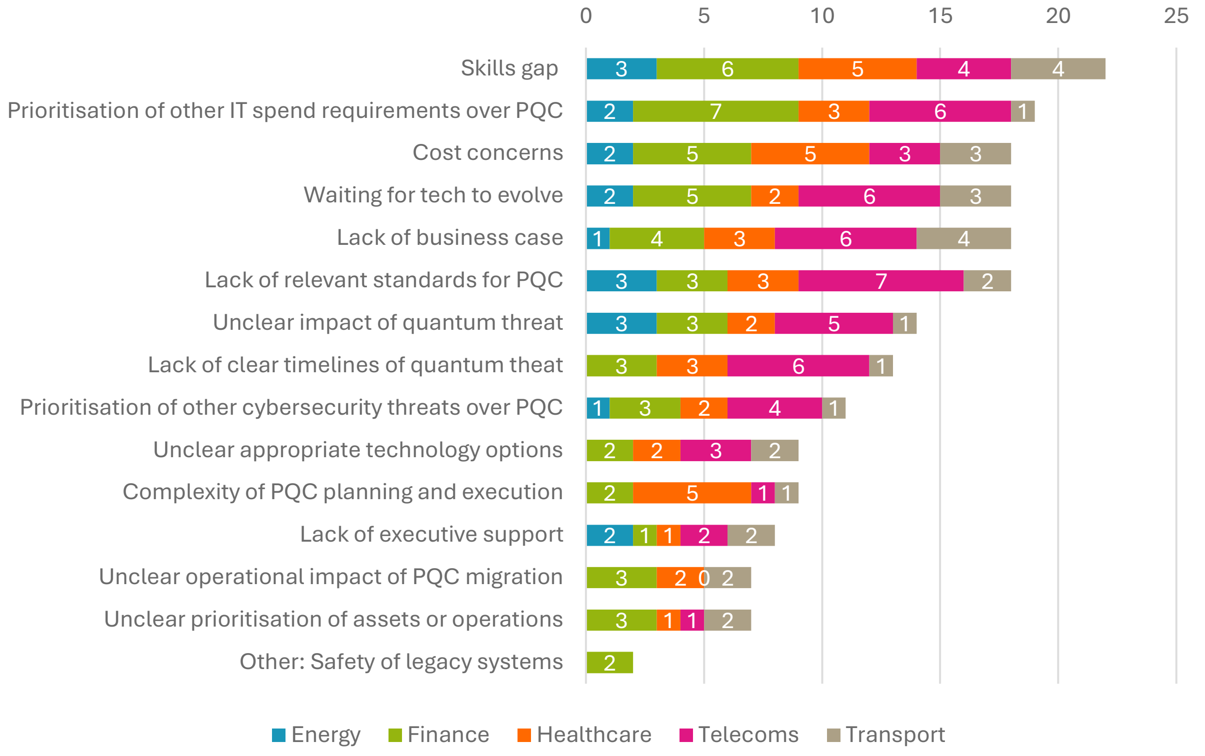
Energy sector

Interviewees from the energy sector reported significant complexity concerns around PQC migration, with a key concern being the expenditure required to remediate 40 years of Diffie-Hellman cryptography, and the lack of guarantee that the new Federal Information Processing Standards (FIPS) algorithms from NIST will remain secure against future threats.

While some expertise in PQC exists, achieving broad buy-in remains difficult due to challenges in articulating risk assessments and translating those into clear commercial justifications. Survey respondents partially disagreed, identifying the skills gap as one of the top 3 blockers. Tackling another challenge identified by survey respondents – unclear impact of the quantum threat - could be key in addressing the other two blockers previously mentioned: skills gap and lack of executive support.

Embedded devices present further obstacles, since many legacy systems lack standardised ciphers and instead rely on proprietary encryption due to resource constraints. Both survey respondents and interviewees agreed that the lack of relevant standards and guidance on PQC make the transition even more challenging.

Figure 2.13. Main PQC migration blockers for organisations, top 3 (count of respondents per sector)



Note: n = 52 survey respondents (6 energy, 12 finance, 11 healthcare, 16 telecoms and 7 transport). Respondents were asked to select their top 3 blockers. Numbers indicate the count of respondents who chose the option as one of their top 3 blockers.

Finance sector

Interviewees highlighted difficulties in effectively communicating the criticality of the quantum threat, with the lack of clear dates and timelines making it challenging to define the requirements for PQC migration. This, in turn, hinders efforts to convey the need for action to non-technical stakeholders and boards.

Both interviewees and survey respondents highlighted that more immediate cyber security threats often take priority, further delaying PQC adoption. One interviewee noted that the lack of official timelines is giving a general impression that PQC adoption is something for the future. Survey respondents also identified ‘waiting for tech to evolve’ as one of the key blockers to PQC migration.

Organisations surveyed also reported ‘skills gap’ and ‘cost concerns’ among the top 3 blockers for PQC adoption.

Finally, legacy systems were identified as another major challenge by interviewees and survey respondents, particularly in organisations with complex or ring-fenced IT environments designed to execute downstream financial tasks.

Healthcare sector

For healthcare interviewees the key issue is the difficulty in ensuring that both internal stakeholders and supply chain partners recognise the significance of transitioning to quantum-safe cryptography. One interviewee expressed a concern that many vendors are unaware that PQC even exists, which explains why many suppliers are not yet working on PQC solutions. Cultural factors also pose a challenge, particularly in conveying the importance of PQC migration within organisations. For survey respondents, the main barriers are different. They believe that the key challenges for PQC migration are skills gap, cost concerns and the complexity of planning and executing the migration.

Telecoms sector

As in other sectors, interviewees perceived cultural resistance (e.g. internal buy-in) as a significant barrier to progress, alongside a lack of PQC-ready solutions in the supply chain. Industry players noted that many suppliers fail to recognise the link between quantum threats and certificates used in everyday communication devices across laptops, TVs, and VR headsets.

For survey respondents, the main barriers come from the regulatory side (e.g. lack of relevant standards for PQC and lack of clear timelines of the quantum threat) and internal business decisions (e.g. prioritisation of other IT spend requirement over PQC, lack of business case and waiting for tech to evolve).

Transport sector

The two most frequently cited challenges by interviewees were justifying a strong business case for the migration (also in the top 3 for survey respondents) and the lack of maturity in the supply chain to provide PQC-ready equipment. Many transport decision-makers struggle with uncertainty around when they need to act, what steps are required, and how to justify investment.

Like other CNI industries with long-lifetime assets, the transport sector also faces a significant backlog of legacy systems that will need to be addressed. Interviewees and survey respondents also highlighted the skills gap as a particular barrier for small- and medium-sized businesses, which often lack access to large or specialised teams capable of developing PQC strategies.

2.2.5 Government measures to support organisations with PQC migration

Government support is seen as crucial for driving PQC adoption across CNI, with regulators, academia, and industry stakeholders calling for clearer guidance, structured transition plans, and regulatory engagement. To understand the required governmental support, the research explored industry perspectives on government intervention, sector-specific challenges, and differences in stakeholder roles and organisational viewpoints. Interviewees were asked about existing guidance they receive and what forms of regulatory or governmental support would be most beneficial. Survey questions further examined industry expectations, highlighting variations in preparedness and the types of interventions that could facilitate a smoother transition.

Overall view

Regulators stressed the need for a coordinated, government-led approach to PQC regulation, while academia highlighted the importance of NCSC guidance, industry knowledge sharing, and assurance standards to accelerate adoption.

The energy, finance, healthcare, telecoms, and transport sectors all called for clear government guidance, structured transition plans, and regulatory engagement, but their priorities differ - finance focuses on enforcement, healthcare on vendor collaboration and SME support, and telecoms on collaboration for standardisation.

Across sectors, key barriers include technical expertise shortages, uncertainty around PQC timelines and supply chain readiness. Whilst different sectors have different needs, this highlights the need for coordinated action and targeted support.

Regulator view

Regulators emphasised the need for a coordinated, consistent approach to PQC regulation, ensuring guidance is aligned where possible while allowing for necessary sector-specific differences. A clear directive from central government and NCSC would help justify resource allocation, as the current uncertainty means more immediate challenges often take priority. More specific examples can be found in Section 3.1.5.

Regulators can also help organisations within their industries by facilitating collaboration via working groups or peer support. They can also increase awareness using “stakeholder’s language” which will help with building a business case to unlock funding.

Academic view

Academic interviewees highlighted the importance of NCSC guidance and the role of academia in providing up-to-date analyses on PQC research. They emphasised the need for government-facilitated knowledge sharing to ensure industry leaders get a realistic grasp of the risks without causing unnecessary alarm. Additionally, the UK has had no Common Criteria certifying body since 2019, when the NCSC chose to stop offering that service. This was noted as a gap, with calls for clear assurance guidelines to help PQC vendors demonstrate that their products are adequately secure.

> “
> *I believe both software and hardware are a bottleneck to migration.*
>
> *In fact, the bottleneck primarily lies in the standards, as these should dictate how software and hardware communicate with each other.*
> *There are ongoing discussions[1] within international standard organisations regarding the format for private keys. NIST permits two formats, but only one can generate both key*

[1] The discussions have now ended: the international standard will support both key formats, with a complex EITHER encoding.

formats. Some hardware and software vendors oppose this change because they cannot convert existing keys to the new format. Early adoption of standards poses risks, particularly for hardware, which is less adaptable than software.

The best way to ensure consensus is to start discussions on solution-agnostic aspects of standard before the solution is chosen, so standards can be established soon after the solution choice, avoiding issues for early adopters.

- ***Academic interviewee***

Sector view

Both interviewees and survey respondents agreed on the need for regulation and guidance[2] on how to migrate to PQC. Government and regulatory involvement are considered crucial for PQC readiness, with a strong need for clear policies, technical guidance, and mandated planning. Challenges such as securing critical infrastructure and managing supply chain risks through structured guidance on cryptographic upgrades emphasised the need for government-driven policies and structured support to navigate PQC adoption effectively.

Interviewees also highlighted needing help in dealing with suppliers and vendors, either by:

- Highlighting what is required from Tier 1 suppliers;
- Working with vendors to ensure that the foundational technology is developed;
- Mandating vendors to warrant “quantum-safe” software and equipment.

For 23 out of 52 (44%) survey respondents, training security staff was identified as the main need government can help with.

Energy sector

Survey respondents were very clear: they need more guidance, either via PQC cryptographic updates (4 of 6 – 67%), PQC maturity assessments (3 of 6 – 50%), or by creating a list of accredited suppliers (3 of 6 – 50%).

Interviewees’ needs extend beyond regulation and guidance, however, and include the creation of an “industry centre of excellence”. This centre would facilitate knowledge sharing among experts and provide high-level guidance for stakeholders and businesses.

Finance sector

Staying updated on the latest PQC protocols is a priority need for 7 out of 12 (58%) survey respondents in the finance sector. There was no clear preference for the remaining options, as the votes were quite dispersed.

Beyond guidance from government, interviewees in the finance sector reported that a centrally coordinated effort across industry will help reduce the individual burden that migration poses to organisations. They also suggested the creation of a cyber advisory board involving government, industry and academia to enable knowledge sharing and technology advancement.

Healthcare sector

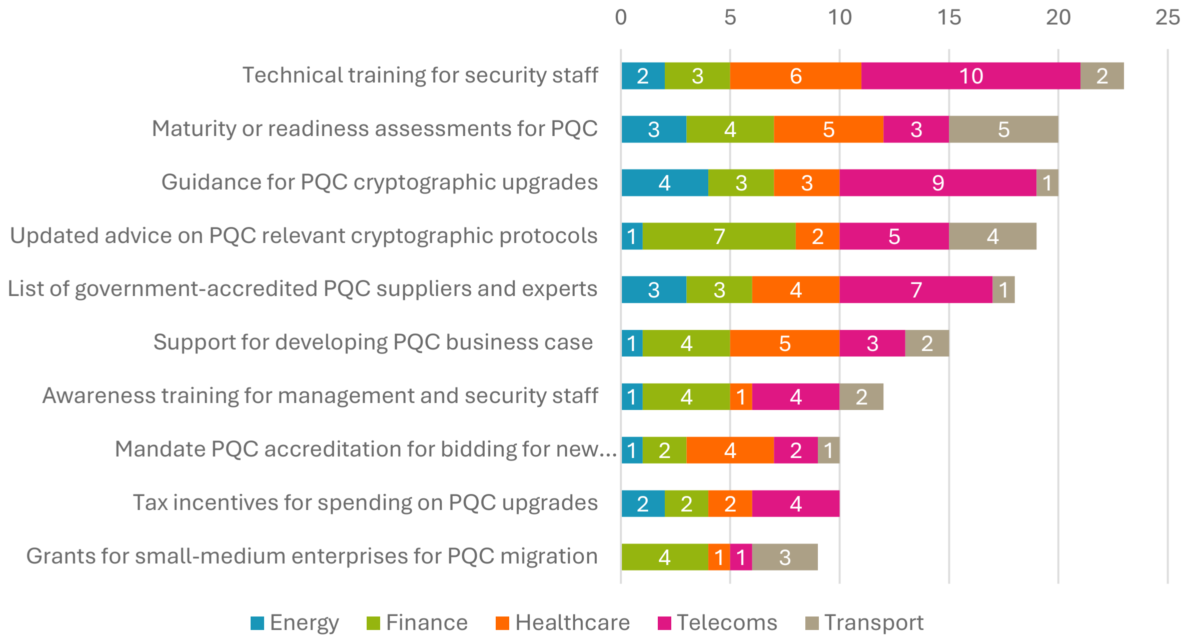
6 out of 11 (55%) survey respondents asked for technical training for their security staff, followed by support with developing a business case and the development of PQC maturity assessments (both 5 out of 11 – or 45%).

Interviewees echoed the overall need for guidance and supply chain management. They also aligned with survey respondents on asking for additional support for SMEs, which have fewer resources to innovate in PQC. They also called for funding PQC research in the UK to establish the country as a leader in this field.

---

[2] The research carried out for this report was undertaken before the public release of NCSC’s PQC migration roadmap [48].

Figure 2.14. Most important PQC migration support from government/regulators for organisations, top 3 (count of respondents per sector)



Note: n = 52 survey respondents (6 energy, 12 finance, 11 healthcare, 16 telecoms and 7 transport). Respondents were asked to select their top 3 requirements from government to support PQC migration. Numbers indicate the count of respondents who chose the option as one of their top 3.

Telecoms sector

For 10 out of 16 (63%) telecoms survey respondents, the priority was on technical training for security staff. This was closely followed by the overall needs of guidance around cryptographic upgrades (9 out of 16 - 56%) and creating a list of accredited PQC suppliers and experts (7 out of 16 - 44%).

Interviewed industry stakeholders seemed to value working with regulatory bodies to provide a coordinated transition plan with defined compliance requirements, recognising the requirement for cross-sector collaboration to strengthen guidance.

Transport sector

Survey respondents in the transport sector demanded clear guidance in the form of a PQC maturity assessment (5 out of 7 – 71%) and updates on relevant PQC protocols (4 out of 7 – 57%).

Although interviewees recognised the need for guidance, they expressed a need to be involved in its drafting early on to ensure that regulation is practical and achievable.

3. Interview programme analysis

This section provides details on the senior industry stakeholder interviews conducted in support of this study. It is structured as follows:

- Context for PQC readiness: Organisations' cyber security goals and maturity (Section 3.1.1)
- Awareness, understanding and preparedness for PQC migration (Section 3.1.2)
- Incentives and drivers for PQC migration (Section 3.1.3)
- Challenges and blockers for PQC migration (Section 3.1.4)
- Government measures to support PQC migration (Section 3.1.5)

The content presented in this section is based on summaries and analyses of the interviews completed by senior executives with technical or managerial leadership roles in the target CNI sectors, regulators for those sectors, and academic experts on quantum and cybersecurity. Methodological details on how we executed and analysed the interviews can be found in Section 2.1.

3.1 Interview findings

3.1.1 Context for PQC readiness: Organisations' cyber security goals and maturity

We asked interviewees the following questions in regards to their organisations' cyber security goals and maturity:

- *Are you familiar with any specific digital security/cybersecurity goals (or priorities) that your organisation has? If so, which are most important?*
- *Are you aware of the type(s) of cryptography your company uses for cybersecurity, and where?*
- *For how many years do you need to ensure that your digital assets are kept secure (please specify the type of assets)?*

3.1.1.1 Most important cyber security goals (Q1)

Interviewees indicated that (1) continuity of operations and (2) ensuring customer data protection and confidentiality were the most important cyber security goals across all sectors. Customer trust was mentioned multiple times as a key driver for the latter goal.

Priority of other goals varied by sector. For energy, data integrity was a key goal, driven by the need to ensure the right data is feeding into operations and control systems. Similarly, a primary goal of cyber security in the transport sector is to maintain the safety of their systems. Regulatory compliance was high on the list of cyber security priorities for financial companies, telecoms, and healthcare sector respondents. Healthcare organisations' main cyber security priorities included ensuring patient safety, and safeguarding R&D findings through intellectual property (IP) protection.

Regulators generally focused on safety of people and data privacy as the main cyber security goals for the sectors they regulate, with secondary objectives being to ensure that firms are following the NCSC guidance and keeping up with emerging threats.

Implications: *Governments and regulators should keep in mind the importance of continuity of operations, ensuring customer data protection and privacy, as key touchstones when communicating about the risks of quantum-enabled cyberattacks. It may be useful to consider prioritising these areas as 'test cases' for PQC migration.*

Energy sector interviewees

Energy sector interviewees expressed their cyber security goals as (in order of importance):

- Availability of Systems: This was the first priority, as consumers are dependent on continuous energy provision, which can only be supported by fully operational technology and information technology (OT\IT) services.
- Integrity of Data: This was a priority in order to ensure that the correct data is used to transmit information about energy usage, requirements and balancing needs that enable the network to function.
- Confidentiality of Data: This was highlighted as it is needed to ensure customer trust.

The energy regulator's view was that having a security strategy is extremely important, and it must be implemented in such a way that energy providers achieve their objectives (e.g. keep lights on/gas flowing).

Finance sector interviewees

The main cyber security goals for finance sector interviewees were:

- Maintaining customer trust
- Becoming leaders in cyber security in the industry
- Ensuring the cyber resilience of the organisation, and increased detection of advanced cyber attacks

The finance regulator we spoke with noted a further goal is to ensure firms are progressing to PQC migration and are aligned with NCSC guidelines.

Healthcare sector interviewees

The main cyber security goals for healthcare interviewees were:

- Regulatory compliance, to ensure license to operate
- Ensuring safety of patients and staff
- Privacy/data protection, as a means of building customers' trust. Healthcare providers viewed it as security-critical to prevent any data leaks
- Company resilience: protecting companies from cyber attacks and emerging threats to ensure they keep running

The sector regulator's priorities for cyber security were aligned with the priorities that were shared by the industry end-user interviewees.

Telecoms sector interviewees

Each telecoms interviewee offered a different view of key cyber security goals:

- Resilience and availability was a key goal: one interviewee commented that a large portion of society would stop working if telecoms networks failed, so networks need robust security to ensure they can continue delivering service.
- Customer data confidentiality and privacy was also an important goal for telecoms interviewees.
- Regulatory compliance was also mentioned as key.

The telco we spoke with highlighted the criticality of being perceived as 'unbreakable and trusted' by customers. The terms of their licence mean they must operate in compliance with both global and local/EU regulations - specifically NIST/DORA.

Transport sector interviewees

The main cyber security goals for interviewees in the transport sector were:

- Safety was the primary driver and goal for cyber security in this sector. From a cryptography perspective, that means preserving the integrity of assets by ensuring only trusted suppliers can push new software.

- Confidentiality was a concern, from an IP protection perspective.

Regulator interviewees

When asked about their sectors' cyber security objectives, regulators we interviewed generally focused on:

- Safety of people
- Privacy

Secondary objectives or concerns relating to cyber security were:

- Ensuring that firms are following the NCSC guidance
- Keeping up with emerging threats
- Managing stakeholder groups.

Academic interviewees

The perspective from academia was that – taking a broad view on the CNI sector - many legacy systems are reaching end of life, and should be replaced with quantum-safe alternatives to avoid expensive rework later.

3.1.1.2 Awareness of cryptography being used by organisations (and areas of deployment) (Q2)

Across the different sectors, interviewees generally reported they had a good understanding of their organisations' cryptographic estates – in other words, the types of cryptography being used for cybersecurity, and what sort of assets are being protected by these. But when commenting on the wider ecosystem within their industries, several interviewees (energy, healthcare, transport) noted they thought it unlikely that all organisations in their sectors would have a similar level of understanding. All interviewees reported being aware of the need to undertake a 'cryptographic inventory', however not everyone had started on this activity, and some sectors (energy, healthcare) reported they expected creating such an inventory to be challenging given skills gaps and availability of information.

Regulators noted that many different technologies are used in the five CNI sectors covered in this study, and these are in turn supported by a wide variety of cryptographic approaches. The challenge of upgrading cryptography for legacy equipment, and the use of bespoke or less secure approaches to cryptography, were particular concerns for energy, transport and finance regulators.

Implications: *A one-size-fits-all solution to PQC migration may not be sufficient to address the needs of all stakeholders. Advice on migration strategy must take into account the variety of currently deployed technologies and infrastructure in different sectors.*

Energy sector interviewees

Energy sector interviewees observed that:

- There were significantly varying levels of cryptographic maturity across different energy organisations; some have a very good grasp of their cryptographic estate, while others clearly do not.
- Creating and maintaining cryptographic inventories, and finding/developing people with the skills required to use cryptography effectively, is challenging.
- A lack of detailed risk information is hampering arguments for investing in cryptography projects.
- The lack of centralisation of cryptographic assets (in other words, the fact that cybersecurity strategies and deployment decisions may be made independently at multiple levels across the energy network) is also a challenge, and is holding back investment in upgrading cryptography and keeping it up-to-date.

Finance sector interviewees

Finance organisations shared the following points:

- They are aware of the types of cryptography used, and are building cryptographic inventories.
- Specific cryptographic schemes cited included Symmetric and Asymmetric Hardware Security Modules (HSM).
- One respondent said they were building a 'landscape map' of threats.
- Larger firms such as banks are more aware of their cryptographic estates than smaller organisations.

Healthcare sector interviewees

Healthcare organisations had the following views on cryptographic awareness in their own organisations, and in the sector more broadly:

- All healthcare organisations we interviewed highlighted that they understood the importance of creating cryptographic inventories.
- However, some commented that the level of detail and rigour varies between organisations across the sector.
- Several respondents mentioned the Cyber Associates Network - a peer-support group for the healthcare sector, hosted by NHS Futures – which hosts discussions and presentations about cyber security topics, including PQC.

The regulator believed that healthcare organisations have knowledge and information about cryptography and how it is threatened by quantum computers, but do not have a strong workforce of experts. The cyber workforce in the sector tends to have jobs that cover a mix of information, governance and cyber security IT roles.

Telecoms sector interviewees

Telecoms sector interviewees indicated they have started to build their cryptographic inventories, and all were highly aware of the importance of doing this.

- One telecoms provider interviewee stated their aim will be to deliver 'quantum-safe' solutions without increasing customer bills.
- Telecoms interviewees indicated their systems rely heavily on public key infrastructure (PKI).
- One of our interviewees in this sector was a certificate authority (which serves the telecoms industry but also other industries). They are already actively migrating their PKI to be secure. Certificate authorities must adhere to strict technical guidelines to ensure interoperability. This means that the industry needs to collaborate on PQC adoption.

The regulator is interested in cryptography analysis to mitigate end-to-end encrypted threat vectors for telecoms apps such as Telegram, Signal, and IRC. They have a vested interest in managing concerns around the nefarious use of encryption. Their focus includes enhancing safety and privacy across encrypted channels, monitoring user behaviours and platforms, and addressing threat vectors associated with VPNs, TOR, and Dark Web channels, including ransomware, sextortion, and catfishing.

Transport sector interviewees

Transport sector interviewees reported using a wide range of cryptographic technologies.

- This variety is driven by the fact that they manage IT and OT systems that have very specific needs.
- Transport organisations that also operate in the US are compelled to build cryptographic asset lists (CBOMs), and reported they were already engaged in that process. Some companies reported that mapping from the application layer down to specific mathematical problems is a challenge.

- One interviewee acknowledged their lack of awareness of which cryptography is being used in their products.

Regulator interviewees

Regulators noted that many different technologies are used in the five CNI sectors covered in this study, with a variety of cryptographic approaches and algorithms used as a result.

- For example, some organisations in the energy sector use bespoke cryptography algorithms that were developed prior to the establishment of standards.
- The transport sector regulator was worried that players in the sector would face challenges in upgrading legacy equipment to support new quantum-safe cryptography.
- In the telecoms sector, there are concerns about misusing encryption for illegal activities.

A specific concern for the finance regulator was risk associated with the use of shorter keys by smaller financial organisations.

Academic interviewees

Academia has access to highly skilled experts who have a deep understanding of cryptographic libraries and the algorithms that need the most pressing attention; however it is not clear that this expertise is currently being utilised to support the needs of industries.

3.1.1.3 Ensuring security of digital assets: Organisations' understanding of requirements for security duration and how this applies to different data/asset types (Q3)

Interviewees indicated a very wide range of different security duration requirements, in the different CNI sectors we engaged with. These ranged from as little as 12-18 months (for healthcare R&D data) to as many as 70 or more years (e.g. for nuclear energy-related data and assets in the energy sector). In general, the energy sector appears to have the longest duration requirements for keeping data and assets secure, with the transport sector also looking at very long-duration security requirements for some cyber-physical systems such as vehicles.

Regulators we spoke with were less specific on the requirements for duration of data security in the sectors they regulate.

Implications: *The variety of digital and physical asset types involved, and the range of secure duration requirements, will add to the complexity of planning for PQC migration. In our view, a key first step - that government and regulators could highlight for industry - will be nailing down specifics on these requirements. This will help to ensure that assets are being prioritised appropriately, so that they will be protected against potential quantum attacks in time, and for the required duration of time. This will need to take into account the potential for 'harvest-now-decrypt-later' attacks as well as more direct quantum-enabled cyber attacks.*

Energy sector interviewees

Different subcategories of energy sector activities need to provide different levels and durations of data/digital asset security, to meet compliance requirements. Compliance in this sector entails meeting multiple objectives: legal, safety, and environmental compliance, as well as market integrity. Data and asset security duration requirements reported by energy sector interviewees were:

- General – Energy Trading and Markets – up to 10 years
- Renewable Energy – up to 20 years
- Oil and Gas – up to 30 years
- Smart Metering – up to 50 years
- Nuclear – up to 70+ years

Finance sector interviewees

For the finance sector, security duration requirements are clear, but vary across asset types:

- Finance regulators mandate keeping data for 5 years after the end of a customer relationship
- Some financial products - such as mortgage data – require data to be kept securely for 25 or more years
- For certain types of engagements, finance sector data protection requirements could be as long as over 120 years

Healthcare sector interviewees

Healthcare sector interviewees differentiated between data and infrastructure security lifetimes.

There were different timelines for data/asset protection, based on the type of data:

- 12-18 months for confidential R&D data (confidentiality is key)
- 7-10 years for financial and recruitment legal compliance (integrity is key)
- Indefinitely: IP data needs to be available for the lifetime of the patent and board information for the lifetime of the company

A further comment regarding infrastructure was that some systems will be in place for 20-30 years, and need to be secured throughout their lifetimes.

Telecoms sector interviewees

In the telecoms sector, a key consideration was timelines for confidentiality of customer data, which are ruled by GDPR guidance.

Digital assets for telecoms interviewees included:

- Customer data
- Communication applications
- Social media applications

Data types identified were:

- Encrypted files for communication
- Passwords used for multi-factor authentication (MFA)

For telecoms infrastructure, interviewees noted that data must be kept secure for the lifetime of the systems.

One concern in this sector was that customers are highly focused on continuous service availability, so switching out equipment (on the customer site) is considered risky, as it may lead to service interruptions. Typically, service lifetime for equipment is 3, 5, or 7 years, but many customers refuse upgrades (want to keep their old equipment), which may leave their devices more vulnerable to cyber attacks.

Transport sector interviewees

In the transport sector, interviewees reported that:

- Some cyber physical systems (e.g. vehicles) need to be maintained for up to 80 years.
- In some cases, the digital assets need to be maintained for up to 30 years beyond that.

Regulator interviewees

Regulators we spoke with were not very specific on this question. Several indicated concern about preserving confidentiality and data integrity. Some of the timeframes they shared were:

- The finance sector has a 25-year retention policy.

- In the energy sector, timeframes are quite varied and could go beyond 70 years for old equipment still in use.

Academic interviewees

Academics were not asked this question.

3.1.2 Awareness, Understanding and Preparedness for PQC migration

We asked interviewees the following questions relating to their awareness of, understanding of, and preparedness for PQC migration.

- *How much do you know about the impact of quantum computing development on cybersecurity?*
- *Are you aware of what types of cyberattacks quantum computers can enable, and/or which types of cryptography are most at risk?*
- *How do you think the risk posed by quantum computers compares to other cyber risks your organisation is managing today?*
- *In your opinion, when do you think quantum computers would constitute a real threat and why?*
- *How do you think the level of risk posed by quantum computers will change in 5-10-30 years' time, in comparison to other cyber risks?*
- *Has your organisation already started exploring or planning for using PQC? If so, please provide details (e.g., expected timeline, expected effort, cost, priority, level of engagement from Board/senior stakeholders)*
- *Are you aware of any PQC advice or resources? Which ones?*
- *Are you currently receiving guidance on PQC migration from any of the following: Government or regulators/Industry associations/External consultants/Cybersecurity technology provider(s)/Other?*

3.1.2.1 Awareness of quantum impact on cybersecurity (including types of attacks and types of cryptography that would be impacted) (Q4 + Q5)

Overall, interviewees were well aware that quantum was likely to impact cyber security. Several interviewees specifically mentioned concern over quantum-enabled 'harvest-now-decrypt-later' attacks. Several also highlighted concerns relating to long lifetimes of infrastructure and/or supply chain contracts, and how quantum might impact the security of the associated assets. In the healthcare sector, there was particular concern over impact on security of patient data.

Some (but not all) interviewees were able to identify specific types of cryptography that could be vulnerable to quantum-enabled attacks

Regulators clearly understood the impact that quantum computers will have on the development of cyber security. Similarly to industry end-users, regulators cited 'harvest-now-decrypt-later' attacks as a threat, and also mentioned legacy infrastructure as a key concern. One regulator specifically called out the need to monitor how quantum compute hardware development (not just algorithms) can affect encryption supply chains.

Implications: *Raising awareness of quantum impact on cybersecurity in general for government and regulators may not be needed; however, more specific support on how to monitor quantum developments, and on specific types of attacks and threat areas, could be valuable.*

Energy sector interviewees

Energy organisations were all aware that PQC is going to impact cyber security:

- One discussed their concerns on the impact of 'harvest-now-decrypt-later' attacks, given the presence in the network of long-lived assets such as smart meters (and their associated data).

- One believed that the commercial potential of PQC could be massive for vendors that can offer 'quantum-safe' solutions.

Energy sector interviewees' awareness of types of quantum-enabled attacks and types of cryptography at was reasonably high.

- The most pressing risk identified by interviewees was 'harvest-now-decrypt-later' attacks, as data can be intercepted between systems today while systems are vulnerable, and subsequently broken when quantum computers become powerful enough to target asymmetric cryptography.
- Energy sector interviewees were aware that asymmetric encryption, key exchange mechanisms and digital signatures are under threat. The key types of schemes they identified as being under threat are RSA, Diffie-Hellman, and elliptic curve encryption schemes. These can be broken using quantum computers that are capable of solving the factorisation of primes (RSA), and the discrete logarithm problem (DH and ECC).

The energy regulator noted that old energy infrastructure and equipment (some of which has been in service for over 30 years) lacks critical cryptographic protections like session authentication and message integrity verification, making it vulnerable to quantum attacks.

Finance sector interviewees

Finance sector interviewees were aware of the significant threat that quantum computing poses to current cryptographic methods.

- They recognised that quantum-enabled cyber attacks, such as 'harvest-now-decrypt-later', are going to expand the threat landscape.
- One interviewee noted that novel types of quantum-enabled attacks are likely to emerge, that haven't yet been seen or thought of, which increases the threat.
- Interviewees in the finance sector saw 'harvest-now-decrypt-later' attacks being the biggest risk, among quantum-enabled attacks.
- One finance sector respondent commented that AES-based encryption is becoming more vulnerable due to quantum computers.

Healthcare sector interviewees

Healthcare sector interviewees were widely aware of quantum computers, and the need for PQC migration was on their radar. Comments from healthcare interviewees included:

- Historically, losing encrypted data was not a confidentiality problem in healthcare, because the encryption was impossible to crack. But with 'harvest-now-decrypt-later' attacks, there is a significant risk relating to data with longer lifespans (e.g. financial or regulatory data).
- High security controls beyond encryption should also be in place to prevent data leaks.
- As algorithms evolve, they will become more difficult to decrypt, which may cause friction in daily activities, as well as increase energy requirements and carbon footprint.
- Quantum computers could negatively affect IT supply chains, because the healthcare sector often has contracts for services and equipment that run for between 10-15 years, and quantum is expected to become a reality in this timeframe.
- Interviewees were aware that digital certificates will be able to be modified and falsified, using quantum-based attack techniques.
- Traditional public key cryptography, especially RSA, will be easily decrypted using quantum.

In terms of regulation, there was a view that companies in this sector need more advice and guidance, because current regulation is too broad.

Telecoms sector interviewees

Telecoms industry end-users we interviewed were highly aware of the risks of quantum, and very knowledgeable about the need for PQC. Key points they raised included:

- 'Harvest-now-decrypt-later' is a current concern. The telecoms provider we spoke to is looking to assess which part of their estate holds valuable data that could be intercepted and then broken by a quantum-enabled attack in five years' time.
- The first target will be the software supply chain; an attacker would be aiming to break one certificate. Once a certificate is stamped, it remains valid indefinitely. Consequently, all software that isn't post-quantum secure will become unreliable, as the integrity of the software's certificates can no longer be guaranteed.
- The Certificate Authority we interviewed stated that they are proactively raising awareness about the importance of migrating to PQC within the industry and their customers. One argument they present is that every company has critical assets that need protection from quantum attacks aimed at cloning root certificates.

The telecoms regulator is reliant on guidance and inputs from industry experts. They are working on understanding the real use cases of quantum for cyber attacks at scale; in other words, those which could impact 80%+ of the UK population.

Transport sector interviewees

Transport sector interviewees focused on 'harvest-now-decrypt-later' attacks and safety threats:

- All respondents mentioned 'harvest-now-decrypt-later' attacks as a likely quantum-enabled threat.
- The importance of safety in this sector means that attacks which compromise integrity [of data/systems] are a significant source of concern.
- One interviewee noted that faking digital signatures using quantum computers will only be an upgraded version of an attack that can currently be performed.
- All interviewees felt that there could be more awareness in the supply chain of the different attacks that quantum could enable.

Regarding awareness of types of cryptography at risk, interviewees in this sector had varying levels of understanding:

- One respondent was aware that quantum computers can easily solve Shor's algorithm, which can crack the three key standards of PKI. They understood that if an attacker can decrypt at speed, they would be able to spoof without being detected (guess the code, change the signal). However, there are challenges in doing that at '30,000 feet in the air'.
- One interviewee identified that asymmetric data is what is at risk from quantum.

Regulator interviewees

The regulators we interviewed clearly understood the impact that quantum computers will have on the development of cyber security. Observations in regards to types of attacks and areas of vulnerability included:

- 'Harvest-now-decrypt-later' attacks will be damaging for things like IP theft, but not so much for safety-critical systems.
- Quantum compute hardware development is critical: as qubit quality increases, so will the threat to secure cryptography.
- PQC can affect encryption and supply chains.

- Old equipment lacks essential cryptographic protections, which makes it vulnerable to quantum computers.
- RSA was mentioned as the main type of cryptography most at risk. But any cryptography reliant on the factorisation of primes is under threat.

Types of quantum-enabled attacks specifically mentioned by regulators were:

- 'Harvest-now-decrypt-later'
- Spoofing (if quantum computers were able to decrypt at speed)
- Faking digital signatures
- Brute force
- Ransomware

Academic and industry association interviewees:

Academics we spoke to had a good understanding of the relationship between quantum computing development and cyber security.

- One academic expressed a strong view that industry end-users were not taking the threat seriously enough, and that early action was really needed. despite what may appear to be a long timeline before a potential attack.
- Re types of cryptography at risk, the academic view was that the impact on asymmetric cryptography is no longer up for debate. Differences in opinion remain on the impact on symmetric cryptography. Some said that the speed-up offered by Grover's algorithm is unlikely to have any meaningful impact, whereas others believed the speed-up could require organisations to increase key lengths to prevent brute force cyber attacks.

3.1.2.2 Prioritisation of quantum threat vs. other cyber security risks (Q6)

All interviewees acknowledged the risk of quantum computers to cyber security. Several interviewees commented that their organisations were not prioritising the quantum threat, because of other immediate cyber security risks. Boards and financial approvers are looking for clear ROI calculations and/or regulatory mandates to drive priorities in this area. Some interviewees – notably in the finance, healthcare and telecoms sectors – suggested that the quantum threat may be a low priority for organisations because it is not being properly assessed. Other comments from interviewees centred on concerns around quantum vulnerability of old and legacy systems, and the need for quantum-safe options for cyber security.

Most regulators believed that quantum computers pose a moderate threat currently, compared to other cyber risks; the view was generally that while quantum's impact will be significant, it hasn't materialised yet.

Implications: *To support organisations in preparing for PQC migration, regulators and government may need to provide clearer information on threat timelines. It will also be valuable to provide support on how stakeholders can communicate the importance of PQC migration planning, in the face of other, seemingly more pressing cybersecurity threats.*

Energy sector interviewees

Energy companies reported that risk management approaches – including anything PQC-related – are heavily driven by compliance requirements and financial metrics.

- One energy company noted that risk management in their organisation is driven by information fed to the board. The challenge is that the board relies on inputs from regulatory bodies and upstream industries. Those industry players generally agree that while the threat is acknowledged, it is not yet urgent. Therefore, the board are prioritising other pressing cyber security risks for now.

- NCSC mandates are necessary for the board to make executive decisions on cyber security, providing them with the incentive to take action.
- Compliance-driven mandates, such as GDPR, also help initiate programmes.
- Action can only be taken if risk is expressed in monetary terms, which are derived from criticality impacts.
- Having a plan is crucial, even if it is not implemented immediately, so that a roadmap of activities can be planned for actioning.

Finance sector interviewees

Financial services organisations reported challenges in prioritising – and communicating about – the risk of the quantum threat.

- Organisations in this sector are aware of the emerging threat of quantum computers and the risks and impacts of 'harvest-now-decrypt-later' attacks.
- Quantum threats are being monitored, but there are other more immediate objectives.
- Quantum risks are qualitatively different from existing risks in the organisations' register.
- Recording and communicating pervasive risks like quantum threats is challenging.

Healthcare sector interviewees

- The quantum threat is not yet realised, so it is not currently considered a high risk.
- Other immediate threats like AI are higher in the stack, and thus prioritised by companies in the sector.
- Among the quantum threats, 'harvest-now-decrypt-later' was perceived as the highest one, so having the right data protection measures in place against intruders is a must.
- Guidance on quantum threats may enable healthcare organisations to get the foundational protection basics right.

Telecoms sector interviewees

Quantum risks did not rank high on the risk priority list for interviewees in the telecoms sector.

- The view was that quantum computers are not available today, and there are more pressing risks they need to focus on.
- One telecoms industry practitioner shared that the reason why the quantum threat is not seen as pressing could be that it is not properly assessed. The interviewee noted that impact and probability are always considered in risk assessment. However, a quantum risk assessment should also consider things such as the value of the data being secured, the lifetime it needs to be secured for, the risk of an attack, and the window of vulnerability – this makes assessment more complex.

The telecoms regulator also indicated their view was that the threat is quite far away, although they are starting to think about it and have commissioned research to do horizon scanning on quantum tech for the next 3-5 years.

Transport sector interviewees

The transport sector interviewees felt that the risk from quantum would worsen in the near future, but that for now there were other risks that were of similar importance.

- Some felt that other sectors would be more attractive to the type of adversary who could access a quantum computer; and that therefore by implication the transport sector would be a follower rather than a leader when it comes to PQC migration.

- In contrast, others felt that the risk of quantum-enabled ‘harvest-now-decrypt-later’ attacks justified immediate action.

Regulator interviewees

Most regulators thought that, compared to other threats, quantum computers lie in the middle of the stack.

- The general view was that although the risk is coming and will have a great impact, it has not been realised yet.
- One regulator (telecoms) has commissioned some work to do relevant horizon scanning for the next 3-5 years; they are ‘keeping a watching brief with NQCC’.

Conversely, one regulator stated that they are more focused on imminent threats, and they lack resources to think about considering policies for matters that are more than 10 years away (e.g. quantum computers).

Academic interviewees

- Academics working in the field are concerned that the threat posed by quantum computers is not well-understood enough by industry to motivate sufficient action.
- The prevailing opinion was that the breaking of asymmetric cryptography is an inevitability, and we may not know when it has been achieved (because this is likely to happen behind closed doors in a government-funded environment).

3.1.2.3 Timeline for the quantum threat (Q7)

Views on the timeline for the quantum threat varied significantly among interviewees. Overall, ~50% of interviewees believed the quantum threat to cybersecurity would become a reality in the next 10 years. Regulators’ views on the timeline for the quantum threat varied, with one regulator (financial) estimating a timeline of ‘less than 5 years’, one estimating ‘5 to 10 years’, and two estimating ’10 to 15 years’ (one was unsure).

Implications: *Providing clarity on the quantum threat timeline will be an important aspect of the support that regulators and government can provide to industry.*

Energy sector interviewees

Energy sector interviewees held a variety of views on the quantum threat timeline:

- One energy network operator said that quantum computers will be a real threat within 3 years, and we will have very little warning.
- Another interviewee believed that quantum computers will become a material threat within 10 years.
- The energy regulator said that quantum computers could be a threat in 5-20 years’ time.

Finance sector interviewees

Predictions from the finance sector regarding the quantum threat ranged from 5 years to 12 years. One organisation mentioned there could be impact from the recent breakthrough by Microsoft which could enable mass production of quantum chips, potentially starting in the next 18 months.

Healthcare sector interviewees

Healthcare interviewees were unclear on the timeline for the quantum threat.

- Answers included five years, less than five years, or longer than five years.
- One interviewee believed that cryptographically-relevant quantum computers are already becoming available, and cited IBM’s major breakthrough in error correction and the intention of making quantum computing available to the public market in 2027.

Telecoms sector interviewees

Telecoms end-user organisations did not give a specific time range, but shared the following views:

- The first time a QC breaks a cryptographic key will almost certainly be done by a nation-state and won't probably be publicised.
- There are a lot of things that need to happen (e.g. physical logic, enough stable qubits, etc.) before a quantum computer becomes cryptographically relevant and cracks Shor's algorithm.
- According to Gartner 2029 is the year when advances in quantum computers will make asymmetric cryptography unsafe [34], but there is some question as to the likely accuracy of that forecast.

The telecoms regulator acknowledged they lack the resources to focus on long-term (10-20 years) policy considerations, due to a tendency to prioritise immediate concerns. However, this could change in the future.

Transport sector interviewees

Transport sector respondents also had varying views about the quantum threat timeline. They acknowledged the potential for 'harvest-now-decrypt-later' attacks, which effectively could be a threat today; other respondents said 10 to 15 years was the likely timeline.

Regulator interviewees

Answers were varied among regulators:

- In the next 5 years, although testing and use cases could be sooner (Finance)
- Between 5-10 years, but could be as long as 20 (Energy)
- More than 10 years (Telecom)
- 10-15 years (Transport)

Academic interviewees

Most academic interviewees gave an estimate of between 5 and 15 years.

3.1.2.4 Expected evolution of risk posed by quantum computers over the next 5-10-30 years (Q8)

Interviewees in most sectors expected quantum computing technology to drive an increase in the likelihood of quantum-enabled attacks as it develops over the coming years; and that thus mitigation efforts would need to increase over time. Most did not expect this to be until attacks are seen in the wild, which they did not believe would be within the next five years. Interviewees generally believed that nation-states are more likely to use a quantum computer first, and to use it against another nation-state. Both energy and telecoms sectors believed that after the nation-state-to-nation-state attack, the finance sector will be next, with rogue actors aiming for financial assets. Among industry end-users, this translates into some extra time for them to prepare against the threat.

Regulators expected the quantum risk to increase within the next five years. Most of them have adopted the continuous monitoring of technological advances as a key strategy. The transport regulator shared their assumptions on the timeline for the first quantum computer. They believe that the first quantum computer will be owned by a nation-state in 10 to 15 years and used to attack other nation-states. In 20 years, the technology will be mature enough to be available to the public.

Implications: *Similarly to the previous question, the implication is that industry practitioners largely believe they have the luxury of some time before quantum-enabled cyberattacks become a significant threat (with finance being the exception), and government and regulators need to help industry to understand not only the timelines for quantum, but also the timelines for migration, in order to help them plan appropriately.*

Energy sector interviewees

Energy end-users did not share specific views on how the quantum cyber risk will change over time.

- One stated that a quantum attack will happen in less than 10 years, but believed it will likely be against the defence or finance sector (rather than the energy sector).
- Another industry practitioner expected Tier 1 suppliers to manage the quantum risk.

The energy regulator's view was that the risk of quantum computers depends on when they actually materialise. In other words, if quantum computers arrive in a couple of years, there is a significant risk (as industries will not be ready), but if they arrive in 30 years, then industries will be better prepared because of the mitigations being put in place between now and then.

Finance sector interviewees

Finance sector interviewees predicted timelines for the threat ranged from less than five years, to 7-12 years.

- Some finance interviewees believed that within the next 18 months, we could see significant advancements in quantum computing capabilities that could pose a threat to legacy encryption methods, particularly AES-based encryption. They expect that AES-256 encryption could potentially remain secure for about five more years.

Healthcare sector interviewees

Healthcare interviewees believed that the quantum risk will increase as technology advances, and that quantum computers will be able to crack polynomial calculations (essentially cryptography).

- However, there were some different, and even contradictory, views among healthcare interviewees on the evolution timeline for the risk.
- One interviewee believed that the risk would likely increase with every technological advancement.
- Another believed that the risk would not change significantly in the next 5 years.

Telecoms sector interviewees

Telecoms industry end-users believed that as quantum technology advances, the risk of cybersecurity threats will increase.

- One interviewee stated that - based on publicly-available roadmaps, quantum computers won't break shared algorithms in the next five years. The interviewee believed that 20 years is a reasonable timeline for quantum computers to become a major threat.
- In terms of the risks that telecoms organisations will face during this time, the Certificate Authority (CA) interviewee believed that the biggest risk lies in the transition to quantum-safe algorithms. Until organisations fully switch over, PKI systems are vulnerable. Governments and defence intelligence might crack encryption with quantum computers before the public is aware, making telecoms companies vulnerable until all root certificate authorities and issuing certificate authorities use quantum-safe algorithms.

The telecoms regulator has an ongoing horizon scanning program to monitor the quantum outlook, and is trying to understand critical aspects of quantum's future evolution; e.g. developments in Partial Quantum error correction capability. The regulator is working closely with the NQCC (National Quantum Computing Centre) to monitor the quantum landscape with a view to being ready for a potential "sputnik moment' in quantum.

Transport sector interviewees

All transport sector interviewees stated the quantum risk would worsen over time.

- Transport sector interviewees acknowledged that nation-states who are developing cryptographically relevant quantum computers would be the most pressing threat, but felt that commercial availability of quantum would be the real driver for increased risk.

Regulator interviewees

All regulators we spoke to are monitoring technological advances in the quantum field.

- One regulator commented that they believe the quantum risk will increase in the next five years.
- Another commented that they expect the first quantum computers to become available in 10-15 years for nation-states, and that they will then be available for broader commercial use in 20 years.

Academic interviewees

Academics believed that the evolution of risk over time will depend on actions taken today.

- Migration to PQC will prevent the risk from getting worse.
- It is important to consider the cost of building and operating scalable quantum computers, which will affect the feasibility of launching widespread attacks.

3.1.2.5 Status of progress on PQC migration – have organisations started planning or implementing migration (Q9)

PQC migration is in early stages for most interviewees' organisations, with respondents indicating varying levels of awareness and organisational preparedness. While some industries are actively planning and implementing early measures for PQC migration, others are delaying due to technical challenges, cost concerns, and reliance on the IT vendor supply chain. Both industry practitioners and regulators acknowledge the importance of monitoring and preparedness in reducing the risk posed by quantum computing. Two distinct approaches could be distilled from the interviewees' responses (bearing in mind that we interviewed a limited number of organisations in each sector, so views may not be entirely representative):

- **Active Preparation**: Organisations proactively producing a cryptographic inventory, engaging with experts and vendors, and implementing measures to safeguard against quantum threats. This was most common in the finance and energy sectors, but some respondents in most other sectors also fall into this category.
- **Passive Monitoring:** Organisations continuously observing the quantum threat landscape, but primarily relying on vendors to develop and provide 'quantum-safe' solutions that can be seamlessly integrated into existing networks. Telecoms and healthcare are more likely to fall into this category; these sectors may face greater challenges due to infrastructure complexity and vendor dependencies.

Regulators indicated they were hesitant to mandate standards for PQC due to the rapid evolution of cryptography. Most were taking a cautious, observational approach. The finance regulator indicated concern over the preparedness of small and medium sized businesses in their sector. Some regulators also perceived that PQC readiness in their sector was lower than our responses from industry practitioners suggests; this would be worth exploring in future industry-level discussions.

Implications: *Governments and regulators could be more proactive in engaging with industry to 'meet organisations where they are' (in different sectors), in terms of progress on PQC migration. There could be a useful role for governments and regulators to assist organisations in understanding when and how to move to more active preparation for PQC.*

Energy sector interviewees

Interviewees in the energy sector stated that they have already started their migration journey.

- One industry end-user noted that some planning has begun, with a few Proofs of Concept (POCs) already established. The initial challenge is scoping the estate, which involves determining what to scope and what to migrate. They acknowledged their high dependency on vendor management, such as Thales for Hardware Security Modules (HSMs), or Entrust for Entrust Online Certificate Authorities (CAs).

- Another industry practitioner added that exploration is also happening at a regulatory level, and that future business cases will require disclosure of PQC plans. This reflects a common theme of complexity and vendor reliance, with some differences in the stages of planning and regulatory involvement.

Finance sector interviewees

All finance interviewees had started planning the migration, but not started the PQC migration itself.

- One of the organisations we interviewed is looking to change internal policy and standards to create more actionable guidance.
- They are also looking to architect the systems to enable updating with future cryptography.

Healthcare sector interviewees

Healthcare organisations have started planning their PQC migration, although none have started the migration itself.

- Healthcare companies depend on their [security] vendors to migrate.
- One interviewee observed that security cannot be treated as a unique selling point (USP) for medical products or services. People expect such devices to be secure, and are not willing to pay extra for it. However, they will question security if something goes wrong.

The regulator believed it is likely that healthcare organisations are aware of the big task of migrating to PQC, and may have started some preparations, but at a minimal level.

Telecoms sector interviewees

Telecoms industry end-users have all started planning for their PQC migration.

- The Certificate Authority we interviewed is ready to issue post-quantum certificates, but noted these will be useless until software companies create post-quantum libraries and software able to work with these new certificates.

Transport sector interviewees

Different transport organisations are at different levels of readiness. Some have already built roadmaps of activities to achieve migration.

Regulator interviewees

- Regulators in the transport and healthcare sectors believed that some minimal advances in preparation for PQC migration are taking place. The energy sector is considering regulatory interventions to request disclosure of PQC plans.
- The healthcare sector has recently aligned with the NCSC's Cyber Assessment Framework (CAF), which sets out a number of outcomes and profiles for organisations to achieve. The CAF-aligned Data Security and Protection Toolkit (DSPT) approach is geared towards using principles and expert judgement to guide competent decision-making, with a focus on achieving key outcomes. Organisations conceive of CAF profiles as the standard they need to achieve. The regulator plans to take action in relation to CAF compliance.

Academic interviewees

All academics emphasised the pressing need for PQC migration. Comments included:

- Most industry end users want to buy in PQC (network vendors, routers, spinning disks), and with general industry estimates indicating that it would take 7 years to replace networks and spinning disks, PQC should be on the agenda now.
- Planning should ideally have started earlier, but protocols were not there.

- Migration should start as soon as possible if hardware permits. Hardware that can support PQC is now becoming available so new software protocols could start to be embedded soon.
- CNI organisations should educate themselves and move to new standards after evaluating what those mean for them.

3.1.2.6 Details of Progress on PQC Migration Journey, from organisations that have already commenced (Q10)

For those organisations we interviewed that had already started planning for or implementing PQC migration, we asked them to share some details of how the journey was progressing. We asked about five areas: (1) the expected length of time they expected migration to require; (2) skills needed and/or expected effort levels; (3) expected costs, to the extent they could comment on this; (4) Board awareness and support for PQC migration; and (5) any other comments. In general, organisations we interviewed reported that they expected significant effort requirements, complexity, and expected costs related to migration. These were often poorly understood – although there was some limited consensus on the expected length of time a PQC migration would take (most respondents said several years would be needed). The lack of clarity is not surprising given the early stage of migration and planning for most organisations, but is in itself a source of risk and potential delay. The need to communicate at an appropriate (and not overly technical) level with boards and senior stakeholders was mentioned by a number of respondents as a particularly important requirement.

Implications: *High levels of uncertainty around many critical aspects of PQC migration were clear from the responses to this question (note that many points raised are addressed more explicitly later in this section, where we discuss responses in regards to challenges for PQC migration). Overall, the limited visibility and certainty around key aspects of the migration task is almost certainly holding many organisations back from embarking on PQC migration planning and execution. Government and regulators could help by providing clearer guidance, support for business case development and materials to enable clear communication about strategies and options for migration. This could potentially be done in partnership with appropriate third parties (e.g. technology vendors, standards organisations, etc).*

Energy sector interviewees

- MIGRATION DURATION – No specific comments.
- EFFORT / SKILLS – Energy interviewees highlighted the need for significant effort in testing, quality assurance, and governance, to transition services to production. They also emphasised the importance of conducting POCs to reduce risks and increase knowledge. There is a need to understand the planning for the cost of IT versus the cost of OT. Testing will likely show that some algorithms perform better with hardware acceleration, although standardisation is still required.
- COST – The estimated cost of PQC migration is high, particularly associated with testing, quality assurance, and governance for service transition to production. Industry practitioners are thinking about the investments needed and are tracking and monitoring these costs.
- BOARD AWARENESS – Interviewees did not provide specific information on board awareness of PQC in the energy sector.
- OTHER – Energy companies are focused on reducing risks and increasing their knowledge through tracking and monitoring. They also noted that testing will likely prove that some algorithms perform better with hardware acceleration, but standardisation of these algorithms is still needed. The regulator emphasised that sector-level planning is still in its early stages and will require government intervention to progress further.

Finance sector interviewees

- MIGRATION DURATION – No specific comments. One organisation mentioned enabling quantum lattice encryption on a customer front-end next year.
- EFFORT / SKILLS – Cryptography knowledge is required. Considerable effort will be necessary, due in part to the need to consider regulatory requirements and impact on integration across systems and organisations.
- COST – The cost was difficult to estimate at this stage of their journey. Organisations reported they were still in the planning stage, and building an inventory.
- BOARD AWARENESS – Organisations mentioned barriers in communicating about PQC to the board. There is a lack of board buy-in, as quantum computers are neither a pressing threat nor a clear business opportunity yet.

Healthcare sector interviewees

- MIGRATION DURATION – Migration was expected to require at least a few years. One of the interviewees expected that announcement of the first known fully viable quantum computer would likely be the trigger for accelerating the migration; although they also recognised that it may be too late by then to protect their own systems, and that they would potentially need to start planning much earlier.
- EFFORT / SKILLS – For big organisations with their own managed services, technical partners and hyperscalers, coordination between all three of these parties will be necessary. The cyber security team may require assistance from external experts/consultants.
- COST – Although noting this was difficult to estimate, the interviewee gave a rough estimate of the order of magnitude: a 'plug and play' transition could be in the realm of £100k, whilst a more radical change could easily require millions of pounds.
- BOARD AWARENESS – The interviewee reported their board had little awareness, and noted that it is difficult to pitch a PQC plan to the board when the topic is so complex and timelines are unclear.

Telecoms sector interviewees

- MIGRATION DURATION – Telecoms providers we interviewed believed that migration could take 2-5 years to complete. They recognised that migration will be gradual, and that some companies in the sector won't be starting the migration in the next 5 years.
- EFFORT / SKILLS – Sector interviewees recognised that the effort required for PQC migration is substantial. Reasons were: (1) migration needs to happen in both hardware and software systems; (2) all teams (especially those building external-facing services that currently use asymmetric cryptography) will need to be involved; (3) the process requires significant collaboration across different regulatory bodies and delivery organisations; (4) updates need to be carried out progressively to address bugs and problems as they arise; and (5) the scale of the task depends on the number of certificates an organisation holds, with larger organisations facing a more daunting challenge.
- COST - The estimated cost of PQC migration was high but non-specific, with industry practitioners indicating that it could run into millions or even billions of pounds. One interviewee expressed concerns about managing larger key lengths (which will be required for PQC), and about the unknown impacts on protocols like TLS 1.3 and HTTP 3.0, which could lead to unexpected costs.
- BOARD AWARENESS – Interviewees did not explicitly mention the level of awareness within their Boards, but they have plans and roadmaps around PQC.

Transport sector interviewees

- MIGRATION DURATION – The shortest expected duration quoted was around 12 months. Some interviewees expected migration would take more than three years.

- EFFORT / SKILLS – Some transport sector interviewees felt that they would not need specialist skills beyond those they already had access to, so long as suppliers could provide equipment that is quantum-safe.
- COST – The view was that the lack of maturity in the PQC ecosystem means cost is still very much unknown.
- BOARD AWARENESS – Some organisations mentioned that articulating the challenge in an accessible way is difficult for such a complex problem.

Regulator interviewees

Most regulators we spoke with recognised that guidance and regulation are necessary to push PQC forward. However, one regulator is waiting to see what the market demands or what other regulators in their sector do.

Academic interviewees

Academic interviewees believed that industry is under-estimating the amount of time that migration will take. There was variance between interviewees on which sectors should be early adopters and which would benefit from a fast-follower model. Sectors discussed included finance, telecoms, public sector, energy, and healthcare.

3.1.2.7 Awareness of PQC resources and current sources of PQC advice (Q11+Q12)

Based on the interviews, industry practitioners are mainly taking PQC guidance from NCSC, NIST or CISA. Some interviewees mentioned following the CAF (framework provided by NIST), and the guidance provided by their sector regulators. Interviewees also mentioned standards organisations like ANSI (American National Standards Institute) or ETSI (European Telecommunications Standards Institute). Other sources mentioned included specific industry forums, e.g., the Certification Authority Browser Forum, and UKRI.

Another commonly-used source of information was engagement with experts - generally supply chain vendors (hardware and software) or consultants - to stay informed of developments on the PQC end. Specific companies mentioned included Google and IBM. Some interviewees also engage with academia on quantum and PQC.

Regulatory bodies are a primary source of guidance for organisations navigating PQC migration and are actively engaged in promoting resources, forums and partnerships, as noted above. However, some interviewees commented that the lack of a single, comprehensive regulatory framework makes it difficult for organisations to align with best practices.

Implications: *Industry is looking to regulators and government-backed industry bodies – particularly those involved in cybersecurity - to help inform their understanding of PQC and to provide guidance. In particular, NCSC and NIST are cited as sources of guidance by nearly all interviewees. However there are a number of other channels that can also be usefully engaged to improve understanding of PQC and migration approaches, and to reach industry end users. These should be considered in the mix, both as sources of information, and when amplifying and designing PQC communications programmes.*

Energy sector interviewees

Energy players reported that they take guidance from various sources, including external consultants, NCSC, and DSIT (reported by regulator).

- NCSC (CAF assessment framework), NIST, CNSA 2.0: General information
- NCSC: General industry compliance guidance
- Ofgem: Sector regulatory compliance guidance
- Cloud Service Providers: Cloud vendor guidance
- Supply Chain: Supply chain vendor guidance

The energy sector regulator we spoke to indicated they are part of quantum working groups together with some of the above organisations.

Finance sector interviewees

Finance interviewees were aware of, or used guidance from:

- NIST
- NCSC
- The Post Quantum Financial Forum
- Regulators
- Academia
- Consultancies – Note that one interviewee stated guidance would not be sought from classic consultancies, but instead from quantum or cyber experts.

Types of information sources consulted included government publications, white papers, and working groups and forums

Healthcare Sector interviewees:

Healthcare sector interviewees noted that guidance is currently scarce. One interviewee commented that government is offering some guidance, but industry practitioners were not aware of anything relevant from regulators. Some are taking a proactive approach and engaging with relevant tech vendors / supply chains (e.g. IBM, Google) and public organisations. For healthcare interviewees, sources of PQC information included:

- NCSC guidance and NIST algorithms, which are widely known.
- Connections with experts or other people interested in PQC, e.g., US investors, major tech vendors such as IBM or Google.
- An additional resource is the peer-network called the Cyber Associates Network (run by NHS Futures, specifically for the healthcare sector).

Telecoms sector interviewees

Telecoms industry practitioners reported that they collaborate with other vendors, regulatory and policy bodies, and standard organisations to jointly address the quantum threat. The regulator is keeping a watching brief, waiting for evidence of societal concern and parliamentary involvement before stepping in.

Interviewees in the telecoms sector reported taking guidance from:

- GCHQ/NCSC
- NIST
- ANSI
- ETSI
- CISA (the US equivalent to NCSC)
- TechUK

They were also actively engaged with:

- The Certification Authority Browser Forum (one interviewee is a certificate authority)
- Major tech companies (Google, IBM)
- the Digital Futures Institutes and quantum networks funded by UKRI, which involves major universities; e.g. Manchester, Edinburgh, Bristol, Cambridge, Southampton and Bath.

- They participate in the Digital Regulation Cooperation Forum with other regulatory bodies, focusing on digital platforms and awaiting evidence of a quantum use case to act.

The regulator reported that they monitor venture capital investments to gauge interest in quantum technologies, and rely on partners for guidance on using PQC tooling, deferring to the NCSC for mandating guidance before updating their policies.

Transport sector interviewees

Transport sector interviewees reported that a mix of government guidance, consultants and academic groups are helping their industry understand the depth of the problem.

All transport interviewees were familiar with NCSC guidance. Some expressed a desire for more accessible guidance for decision-makers.

Regulator interviewees

Regulators mentioned the following sources for PQC guidance:

- NCSC (UK) - Four of the five regulators we interviewed said they had ongoing engagement with NCSC on quantum matters. The fifth one is waiting for NCSC to publish guidance about quantum.
- CAF (Cyber Assessment Framework – issued by NCSC) – this is currently followed for any type of cyber security guidance, and which could also include PQC in the future.
- NIST (US)

Regulators are actively engaging and promoting different forums and partnerships with other regulators, universities or industry practitioners, although one noted that a quantum-focused partnership mixing these three groups does not yet exist. One of the regulators we spoke with is taking a more proactive stance; they believe that PQC will require collaboration from industry, academia and government, and are therefore establishing connections among the three and pushing for a globally aligned approach.

Academic interviewees

Academics noted that they could be a valuable source of technical leadership for organisations that need a deeper understanding of the problems presented by quantum and PQC.

- All academic interviewees were aware of NCSC as a source of advice.
- Academics also highlighted that there are now dedicated conferences looking at the topic of PQC, providing a forum for sharing detailed research.

3.1.3 Incentives and drivers for PQC migration

We asked interviewees the following question in regards to incentives and drivers:

- *What are the main factors driving your organisation to start planning for or executing on your PQC migration?*
- *In your opinion, what would be the most compelling reason or driver that would push your organisation to embark on a PQC migration?*

3.1.3.1 Incentives and drivers for organisations to start PQC migration (Q13)

Interviewees identified several main drivers that would push them (or already had pushed them) to take action on PQC migration. The first was the need to manage long-term assets; specifically, to prepare for future risks to the security and safety of such assets (especially in the energy sector and transport sectors). Second was the ability to create a cost/benefit case for PQC migration, which is needed to ensure that spend can be justified, and to highlight the economic benefits of migration. Third, regulation and standards are critical drivers, with NIST's standardisation and push on quantum security mentioned by many interviewees.

Most regulators we interviewed recognised that guidance and regulation are necessary to push PQC forward. However, not all are taking a pro-active approach. One regulator explicitly said they are waiting to see what the market demands, or what other regulators in their sector will do. Industry end users also commented on the role of regulation as a driver: one respondent pointed out that regulation often struggles to keep up with fast-paced technology development, while another highlighted the importance of developing regulation in conjunction with industry, to ensure that recommendations and expectations were feasible.

Implications: *Regulators and government have a critical role to play in helping to make sure the right incentives and drivers are in place to drive PQC migration forward. This includes not just working specifically on standards development and regulatory incentives, but also advising on strategies in regard to long-term assets, providing relevant inputs and evidence for business case development.*

Energy sector interviewees

Main drivers for PQC migration planning for the energy sector interviewees were:

- Long asset lifecycles are forcing a more strategic and long-term approach to PQC.
- NIST's drive for PQC is acting as a catalyst for planning.
- Access to funding [for cyber security investment] is easier for regulated businesses to access (e.g. via government innovation funding), if they can build a solid business case.

Finance sector interviewees

For finance sector interviewees, the main driver reported was concern over the threat of quantum computers generally.

Healthcare sector interviewees

Healthcare sector interviewees reported that their main drivers for PQC planning were:

- A need to ensure secure handling of human data.
- PQC being part of the strategic roadmap of their organisation.

Telecoms sector interviewees

Telecoms sector interviewees reported the following as drivers for starting planning for PQC migration:

- The need to build a sound understanding of the quantum computing threats
- Demand from customers (for high levels of security)
- Regulatory compliance

- Business opportunity of selling quantum-safe equipment

The regulator is waiting to see where venture capitalists and the government invest (in quantum and PQC), before following a defined migration approach and developing capability to deliver the migration.

Transport sector interviewees

Transport sector interviewees saw a variety of different drivers:

- Several transport organisations we spoke to said they and others in the sector anticipated that system integrators and legislators will demand PQC migration (from their suppliers), and they are keen to be knowledgeable suppliers.
- One interviewee said drivers were linked to their organisational goals: ensuring customer trust and IP protection.
- However, one transport interviewee stated that they will wait until a quantum computer becomes operational to worry.

Regulator interviewees

Regulators highlighted that legislation from government is likely to be the strongest driver for PQC migration.

- Building a business case for PQC migration was also viewed as essential to keep pushing things forward. One regulator shared that if the business case focused on the economic impact of *not* adopting PQC (e.g. IP theft, critical data hitting a GDPR stamp), it would make migration compelling enough for companies to invest in.

Academic interviewees

Academic interviewees noted that:

- Sectors that have already started to migrate have been driven by legislation in other countries.
- However, some organisations do understand the privacy and confidentiality challenges that they will face, if they do not act today.

3.1.4 Challenges and blockers for PQC migration

We asked several interview questions relevant for understanding barriers to PQC migration:

- *What barriers would make building an inventory of cryptography challenging for your organisation?*
- *What barriers are currently preventing or slowing down planning for or migration to PQC for your organisation? [overall, technical, non-technical]*

3.1.4.1 Barriers to undertaking a cryptographic inventory (Q14)

While some interviewees were already in the process of completing a cryptographic inventory – which is an important early step in the PQC migration journey - many identified barriers to completing this type of assessment of what types of cryptography were being used (and where) across their organisations. The most commonly mentioned barrier was the difficulty of evaluating cryptography in use due to limited visibility of third part/supply vendors' cryptographic approaches. The presence of legacy systems and the complexity and diversity of systems in use were also cited as issues by many interviewees. Other comments focused on the uncertainty of the cost or the risk level, and the need for significant 'manual' support and expertise to undertake the inventory.

Implications: *Creating a cryptographic inventory is a key part of the PQC migration journey, and it is clear that many organisations are finding this challenging. Support in this area – potentially in partnership with providers of tools that help to build such inventories (though these are rarely able to fully accomplish the task as noted by one interviewee) – and help in planning and costing the exercise could be valuable ways for government to help CNI organisations take this initial step. The fact that the NCSC has now put a timeline on the requirement for CNI organisations to identify vulnerable assets should act as a driver, but support will be needed by many organisations if they are to meet this deadline.*

Energy sector interviewees

Energy sector interviewees cited a lack of buy-in from leadership across energy sector as an issue for progressing with cryptographic inventories.

- This is linked to the difficulty of articulating risk assessment to the board, and of translating the commercial impact.
- Boards are reluctant to release funds due to the lack of immediacy of the need for an inventory (to support PQC readiness), given the availability of a cryptographically relevant quantum computer is further down the line.
- The presence of third-party software supply chains (e.g. cloud services) makes doing an inventory challenging. It is very difficult to fully test everything that is going on (e.g. automated discovery, put controls in place) because different suppliers are running those systems.
- One interviewee commented that the approach should focus on sensitive assets first, and use NIST guidance.

Finance sector interviewees

Interviewees in the finance sector cited a number of challenges in undertaking cryptographic inventories, including:

- Significant manual effort is required, due to the large and complex systems in place.
- The presence of legacy systems adds complexity to the inventory process, as these systems may use outdated or varied cryptographic methods.
- Financial sector organisations often use a variety of systems and programming languages, making it challenging to create a comprehensive inventory.
- Large organisations in the sector (e.g. banks) typically have large estates with compartmentalised systems that limit the deployment of enterprise discovery tools, hindering the inventory process.
- There is the additional complication of acquisitions and mergers in the sector leading to complicated IT estates (from combining different organisations)

Healthcare sector interviewees

Healthcare sector interviewees did not comment extensively on cryptographic inventory challenges, however one point cited was the lack of awareness of cyber security schemes used by vendors (supply chain).

Telecoms sector interviewees

Telecoms sector interviewees cited the following challenges related to cryptographic inventories:

- Lack of visibility of what cryptography suppliers (supply chain vendors) provide is an issue.
- Discovery of certificates is a significant barrier, and scans (e.g., using commercially available tools) are limited by network topology. There is not a single solution that provides complete visibility of the certificates being used
- Legacy systems also add to the complexity of completing a cryptographic inventory.

Transport sector interviewees

Transport sector interviewees did not comment extensively on this topic, but one industry practitioner noted that security controls make it difficult to create a cryptographic inventory, since they render it more difficult to "see" what's on the network.

Regulator interviewees

While regulators did not comment extensively on this topic, several acknowledged the complexity of creating an inventory.

- The finance regulator noted that companies in the finance sector may have complex IT set-ups, due to mergers and acquisitions.

Academic interviewees

One comment from academic interviewees was that multinational companies may find that cryptographic inventories are particularly complex, due to the different requirements in different countries making the management of cryptographic assets/material more difficult.

3.1.4.2 Barriers preventing or slowing down organisations' planning or journey, for PQC migration (Q15)

Across sectors, key technical barriers to PQC migration planning and execution that interviewees identified included (1) presence of legacy systems which could be difficult or impossible to upgrade for PQC; (2) complexity of systems and limited visibility of these, which make migration planning complex as well; and (3) heavy dependence on third parties/supply chain for cybersecurity.

Non-technical barriers they identified included (4) skills gaps/technical expertise shortages; (5) uncertainty around PQC timelines; and (6) concerns about supply chain readiness. A further barrier mentioned by interviewees from most sectors was (7) the need to find better and clearer ways to communicate timelines, value and urgency of PQC migration to Boards and senior stakeholders. Barriers cited were generally consistent across sectors.

Implications: *The clear alignment across sectors on key barriers to PQC migration highlights the need for coordinated action and targeted support to address the specific pain points cited by interviewees. Some of the barriers are more readily addressable by government or regulator intervention than others (for example, supply chain vendors will be key stakeholders and could take a leading role is some aspects of developing guidance to industry). Guidance will be most effective if it pre-emptively addresses the barriers identified here.*

Energy sector interviewees

Technical barriers identified by energy sector interviewees were:

- Embedded devices have fewer computational resources (which may make applying different/more complex cryptography difficult). Some legacy systems use proprietary cryptography, because standard algorithms require more resources than are available on the devices.
- Remediation of infrastructure will require clear understanding and planning as pre-requisites to initiating a change to the underlying ciphers, in order to plan for additional costs that must be considered, such as testing, PoCs, planning, budgeting, and business case development.
- OT is an element of concern as well as IT because:
  - OT will require significant amounts of testing.
  - Some devices won't be able to support these ciphers.
  - There will be a bandwidth impact of using cryptography with bigger signatures.

Non-technical barriers identified by energy sector interviewees were:

- Energy sector players struggle to identify common problems, and to solve them effectively from a central group or point. There is a risk of various parties approaching the problem in different, uncoordinated ways.
- The sector is used to following required policy and guidance in setting out cyber security strategy, but is not generally proactive in seeking out expertise in novel areas of cyber security from academia, government and consultants.
- Expertise is limited to small pockets of specialists, so the industry is not ready to engage the supply chain on this issue.
- There is significant dependence on the supply chain for cyber security.
- Complexity across the sector is an issue.
- Knowledge and skills shortages.
- Risk of poor articulation of issues to the Board, and not getting buy-in.
- Impacts need to be carefully gauged and expressed clearly, in order to communicate them to senior audiences in a manner that will generate board action.
- The biggest concern is that investing now to remediate 40 years of Diffie-Helman (a type of key exchange widely used to securely generate and exchange symmetric cryptographic keys over a public channel, which will be vulnerable to quantum attacks) could still be insufficient to defend assets for the future, as quantum capabilities evolve. In other words, remediation undertaken now cannot guarantee that the new Federal Information Processing Standards (FIPS) algorithms deployed to mitigate against quantum now will be invulnerable to future attacks. For example, an attack could happen again in a relatively short timeframe even post-mitigation, so the cyber team could end up needing to argue a case for re-expending budget (that is already scarce) on more mitigations.

Finance sector interviewees

Technical barriers identified by finance sector interviewees were:

- Complexity due to legacy systems and the need to support various customer requirements and constraints.
- Legacy source codes, and a variety of systems and programming languages adding to the challenge.
- Dependence on vendors (supply chain) to provide updated technology that supports PQC.

- Technology from vendors not yet available to support migration.
- Large numbers of ring-fenced systems executing downstream tasks in this sector.
- Implementing necessary upgrades to mainframes will be challenging.

Non-technical barriers identified by finance sector interviewees were:

- Challenge of securing support from non-technical stakeholders and effectively communicating the importance of PQC migration.
- Lack of board buy-in: quantum computers are not a pressing threat.
- Existence of more pressing and imminent cyber security threats that may take priority over PQC migration.
- Lack of trained cryptography experts to support the migration process.
- Significant financial investment required to upgrade systems and processes for PQC.
- Need for clear regulatory guidelines and support to drive the migration.

Healthcare sector interviewees

Technical barriers identified by healthcare sector interviewees were:

- Migration must occur at approximately the same time throughout the whole supply chain.
- Dependency on vendors to provide quantum-safe technology .
- Supply chain / vendors not working on the migration themselves.
- Lack of appropriate resources and skills: good system architects will be needed in case of a "plug and play" migration.
- Complexity of cryptographic key management.
- Transitioning while maintaining ongoing operations.

Non-technical barriers identified by healthcare sector interviewees were:

- Lack of business buy-in (board and employees).
- Lack of business awareness about the importance of PQC migration.
- Lack of funding.
- Regulatory divergence (differences among countries, sectors).

Telecoms sector interviewees

Technical barriers identified by telecoms sector interviewees were:

- Software doesn't come with a "bill of materials" so it's difficult (or even impossible) to know what's inside (from a cryptography and functionality point of view).
- Most certificate authorities can issue post-quantum certificates for software today, but these cannot be read because the software houses have not developed post-quantum libraries (identified as an issue by a Certificate Authority we interviewed).
- Legacy hardware, such as electricity meters and IoT devices, will be challenging to upgrade for the post-quantum era.
- Technical problems could arise throughout the migration process, and there is limited ability to manage these.

Non-technical barriers identified by telecoms sector interviewees were:

- There is a general lack of impetus to act quickly around the quantum security threat.
- The skills gap – although opinions were divided on this. One interviewee believed that PQC migration requires enterprise architecture and security skills, both of which are already in short supply, while another interviewee did not consider it a major problem.

- Culture barriers – It is difficult to motivate people (employees and supply chain) to act to mitigate a high risk that may or may not materialise.
- End users don't realise the link between quantum and certificates which are used in any communication between devices (laptops, TVs, mobile phones, VR headsets, etc.) – there are going to be significant challenges regarding quantum threats to data integrity and security of identity.
- Last-minute political decisions (e.g. removing Huawei as a supplier).
- Lack of standardisation: there is a need for more regular updates and guidance from telecoms companies, Ofcom, and other UK regulatory bodies to establish clear standards.

Transport sector interviewees

Technical barriers identified by transport sector interviewees were:

- There is a lack of clarity about when specific systems will be vulnerable.
- There are still few vendors offering quantum-safe equipment.
- Legacy systems will require careful assessment to migrate, and not all will support PQC, so organisations will need to explore alternative approaches.

Non-technical barriers identified by transport sector interviewees were:

- Deploying cryptography correctly requires staff to upskill.
- Many decision-makers are struggling to understand the challenge and how much to invest.
- Building convincing business cases based around risk reduction rather than cost reduction is an ongoing security challenge.
- Some suppliers are unaware that the problem exists at all.

Regulator interviewees

Technical barriers identified by regulator interviewees were:

- Dependence on research results from hyperscalers (e.g. Google, Microsoft, Apple, Meta, etc.).
- Legacy systems - which will be difficult to upgrade for PQC.

Non-technical barriers identified by regulator interviewees were:

- Lack of relevant cryptography knowledge among people working in cyber security.
- Skills gap: Lack of in-house capability to move the migration forward.
- Lack of board buy-in; board members are going to consider risk v cost to decide.
- Cultural barriers: people may struggle to incorporate new ways of thinking.
- Cost: the larger the organisation, the higher the cost to migrate the entire IT estate.
- Limited funding to accomplish all relevant transformation projects.
- Lack of clear timelines.

Academic interviewees

Technical barriers identified by academic interviewees were:

- Technical risks introduced by taking action to migrate. Some organisations will want to be fast-followers, and are waiting to see what others do first.
- Legacy equipment – which will be difficult to upgrade for PQC.

Non-technical barriers identified by academic interviewees were:

- Costs of replacing software and equipment.
- Skills gap: There are very few people skilled enough to reliably implement and deploy cryptography.

3.1.5 Government measures to support organisations with PQC migration

We asked interviewees the following questions, in regards to what forms of regulatory or governmental support would be most beneficial:

- *What would be most helpful from regulators or government, to encourage, enable or support your organisation in preparing for the transition to PQC?*

3.1.5.1 Support or interventions from government and regulators to help organisations prepare for the PQC transition (Q16)

Government support was seen as crucial for driving PQC adoption across CNI, with regulators, academia, and industry stakeholders calling for clearer guidance, structured transition plans, and regulatory engagement. The energy, finance, healthcare, telecoms, and transport sectors all called for clear government guidance, structured transition plans, and regulatory engagement, but their priorities differ - finance focuses on enforcement, healthcare on vendor collaboration and SME support, and telecoms on collaboration for standardisation.

Regulators we spoke to stressed the need for a coordinated, government-led approach to PQC regulation, while academics we interviewed highlighted the importance of NCSC guidance, industry knowledge sharing, and assurance standards to accelerate adoption.

Regulators emphasised the need for a coordinated, consistent approach to PQC regulation, ensuring guidance is aligned where possible while allowing for necessary sector-specific differences.

Implications:*. A clear directive from central government and NCSC would help justify resource allocation, as the current uncertainty means more immediate challenges often take priority over PQC migration planning. Regulators can also help organisations within their industries by facilitating collaboration via working groups or peer support. They can also increase awareness using "stakeholder's language" which will help with building a business case to unlock funding. Guidance on the level of assurance that should be achieved by PQC implementations could accelerate adoption of trusted vendors. If government facilitated knowledge sharing between academia and industry, this could help ensure that the C-suite has a realistic view of the risk, without causing unnecessary panic.*

Energy sector interviewees

Energy sector

- PQC readiness planning requires policies to be driven by the government and regulators. If there is a government-imposed obligation to start planning, then it's easier to enable a set of actions and next steps.
- PQC readiness planning requires further advice and clarification of risks and issues from government bodies such as DSIT; e.g. further advice is needed on challenging issues such as replacing encryption on power stations that can't be switched off, and challenges with the supply chain.
- Guidance should highlight the actions needed from big Tier 1 technology suppliers (e.g., Google, Microsoft, IBM).
- Reassurance and engagement with individual businesses are needed, to assure organisations that they don't need to worry.
- Industry needs to conduct analysis to offer more specific guidance to businesses (what they need to do about the quantum threat, and most importantly what *not* to do).
- There is a need for greater visibility of intelligence and more knowledge sharing. What is missing is an industry centre of excellence or similar – something that would bring all the right knowledge together across all industry sectors, and enable knowledge and guidance to be leveraged from any industry, in an industry-agnostic way. This is essential as an enabler at the first level; such a group

could give industry sector stakeholders high-level guidance, directing what activities need to be focused on.

Finance sector interviewees

Interviewees in the finance sector said there is a need for more proactive communication and support on PQC from government.

- Interviewees would strongly encourage government to place more focus on everything related to PQC, including providing risk scoring, timelines, and penalties if deadlines are missed.
- They also suggested setting up a centrally coordinated function across the industry to provide PQC guidance, in order to reduce the individual burden on organisations.
- Finance interviewees also recommended the creation of a cyber advisory board involving government, academia, and industry, to enable knowledge sharing and technology advancement.
- They suggested that government mandate that vendors warrant their software as quantum-safe. Related to this, vendor liability is seen as crucial, to ensure the quality and security of cryptographic solutions.

Healthcare sector interviewees

Healthcare sector organisations we interviewed suggested that more guidance on what to do in regards to PQC migration, and when, is needed for businesses. This should be written using business language, so that it is easier for boards to understand.

- Pressure and/or work with foundational technology vendors like hyperscalers and telecoms, because the healthcare industry will just be an end-consumer of the quantum-safe technology that those companies produce
- Provide support for SMEs, since they have fewer human resources to innovate in PQC
- They also suggested that government needs to fund more PQC research, if the UK wants to be a leader.

Telecoms sector interviewees

Telecoms industry practitioners we interviewed are working closely with - and discussing PQC guidance with, the following groups:

- Regulatory bodies: NCSC, NIST
- Standards organisations
- Technology vendors.

Transport sector interviewees

Transport sector organisations we interviewed had the following suggestions:

- One interviewee felt transport organisations would welcome PQC-related regulation, since it would introduce certainty. But they felt it was important that industry was engaged in developing regulations, to ensure that regulation was practical and achievable.
- Another interviewee noted that there are many small-to-medium organisations in this sector that may not have access to cryptography specialists and will require clear guidance that meets their needs.

Regulator interviewees

Regulators we interviewed identified the following areas where they could potentially offer help, as a regulator (note – these are suggestions and are not necessarily being offered today)

- Establishing working groups

- Helping to build business cases for PQC migration that unlock funding
- Running a “proof-of-concept” to have a baseline to regulate from
- Coordinating industry efforts centrally
- Creating awareness campaigns using “stakeholders’ language”
- Encouraging of peer-support models.

Regulators also had suggestions on areas where they themselves are looking for help from government:

- Guidance on PQC migration best practice (e.g. by creating case studies/blueprints)
- Regular sessions for upskilling regulators and policymakers on the implications of quantum computers and PQC migration
- Collaboration with regulators to create appropriate guidance for specific sectors
- Facilitating engagement between academia, industry and regulators, maybe by creating an action group
- Creating an industry standards body for the migration
- Strategic engagement with critical suppliers (e.g. software vendors)
- Considering future funding and review spending, acknowledging the significant work that a PQC migration requires
- Providing further advice and promoting awareness of the need for migrating to PQC, especially on ways to manage challenging issues (e.g. supply chain)

Academic interviewees

Academic interviewees highlighted the importance of NCSC guidance and the role of academia in providing up-to-date analyses on PQC research. They emphasised the need for government-facilitated knowledge sharing, to ensure industry leaders get a realistic grasp of the risks without causing unnecessary alarm.

Additionally, the UK has had no Common Criteria certifying body since 2019, when the NCSC chose to stop offering that service. This was noted as a gap, with calls for clear assurance guidelines to help PQC vendors demonstrate that their products are adequately secure.

4. Online survey analysis

This section provides details on online survey responses gathered in support of this study. It is structured as follows:

- Context for PQC readiness: Organisations' cyber security goals, maturity and outsourcing strategy (Section 4.1.1)
- Understanding of PQC and expectations for migration (Section 4.1.2)
- Incentives and drivers for PQC migration (Section 4.1.3)
- Challenges and blockers for PQC migration (Section 4.1.4)
- Government measures to support organisations with PQC migration (Section 4.1.5)

This section presents findings from the online survey in detail, and an analysis of responses by sector. Methodological details on how we executed and analysed the survey can be found in Section 2.1.

4.1 Survey outcomes

4.1.1 Cyber security goals, maturity and outsourcing Strategy

To set the scene and provide context for questions on PQC awareness and readiness, the survey included a series of questions on organisations' cyber security goals and maturity. Overall, respondents had clear views on their organisations' cyber security goals, and a reasonable understanding of their organisations' cyber security policies and strategies. We also asked about in-house vs outsourced approaches to cyber security planning and strategy, and ongoing security management.

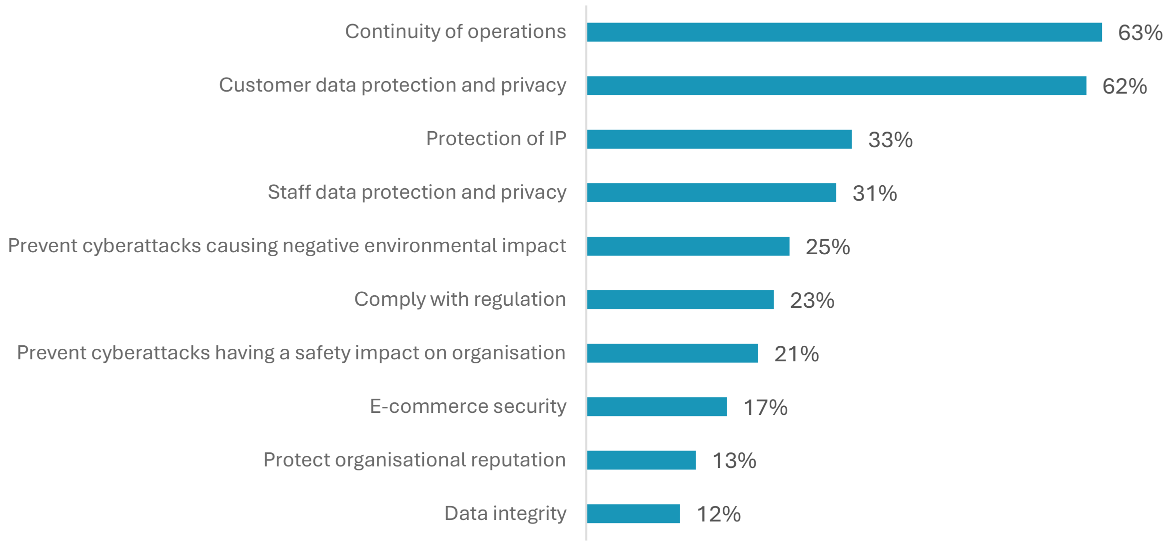
Key takeaways:

- The top goals of ensuring continuity of operations and customer data protection and privacy should be kept front of mind when devising PQC migration support programmes.
- Cryptographic maturity among respondents' organisations varies somewhat by sector. While energy and finance were more mature overall, based on our indicative assessment, even those sectors have gaps in their understanding of their organisations cryptographic estates and strategies. The implication is that some baseline guidance on the key foundations of cyber security and cryptography best practice will be needed, before pushing organisations to start a PQC migration process. For example, a lack of up-to-date cryptographic inventories could make the PQC migration process ineffective or result in incorrect prioritisation of assets. Some organisations rely on software vulnerability monitors to flag when cryptographic functions require upgrading. This reactive strategy is less effective than strategically managing the quantum risk but is a route to driving organisations away from vulnerable cryptography. This relies on a CVE (common vulnerabilities and exposures) report about quantum vulnerability of a specific algorithm being submitted and accepted to the National Vulnerability Database, which is only likely once a real-world exploit has been recorded.
- Approaches to cyber security planning and strategy varied significantly by sector, and also by size of organisation. Most organisations prefer to manage this activity in-house, although there was significant variation by sector. Finance, telecoms and transport respondents were significantly more likely to report that they keep strategy and planning entirely in-house, while energy and healthcare respondents were more likely to partially or completely outsource. For ongoing cyber security upgrades and management, most respondents reported partially outsourcing this activity, although significant minorities of telecoms (25%), healthcare (18%), energy (17%) and finance (17%) respondents keep this fully in-house. The clear sectoral differences in strategies for outsourcing cyber security must be taken into account when developing PQC migration incentives and support, to make sure they are appropriately targeted.

- Smaller organisations were significantly more likely to partially or fully outsource both cyber security planning and ongoing management, likely reflecting the limited capacity of in-house cyber teams. Organisations of 5000+ employees were more likely than their smaller peers to keep things entirely in-house. This implies that different strategies should be developed to reach SMEs and large organisations for PQC migration support, with suppliers of IT services being significantly more important for the former SMEs.

4.1.1.1 Organisations' cyber security goals

Figure 4.1. Main cyber security goals for organisations, top 3 (share of respondents)



Note: n = 52 survey respondents. Respondents were asked to select their organisation's main cyber security goals. % shows share of respondents who chose the option as one of their top 3.

The top priorities for cyber security across all respondents were continuity of operations (selected by 63% of respondents) and customer data protection (62% of respondents), highlighting a strong focus on ensuring business resilience and safeguarding sensitive customer information.

Protection of intellectual property (33%) and staff data (31%) were important but secondary concerns, reflecting the importance of internal security alongside external threats.

Interestingly, the goals relating specifically to preventing cyber attacks—both environmental (25%) and customer-targeted (21%)—ranked relatively low, as did regulatory compliance (23%).

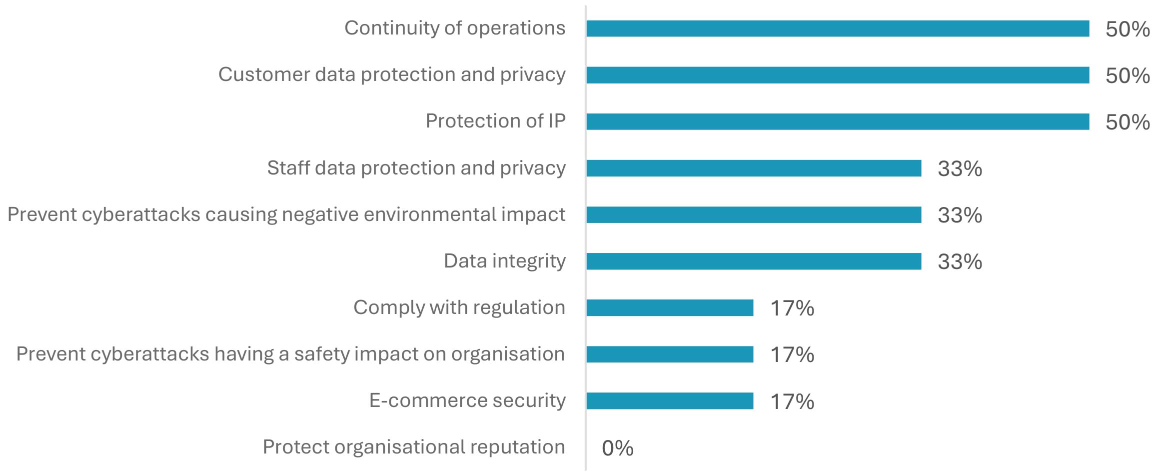
E-commerce security (17%), organisational reputation (14%), and data integrity (12%) ranked lowest, indicating that whilst important, these factors were not the primary motivators for PQC adoption.

Sector analysis

Energy sector

In the energy sector, maintaining continuity of operations, ensuring data protection and privacy for customers, and protecting intellectual property were equally prioritised, with 50% of respondents selecting each of these for the top 3 goals. This indicates that organisations in this sector view cyber security as a balance between ensuring uninterrupted service delivery in the face of evolving cyber threats, safeguarding critical infrastructure, and protecting sensitive data.

Figure 4.2. Main cyber security goals for organisations in the energy sector, top 3 (share of respondents)

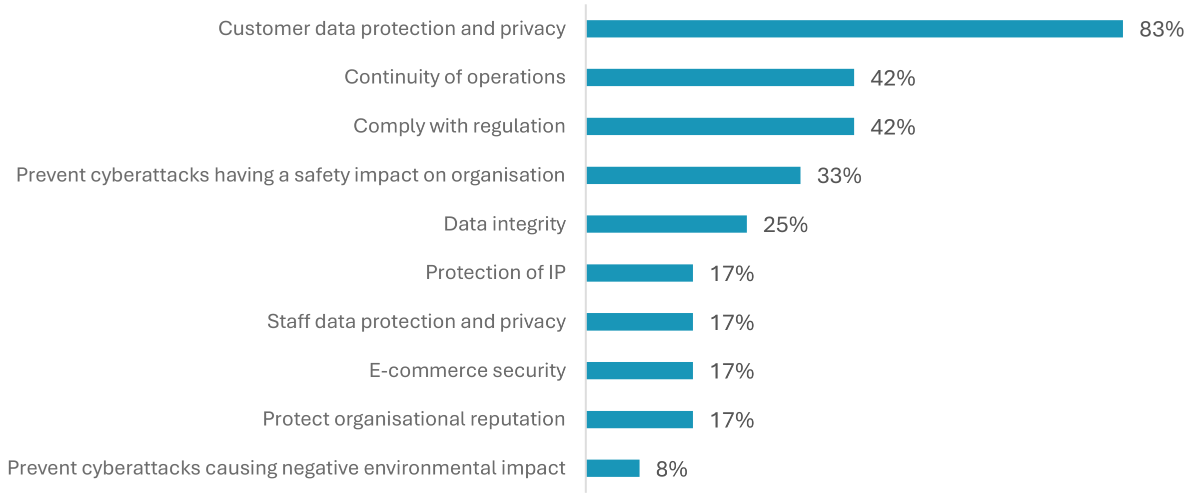


Note: n = 6 respondents. Respondents were asked to select the top 3 goals. The percentages represent the proportion of respondents who selected each option as one of their top 3 goals.

Finance sector

In the finance sector, ensuring data protection and privacy for customers was the top cyber security priority (83%), reflecting the industry's strong focus on safeguarding sensitive financial information. Ensuring continuity of operations and complying with regulations were equally important (42%), indicating that financial institutions prioritise both business resilience and adherence to regulatory requirements to maintain trust and security in their operations.

Figure 4.3. Main cyber security goals for organisations in the finance sector, top 3 (share of respondents)

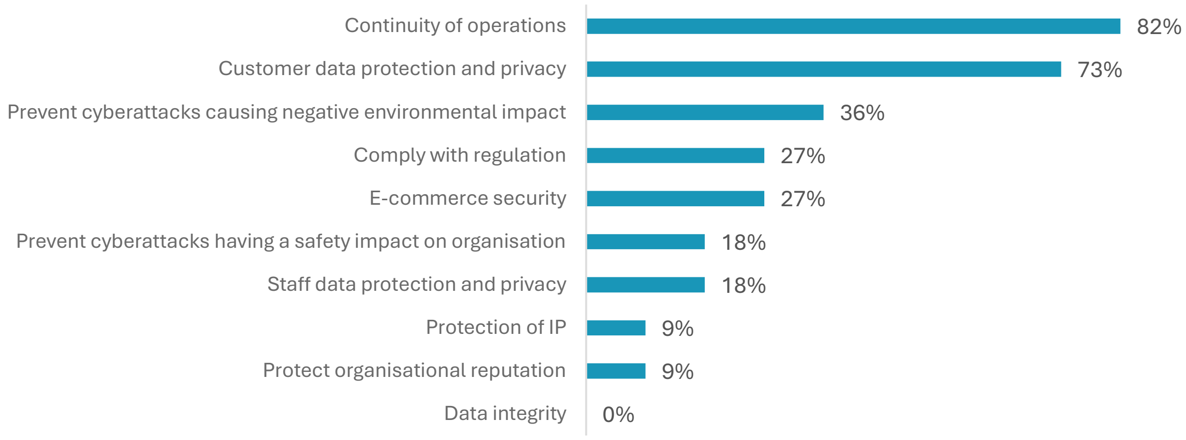


Note: n = 12 respondents. Respondents were asked to select the top 3 goals. The percentages represent the proportion of respondents who selected each option as one of their top 3 goals.

Healthcare sector

The top priority for healthcare sector survey respondents was ensuring continuity of operations, with 82% recognising the need to maintain business resilience during PQC migration. Data protection and customer privacy followed closely at 73%, highlighting the importance of patient safety and of securing sensitive information against emerging threats. Preventing cyber attacks from causing environmental harm was a lower priority at 36%, suggesting that, while acknowledged, it is not as immediate a concern as operational continuity and data security.

Figure 4.4. Main cyber security goals for organisations in the healthcare sector, top 3 (share of respondents)

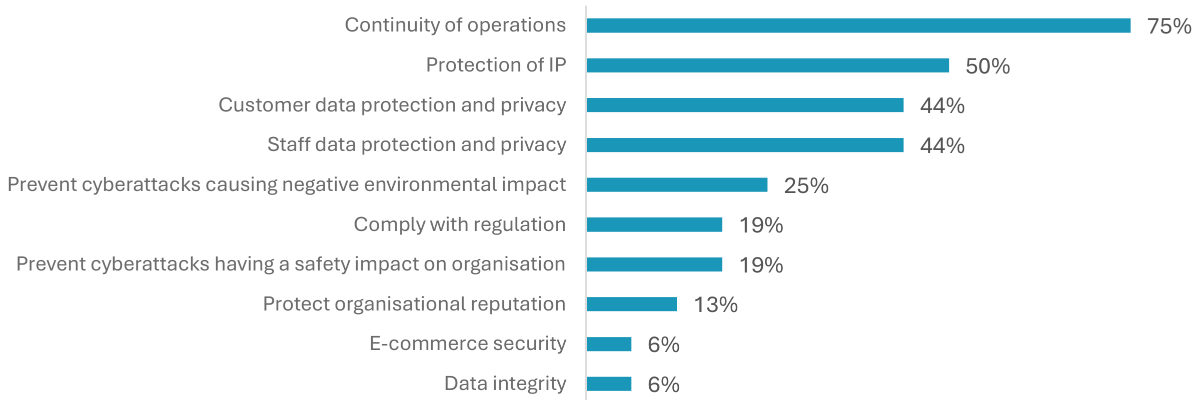


Note: n = 11 respondents. Respondents were asked to select the top 3 goals. The percentages represent the proportion of respondents who selected each option as one of their top 3 goals.

Telecoms sector

In the telecoms sector, ensuring continuity of operations was the top cyber security priority at 75%, reflecting the industry's focus on maintaining uninterrupted services. Protecting intellectual property followed at 50%, highlighting concerns over securing proprietary technologies and network infrastructure. Ensuring data protection and privacy for customers was also a key focus at 44%, indicating that while safeguarding user information is important, operational resilience and intellectual property security take precedence.

Figure 4.5 Main cyber security goals for organisations in the telecoms sector, top 3 (share of respondents)

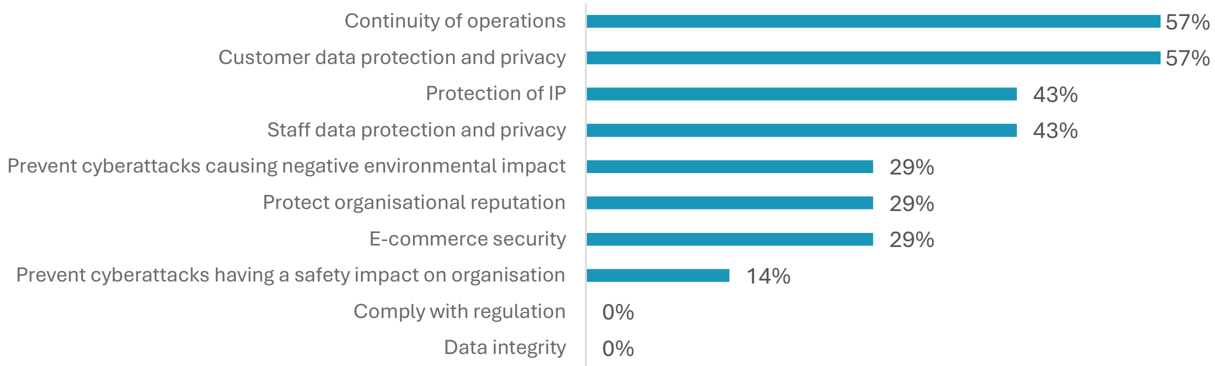


Note: n = 16 respondents. Respondents were asked to select the top 3 goals. The percentages represent the proportion of respondents who selected each option as one of their top 3 goals.

Transport sector

In the transport sector, the two main priorities at 57% were ensuring continuity of operations and ensuring data protection and privacy for customers. Transport companies were aware of the critical need to build trust with their customers by providing reliable services and protecting customers' personal data. Protecting intellectual property was also a key focus for 43%, reflecting the value of intellectual assets for transport companies and their commitment to protecting them to sustain growth and innovation.

Figure 4.6. Main cyber security goals for organisations in the transport sector, top 3 (share of respondents)



Note: n = 7 respondents. Respondents were asked to select the top 3 goals. The percentages represent the proportion of respondents who selected each option as one of their top 3 goals.

4.1.1.2 Cryptographic maturity

Survey respondents were asked to indicate their organisation's level of cryptographic maturity, based on their knowledge or awareness of the following statements:

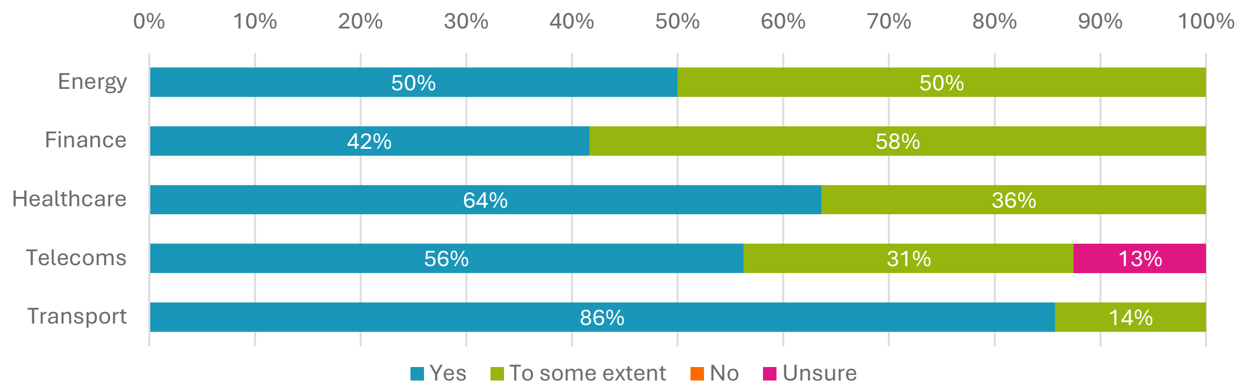
1. We know where our sensitive data is stored
2. We know how long our data needs to be stored and secured for
3. We have a mostly complete inventory of where our organisation uses cryptography
4. We have a team of internal staff with cryptographic skills
5. We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of "banned" algorithms that cannot be introduced
6. Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations
7. Our senior management understands how cryptography contributes to our organisational goals and business strategy

The aim of this question was to understand organisations' baseline preparedness to start planning for PQC migration. For example, the readiness of an organisation to respond to flaws in their cryptography is a good proxy for their overall capability of responding to security flaws that have evolved in their estate, and by extension their ability to plan for PQC migration effectively and proactively.

Overall, the picture for cryptographic maturity across sectors is mixed. The implication is that organisations (especially in sectors such as transport, telecoms and finance) could benefit from clear directions on the foundational steps for robust cryptographic management more generally, as an initial step towards PQC migration readiness.

Survey respondents across all CNI sectors fully knew or knew to some extent where their sensitive data is stored (see Figure 4.7). For example, 86% of respondents in the transport sector confirmed they have complete knowledge of where their sensitive data is stored. Healthcare (64%) and telecoms (56%) also showed strong awareness. Financial institutions (42%) and energy (50%) reported lower levels of certainty, with a higher percentage (58% and 50%, respectively) indicating only partial understanding. Notably, 13% of telecoms respondents were unsure of where their sensitive data is stored, suggesting that some organisations, particularly in these industries, may lack clear visibility over long-term data management practices.

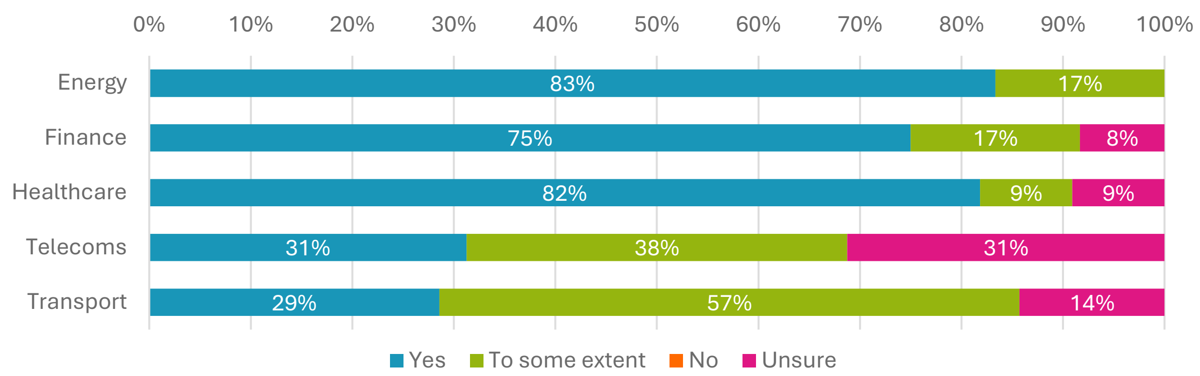
Figure 4.7. Cryptographic maturity statement 1: We know where our sensitive data is stored (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "We know where our sensitive data is stored".

Survey responses indicated that most sectors have a strong understanding of how long their data need to be stored for (see Figure 4.8), with 83% of energy companies, 82% of healthcare providers, and 75% of financial institutions confirming they are fully aware of their data retention policies. However, uncertainty was highest in the telecoms (31%) and transport (14%) sectors, suggesting that some organisations in this sector may lack clear policies or governance structures for long-term data retention. Additionally, a significant proportion of transport (57%) and telecoms (38%) respondents indicated only partial knowledge.

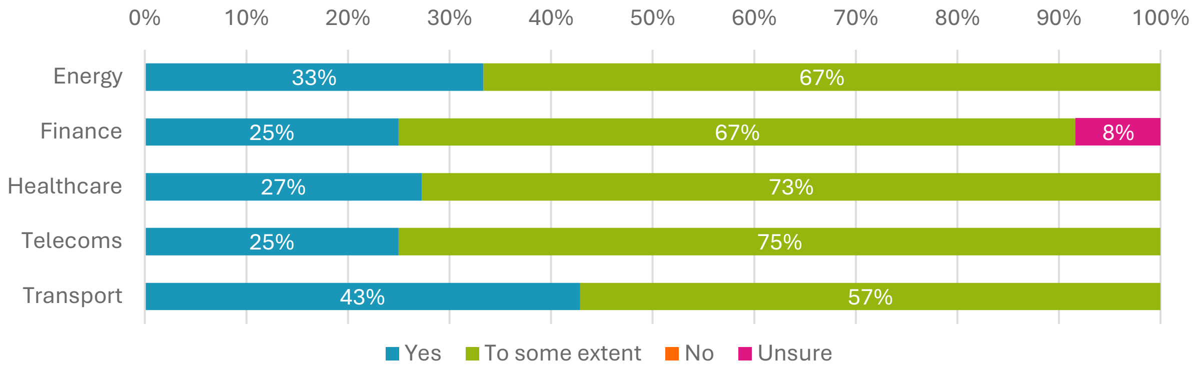
Figure 4.8. Cryptographic maturity statement 2: We know how long our data needs to be stored and secured for (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "We know how long our data needs to be stored and secured for".

Most respondents across all the sectors reported having completed their cryptographic inventory only 'to some extent' (see Figure 4.9). With telecoms (75%) and healthcare (73%) having the highest proportion of respondents choosing this answer. The transport sector seems to be the most advanced in cryptographic inventory, with 43% of its respondents confirming they have mostly completed it. The finance sector was the only one where respondents (8%) were unsure about the state of their cryptographic inventory. suggesting that some organisations in this sector may have very complex systems, limited resources or a lack of clear cryptographic policies.

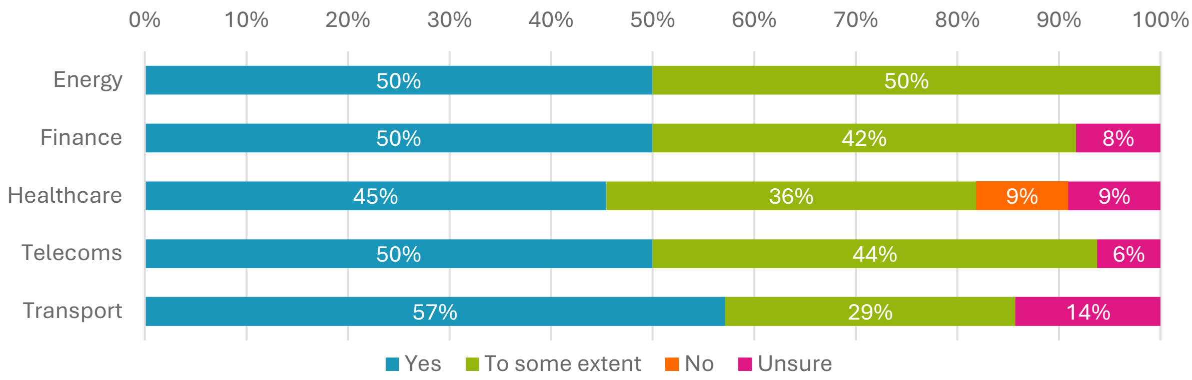
Figure 4.9. Cryptographic maturity statement 3: We have a mostly complete inventory of where our organisation uses cryptography (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "We have a mostly complete inventory of where our organisation uses cryptography".

Most organisations reported having internal staff with cryptographic skills at least 'to some extent' (see Figure 4.10). The energy sector showed a 50-50 split between 'yes' and 'to some extent', whilst other sectors expressed uncertainty about their internal skills. Interestingly, the transport sector had the highest percentage of respondents (57%) reporting having an internal team with cryptographic skills, but also the highest percentage expressing uncertainty (14%). The healthcare sector was the only one reporting organisations having a lack of internal staff with cryptographic skills (9%).

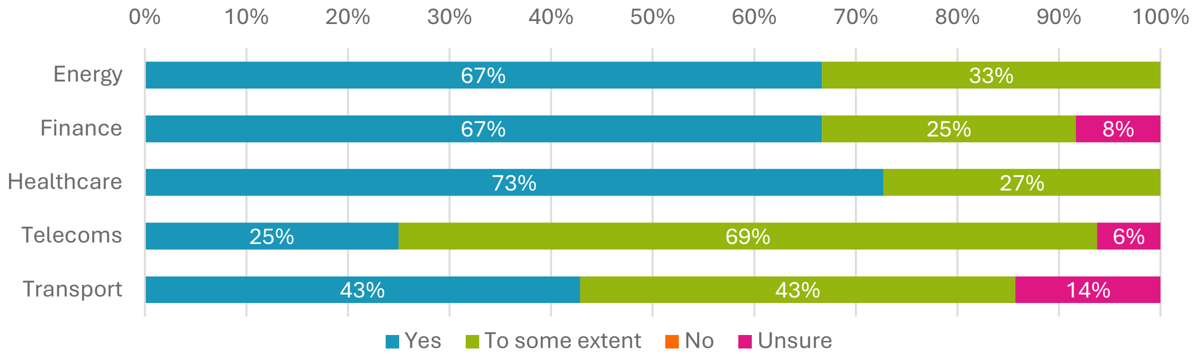
Figure 4.10. Cryptographic maturity statement 4: We have a team of internal staff with cryptographic skills (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "We have a team of internal staff with cryptographic skills".

We asked respondents whether assessing cryptographic libraries was a requirement as part of their process of managing software vulnerabilities (see Figure 4.11). Responses to this statement varied across sectors. Energy (67%) and financial institutions (67%) reported following the approach described in the statement. By contrast most telecoms respondents (69%) recognised following this approach to some extent. There was also some uncertainty in sectors like transport (14%), finance (8%) and telecoms (6%). None of the respondents reported not following the proposed approach at all, indicating a strong integration of cryptographic risks within their security frameworks.

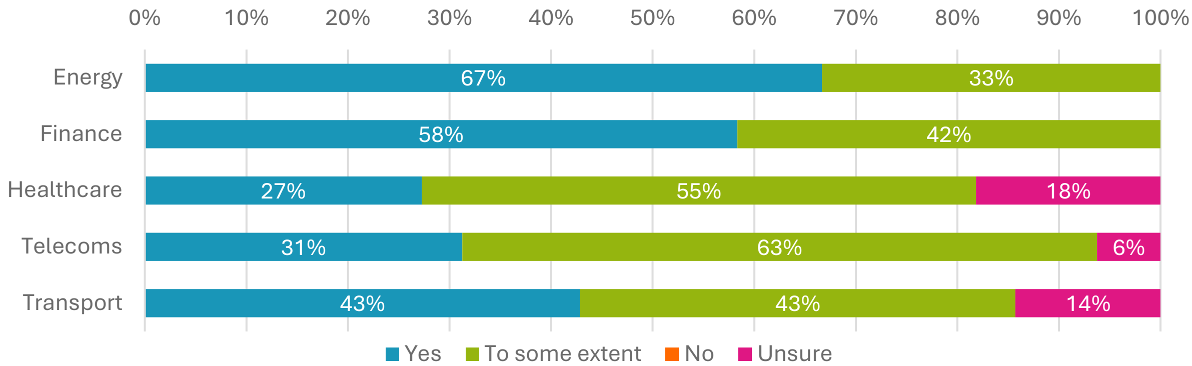
Figure 4.11. Cryptographic maturity statement 5: Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations".

We asked survey respondents whether they maintained a list of acceptable and banned cryptographic algorithms and most of them answered either 'yes' or 'to some extent' (see Figure 4.12). Organisations in the energy and finance sector seemed to rank higher in this cryptographic maturity statement, with most of their respondents reporting maintaining the list (67% for energy and 58% for finance) and the rest maintaining it to some extent. Meanwhile, the other three sectors seemed to show less maturity with this statement, with some organisations being uncertain about whether they maintained a list of algorithms or not (18% for healthcare, 14% for transport and 6% for telecoms) and high percentages of respondents doing it 'to some extent' (55% for healthcare, 43% for transport and 36% for telecoms). This suggests that while organisations recognise the importance of cryptographic governance, many do not have confidence that their organisations apply it thoroughly or consistently.

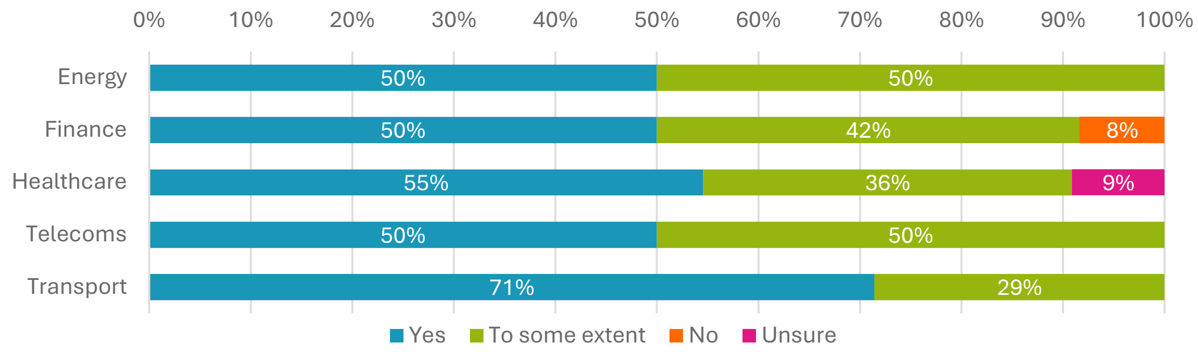
Figure 4.12. Cryptographic maturity statement 6: We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of 'banned' algorithms that cannot be introduced (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of 'banned' algorithms that cannot be introduced".

The last statement addressed the awareness of cryptography's contribution to organisational goals and business strategy among senior management (see Figure 4.13) Responses showed slight variations per sector. Transport sector respondents were most confident that their senior leadership understands the value of cryptography (71%). About half of the respondents in the healthcare (55%), finance (50%), telecoms (50%), and energy (50%) sectors, reported they are confident of senior management awareness, indicating a reasonable but not universal level of understanding. 8% of financial institutions indicated their senior management does not understand cryptography. This means that some leadership teams in this sector potentially lack the technical knowledge necessary for informed decision-making on cyber security strategies, which could then impact their willingness to invest in PQC readiness.

Figure 4.13. Cryptographic maturity statement 7: Our senior management understands how cryptography contributes to our organisational goals and business strategy (share of respondents per sector)

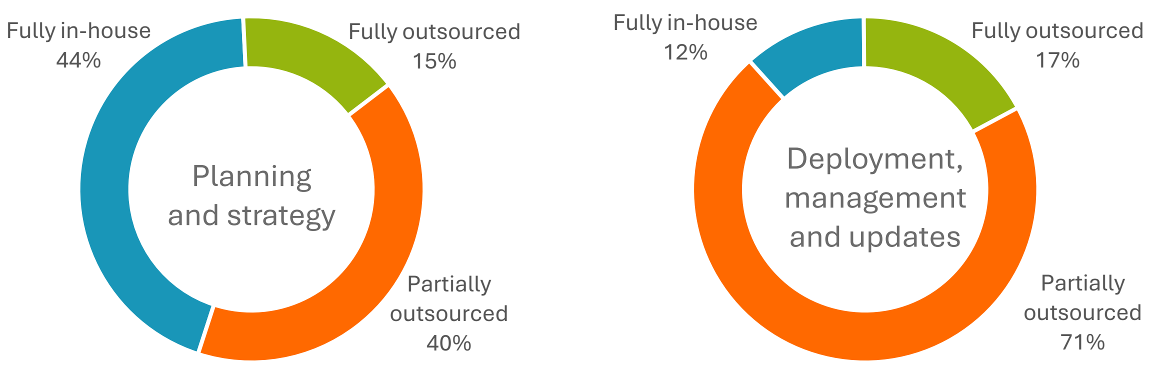


Note: n = 52 survey respondents. Respondents were asked to evaluate how the following statement reflects the reality in their organisations: "Our senior management understands how cryptography contributes to our organisational goals and business strategy".

4.1.1.3 Approaches to in-house vs outsourcing cyber security

We asked respondents to tell us whether their organisations took an (1) in-house-led approach to 'cyber security planning and strategy', and 'ongoing cyber security management and updates'; or (2) whether these activities were outsourced to third-party vendors (see Figure 4.14). We analysed trends by sector and by company size. The purpose of this question was to establish the extent to which organisations rely on third parties for cyber security. If the supply chain is critical for a particular sector, then the implication is that support for PQC migration and readiness needs to address that supply chain directly besides addressing the needs of end-user organisations.

Figure 4.14. Cyber security approach - in-house vs outsourced (share of respondents)



Note: n = 52 survey respondents. Respondents were asked to indicate who is responsible for different aspects of their cyber security approach.

Cyber security approach to planning and strategy

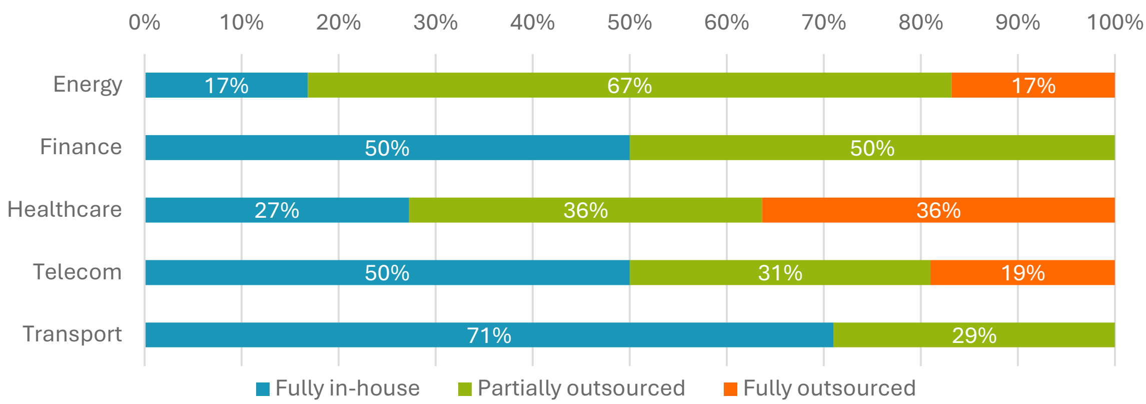
For cyber security planning and strategy, our survey responses indicated that the largest share of organisations prefer to manage this activity in-house, although there was significant variation by sector.

In total, just under half of respondents stated that their cyber security planning and strategy is fully handled by internal teams. Some sectors were significantly more likely to keep strategy and planning entirely in-house; notably finance (50%), telecoms (50%) and transport (71%) . By contrast, only 27% of healthcare respondents and 17% of energy respondents said their organisations kept cyber security planning and strategy fully in-house.

Partial outsourcing of planning and strategy for cyber security is also a popular approach, with 39% of respondents in total leveraging external vendors or consultants to supplement their internal efforts. This was by far the most common approach in the energy sector (67%) and was also common in finance (50%), while in other sectors only around 33% of respondents took this approach.

Fully outsourced approaches to cyber security planning and strategy are less common, with only 19% of respondents overall opting for this. However, this varied significantly by sector. Notably, none of our finance and transport respondents reported full outsourcing of cyber security strategy and planning, while more than a third of healthcare respondents (36%) reported that they fully outsource cyber security planning and strategy. Energy and telecoms sectors fell somewhere in the middle.

Figure 4.15. Organisations' approach to cyber security for digital assets – Planning and strategy (share of respondents per sector)



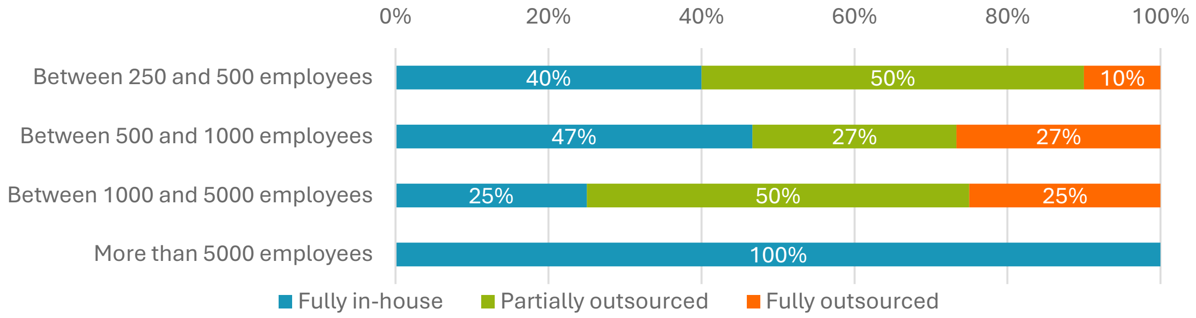
Note: n = 52 survey respondents. Respondents were asked to indicate who is responsible for planning and strategy. This is a duplicate of Figure 2.3, included again for explanatory purposes.

Looking at cyber security planning and strategy by organisation size revealed some interesting trends. Fully outsourced cyber security strategies are rare among organisations surveyed. Only 10% of companies with 250-500 employees and none of the ones with more than 5000 employees.

47% of organisations in the 500-1000 employee range reported that they managed cyber security strategy and planning fully in-house. While a partial approach was preferred among half of the organisations with 250-500 employees and 1000-5000 employees.

Organisations with more than 5000 employees preferred to manage their cyber security planning and strategy fully in-house (100%).

Figure 4.16. Organisations' approach to cyber security for digital assets – Planning and strategy, by organisation size (share of respondents per organisation size)



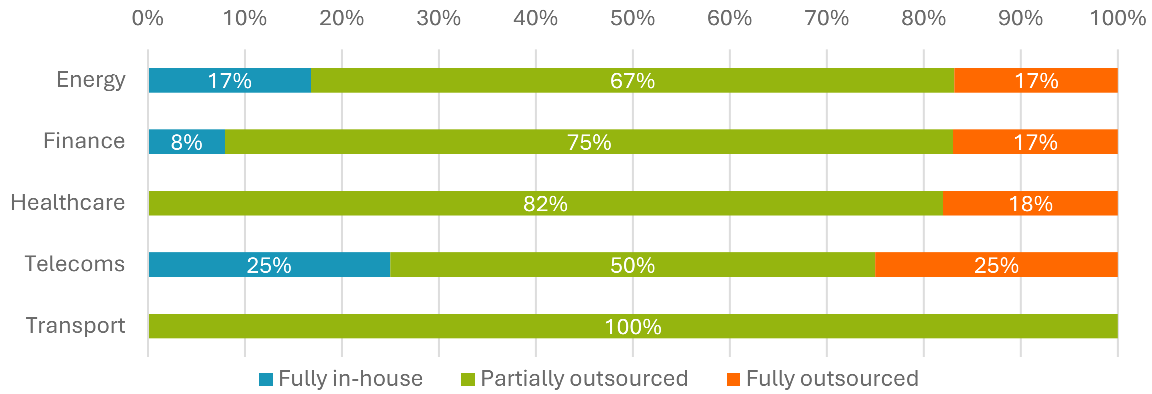
Note: n = 52 survey respondents. Respondents were asked to indicate who is responsible for planning and strategy.

Cyber security approach to deployment, management and updates

Looking at deployment, ongoing management, and update responsibility for cyber security, most respondents' organisations rely on outsourcing to some extent. Partial outsourcing is the most common approach by far, being used by 71% of all respondents, see Figure 4.14.

However, some sectors had a more mixed approach. Some respondents in the energy, finance and telecoms sectors reported that their organisations keep ongoing cyber security management and updates fully in-house; while all sectors other than healthcare had some respondents who fully outsourced this activity.

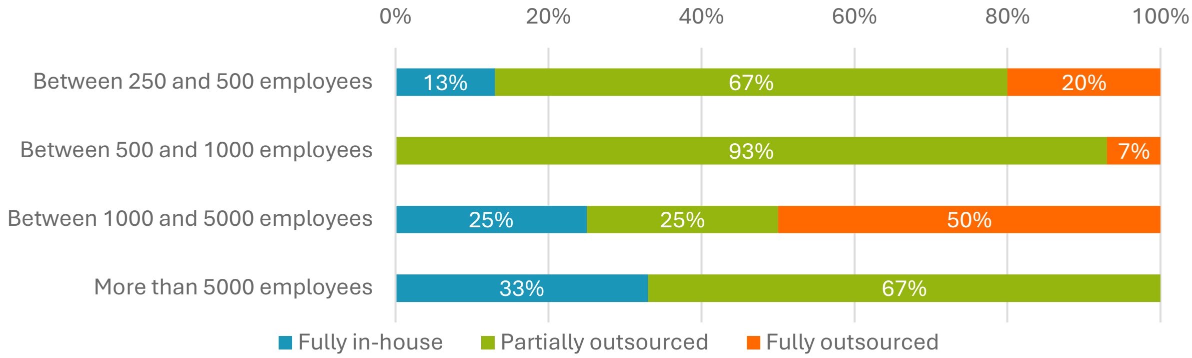
Figure 4.17. Organisations' approach to cyber security for digital assets – Deployment, management and updates (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to indicate how their organisation handles cyber security deployment, management and ongoing updates. This is a duplicate of Figure 2.4, included again for explanatory purposes.

To better understand this result, we analysed the data by comparing responses for different company sizes. Partial outsourcing was the most common response for all sizes of companies other than those in the 1000-5000 employee range. As with planning and strategy, a fully in-house cyber security management approach was unusual for smaller companies, with only 13% of companies with 250-500 employees and none in the 500-1000 employee range taking the fully in-house approach. Notably, no larger companies (more than 5000 employees) reported fully outsourcing their cyber security management and upgrades.

Figure 4.18 Organisations' approach to cyber security for digital assets – Deployment, management and updates, (share of respondents per organisation size)



Note: n = 52 survey respondents. Respondents were asked to indicate how their organisation handles cyber security deployment, management and ongoing updates.

4.1.2 Understanding of PQC and expectations for migration

Summary

A primary objective of the survey was to establish how familiar respondents were with PQC, what level of necessity they felt to push for PQC migration, and how far their organisations had progressed with migration planning and deployment. We also wanted to understand what resources respondents used to keep up-to-date with information on the quantum threat and PQC, and how long they expected migration to take. Organisations that have unrealistically short expectations for when a cryptographically relevant quantum computer will emerge are likely to act sooner. This controls their risk profile but could result in additional costs as they are forced to engage with the limited ecosystem. Additionally, they may find that they starve other short-term security activities of resources. Organisations that have unrealistically long expectations are obviously at risk of needing to take expensive, reactive measures later, or of being the victims of cyberattacks.

Key takeaways:

Most of our survey respondents stated that they were moderately or very familiar with PQC and the concept of PQC migration.

- Most respondents (70%) were “very familiar” (62%) or “extremely familiar” (8%) with PQC.
- 46% of respondents expected that a quantum-enabled cyber-attack on their organisations will be possible within 5 to 10 years; 40% predicted it will take 10 to 20 years. Only 8% believed an attack could occur in the next 5 years, indicating that most organisations do not consider PQC a matter to prioritise. However, those respondents who considered themselves to be PQC experts were much more likely to estimate the timeline for an attack to be <5 years.
- Respondents reported consulting a diverse range of sources to stay informed about quantum cyber security technologies and issues. Tech news and community forums were most popular, closely followed by guidance and information from public sector organisations and schemes (e.g. NCSC, Cyber Essentials).
- Most organisations (69%) are actively developing a strategy for PQC migration, but are yet to begin execution, while 23% reported they have already started migrating their cryptography. A smaller proportion (8%) are aware of the need for migration but are not yet ready to start. This indicates that most organisations recognise the importance of PQC but are at varying stages of preparedness.
- Around half of respondents (46%) anticipated that completing their PQC migration - once started – will require 3 to 5 years. Another 39% expected migration to require between 1 to 3 years. In the context of the finding that roughly half (46%) of the respondents believed a cryptographically relevant quantum computer will emerge in five to ten years, this suggests that some organisations are comfortable with extremely narrow margins for their estimations and may soon enter a situation where they believe they need more time than they have. Encouraging organisations to consider their estimates together in this way could be a motivating factor for migration.

4.1.2.1 Familiarity with PQC

We asked survey respondents to self-asses their level of familiarity with PQC. They could choose between:

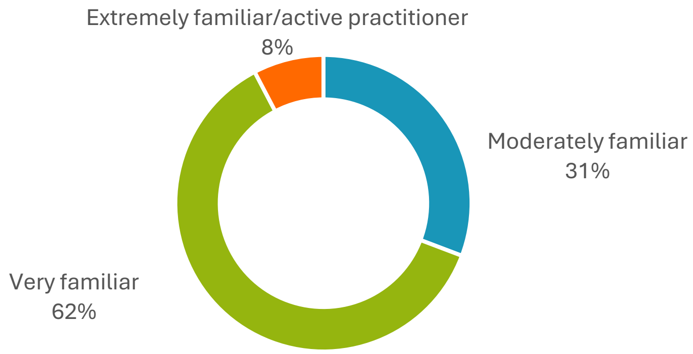
- Not familiar at all
- Slightly familiar: I am aware of its existence
- Moderately familiar: I have some technical knowledge in this area
- Very familiar: I have deep technical knowledge in this area

- Extremely familiar/active practitioner: I contribute to the development of this area via research papers, thought leadership reports, etc.

We used this question to screen out those that were unfamiliar with PQC since they would not be able to answer the questions in the main body of the survey.

Surprisingly no one reported being slightly familiar, instead most respondents (70%) reported a high level of familiarity with PQC, with 62% being 'very familiar' and 8% being 'extremely familiar'. This is perhaps not surprising given that the survey pool was focused on those in IT and cyber security roles. But it does give a clear indication that most respondents in roles with some level of responsibility for IT or cyber security strategy or deployment have a meaningful level of familiarity with the PQC challenge.

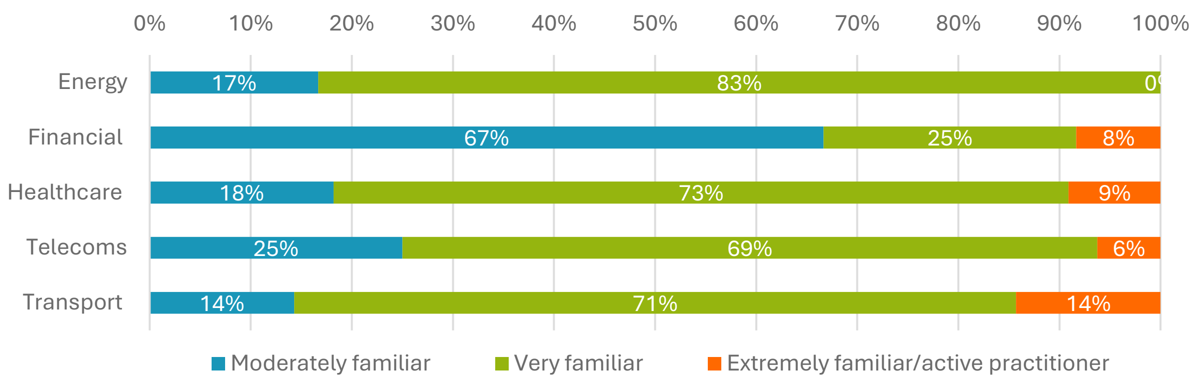
Figure 4.19. Respondents' familiarity with PQC concepts and technologies (share of respondents)



Note: n = 52 survey respondents. Respondents were asked to select the statement that best described their familiarity with PQC.

We analysed this data by sector (see Figure 4.20). The sector with the most familiar respondents with PQC is transport, with 14% of organisations being 'extremely familiar' and 71% being 'very familiar'. Healthcare and telecoms seemed to follow, with fewer 'extremely familiar' respondents (9% and 6% respectively) but high percentages of 'very familiar' respondents (73% and 69% respectively). The energy sector did not have 'extremely familiar' respondents, but did have the largest percentage of 'very familiar' respondents (83%) across all sectors. The finance sector came last in the familiarity ranking due to most of their respondents being 'moderately familiar' with PQC concepts and technologies.

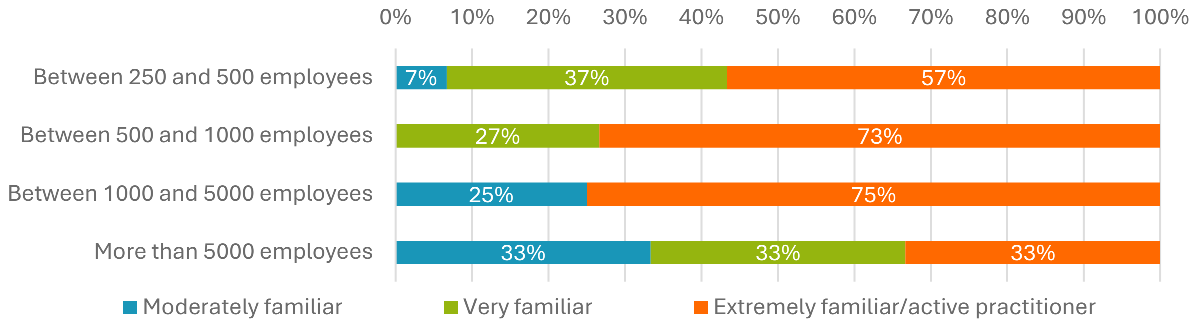
Figure 4.20. Familiarity with PQC concepts and technologies (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to select the statement that best described their familiarity with PQC.

We also analysed responses by organisation size. Of companies with 250-500 employees, only 57% reported being very familiar with PQC, with 37% stating they were moderately familiar, suggesting a more limited internal capability. As organisations become larger, respondents were more likely to say they are very familiar or extremely familiar with PQC. Organisations in the 500-1000 employee range were split between moderately familiar (27%) and very familiar (73%). Among organisations with 1000-5000 employees, 100% of respondents reported being very familiar (75%) or extremely familiar (25%) with PQC. The three respondents belonging to organisations with more than 5000 employees were equally split between moderately familiar (33%), very familiar (33%) and extremely familiar (33%).

Figure 4.21 Familiarity with PQC concepts and technologies (share of respondents per organisation size)

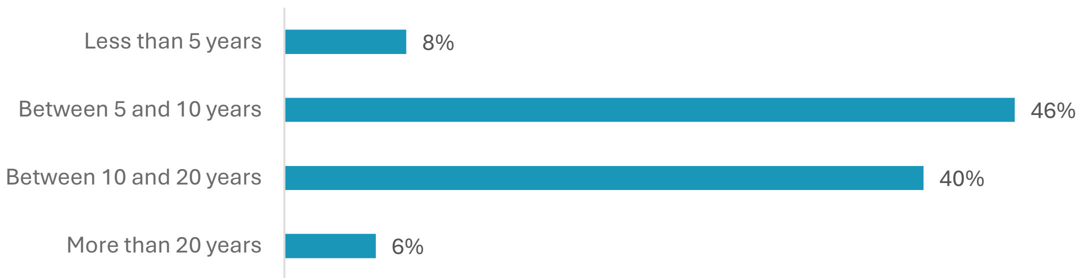


Note: n = 52 survey respondents. Respondents were asked to select the statement that best described their familiarity with PQC.

4.1.2.2 Understanding the quantum threat timelines

Among qualified survey respondents from our five target CNI sectors, most anticipated that a significant quantum threat will emerge within the next 5 to 20 years, with 46% expecting an attack within 5 to 10 years and 40% predicting it will take 10 to 20 years (see Figure 4.22.) This suggests a widespread belief that quantum threats are on the horizon but not necessarily imminent. Only 8% believed an attack could occur in the next 5 years, indicating that most organisations do not yet perceive PQC as an urgent priority. Only 6% expected quantum threats to take more than 20 years to materialise.

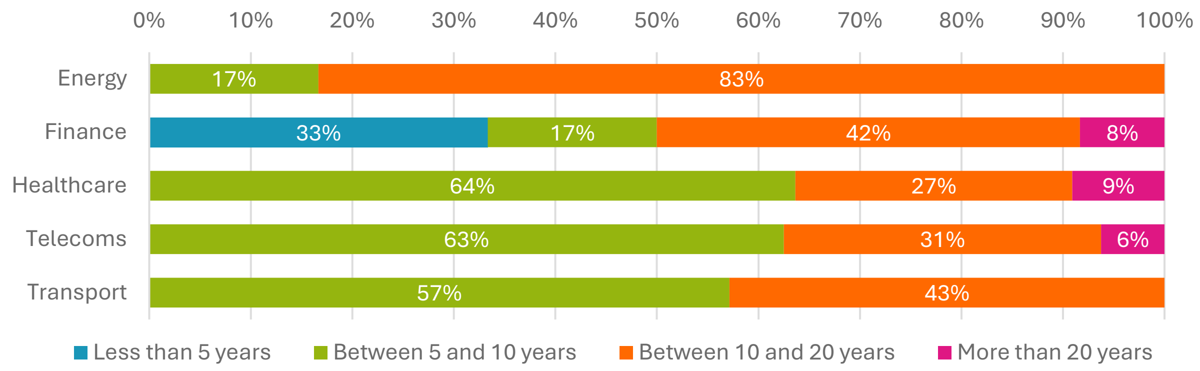
Figure 4.22. Expectation of time until a quantum computer enables a cyber-attack against organisations (share of respondents)



Note: n = 52 survey respondents. Respondents were asked how many years it could take for a quantum computer to enable a cyber attack against an organisation's system.

Survey responses indicated quite varied opinions among financial institutions, with 33% of respondents believing that the quantum threat is less than 5 years away (see Figure 4.23). This statement was unique to the sector. Most respondents in the healthcare (64%), telecoms (63%) and transport (57%) sectors believed that a quantum computer will become available in 5 to 10 years. The energy sector seemed to see the threat as further away, with 83% of respondents positioning the timeline of the first quantum computer in the 10 to 20 years' range. Few respondents in the healthcare (9%), finance (8%) and telecoms sectors (6%) anticipated the quantum threats taking more than 20 years to materialise.

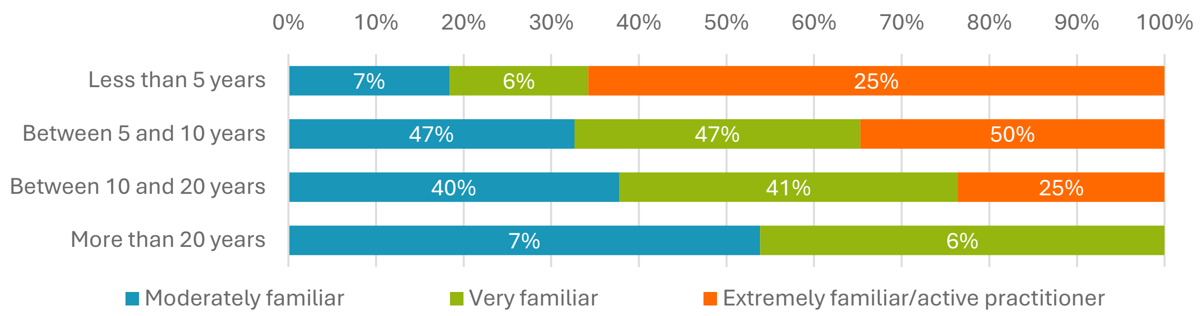
Figure 4.23. Expectation of time until a quantum computer enables a cyber-attack against organisations (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked to estimate likely number of years until a quantum computer could enable a cyber attack against an organisation's systems. This is a duplicate of Figure 2.6, included again for explanatory purposes.

Looking across all sectors, familiarity with PQC was a strong predictor of perceived criticality (see Figure 4.24). Among those extremely familiar with quantum security, 25% believed attacks could happen in less than 5 years, while 50% expected them within 5 to 10 years. Those moderately or very familiar were more evenly split between 5-10 years and 10-20 years. This suggests that deeper technical expertise may correlate with a greater sense of concern around quantum security risks.

Figure 4.24. Expectation of time until a quantum computer enables a cyber attack mapped against respondent's level of familiarity with PQC (share of respondents)



Note: N = 52 survey respondents. Respondents were asked to estimate the number of years until a quantum computer could enable a cyber attack against an organisation's systems.

Among the combined 90 screened-in and screened-out participants, including respondents from academia and other non-target sectors, the most common prediction for when a quantum computer will enable an attack was between 5 and 10 years (31%), followed by 10 to 20 years (27%) (see Figure 2.7). This full respondent pool was more likely than our qualified CNI survey respondent group to believe an attack could happen within 5 years (18%). Notably, 20% reported being unsure, this contrasts with how none of the qualified respondents were unsure, even though this question was not used for screening purposes.

4.1.2.3 Migration journey: Status and timings

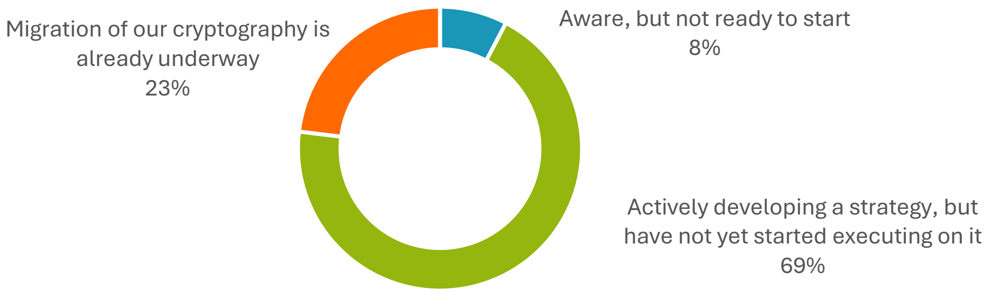
To understand the PQC migration journey of the organisations we surveyed, we asked two questions:

- What is the current status of your PQC migration?
- How long do you expect migration to take, once started?

The intention was to establish a baseline understanding of how far organisations have progressed, with a view to ensuring interventions can 'meet them where they are' to provide the most effective support.

Most organisations (69%) are actively developing a strategy for PQC migration, but are yet to begin execution (see Figure 4.25). While 23% reported they have already started migrating their cryptography. A smaller 8% are aware of the need for migration but are not yet ready to start, indicating that most organisations recognise the importance of PQC but are at varying stages of preparedness.

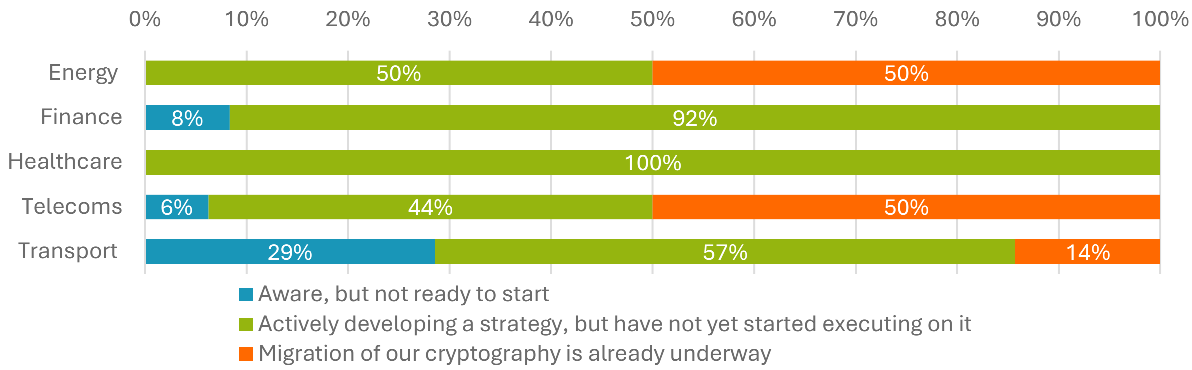
Figure 4.25. Status of PQC migration planning and execution (share of respondents)



Note: n = 52 survey respondents. Respondents were asked "Which of the following statements best characterises the current status of your organisation's migration towards PQC?".

The telecoms and energy sectors are leading in PQC migration, with a significant portion of organisations already implementing cryptographic upgrades, reflecting a proactive approach to securing critical infrastructure (see Figure 4.26). Finance and healthcare are heavily engaged in strategy development, indicating strong awareness but slower execution, likely due to implementation complexities and regulatory concerns (e.g. regulation being too vague on cryptography, lack of detailed guidance, or lack of PQC certification algorithms that ensure adoption) and implementation complexities. Transport lags behind, with 30% of organisations still in the early awareness phase, suggesting a lack of readiness or prioritisation compared to other industries.

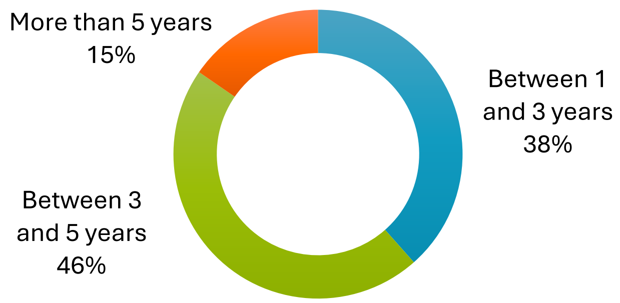
Figure 4.26. Status of PQC migration planning and execution (share of respondents per sector)



Note: n = 52 survey respondents. Respondents were asked if they were actively developing a migration strategy. This is a duplicate of Figure 2.9*, included again for explanatory purposes.*

Most respondents anticipated that completing their PQC migration journey, once started, will take between 3 to 5 years (46%) (see Figure 4.27). A significant 39% expected to complete migration within 1 to 3 years of starting. However, 15% believed it will take them more than 5 years to complete their migration.

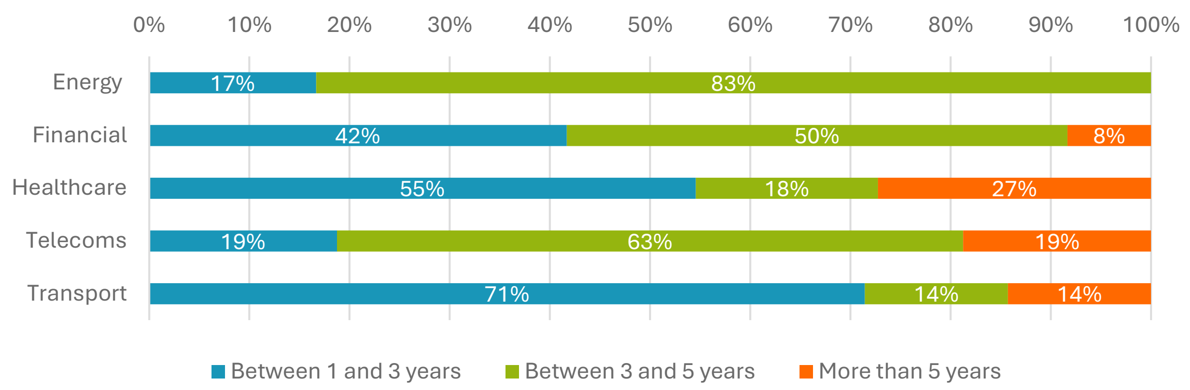
Figure 4.27. Respondents' estimate of time required for PQC migration planning and execution (share of respondents)



Note: n = 52 survey respondents. Respondents were asked how long it will take their organisation to complete their PQC migration journey, once started.

The expected timeline for PQC migration completion varied significantly across sectors (see Figure 4.28). 71% of transport respondents anticipated completion within 1-3 years, followed by healthcare (55%) and finance (42%), indicating that these industries are prioritising rapid migration efforts. Energy (83%) and telecoms (63%) mostly expected completion in 3-5 years, suggesting a more measured pace to implementation. However, notable portions of healthcare (27%), telecoms (19%), and finance (8%) expected migration to take more than 5 years, reflecting potential regulatory, technical, or resource-based challenges in fully transitioning to PQC security.

Figure 4.28. Respondents' estimate of time required for PQC migration planning and execution (share of respondents per sector)



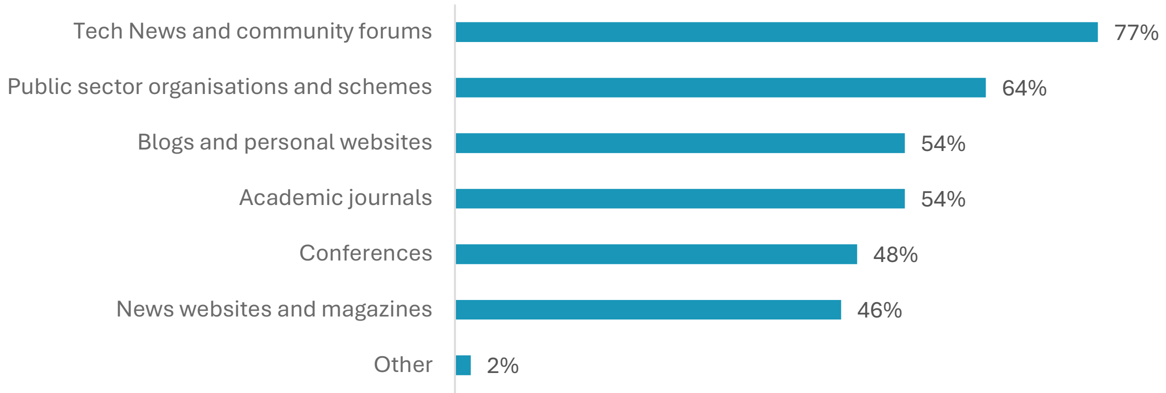
Note: n = 52 survey respondents. Respondents were asked how much time their organisation's full migration to PQC will take, once started. This is a duplicate of Figure 2.10, included again for explanatory purposes.

4.1.2.4 PQC resources

All respondents consulted a diverse range of sources to stay informed about quantum cyber security technologies and issues. Tech news and community forums were the most popular (examples given to respondents were Ars Technica, Hacker News, and Bleeping Computer) (see Figure 4.29). Guidance and information from public sector organisation and schemes (e.g. NCSC, Cyber Essentials) was the second most popular source. These are by no means the only sources respondents turn to, and the other four sources that were offered as response options were each chosen by around half of the respondents.

The implication is that for PQC migration information and guidance to achieve the widest reach, DSIT should focus first on tech news and community forums, and on working with public sector organisations and schemes such as NCSC. But there are also opportunities to communicate with industry end-users via other channels.

Figure 4.29. Sources consulted and followed by respondents for quantum cyber security information (share of respondents)

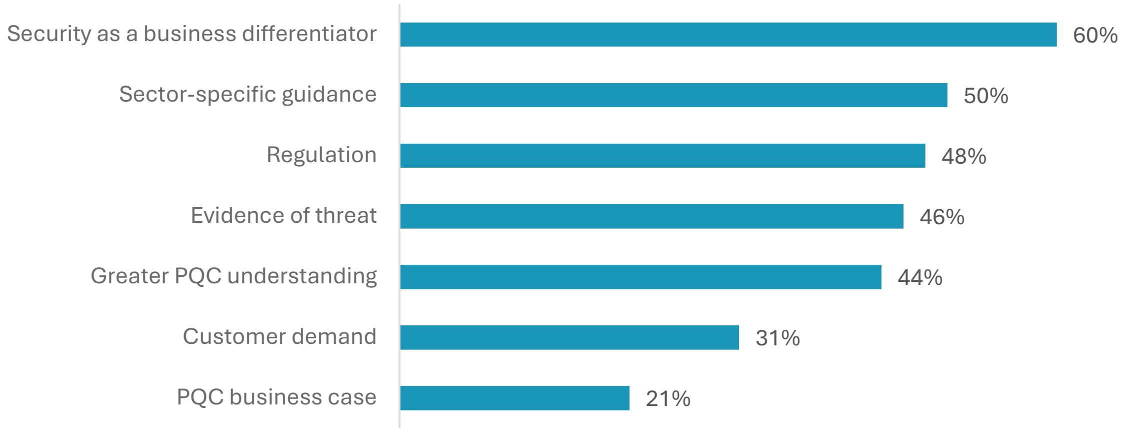


Note: n = 52 survey respondents. Respondents were asked to ‘select all that apply’. Chart shows the share of respondents who selected each option. This is a duplicate of Figure 4.12, included again for explanatory purposes.

4.1.3 Incentives and drivers for PQC Migration

We asked respondents to share what their most important drivers and incentives were for PQC migration (see Figure 4.30). The list of drivers we provided were examples of actual and potential drivers. Overall, the ability to use higher levels of security as a business differentiator (i.e. being more secure than their competitors to capture more market share), the availability of sector-specific guidance, and government/regulator requirements or mandates were the top 3 drivers.

Figure 4.30. Main PQC migration drivers for organisations, top 3 (share of respondents)



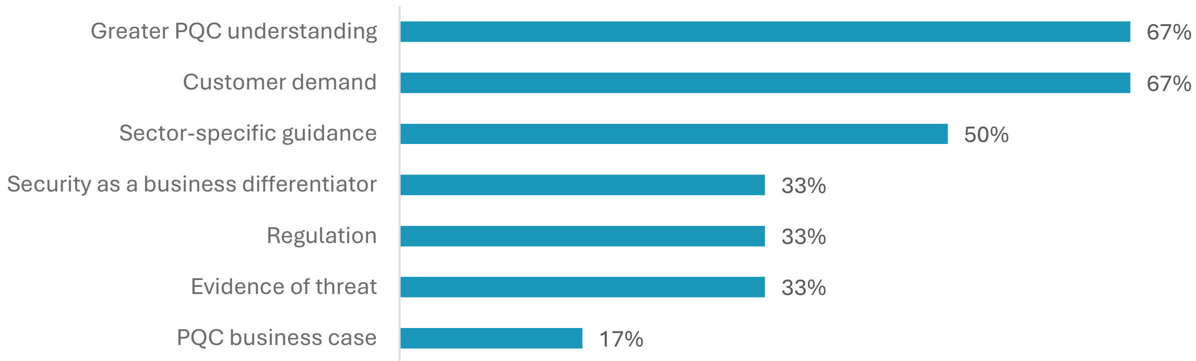
Note: n = 52 survey respondents. Respondents were asked to select the top 3 drivers for their organisation to start planning for or deploying PQC migration. Chart shows % of respondents who chose the option as one of their top 3 within all data.

However, the drivers of PQC migration varied significantly by sector, organisation size, role, board membership, budget influence, and familiarity with PQC. For example, security as a business differentiator was the top driver in only one sector: healthcare. Note that the healthcare sector in this context should be understood as both healthcare providers and vendors to providers.

Sector-level analysis

Energy sector

Figure 4.31. Main PQC migration drivers for organisations in the energy sector, top 3 (share of respondents)



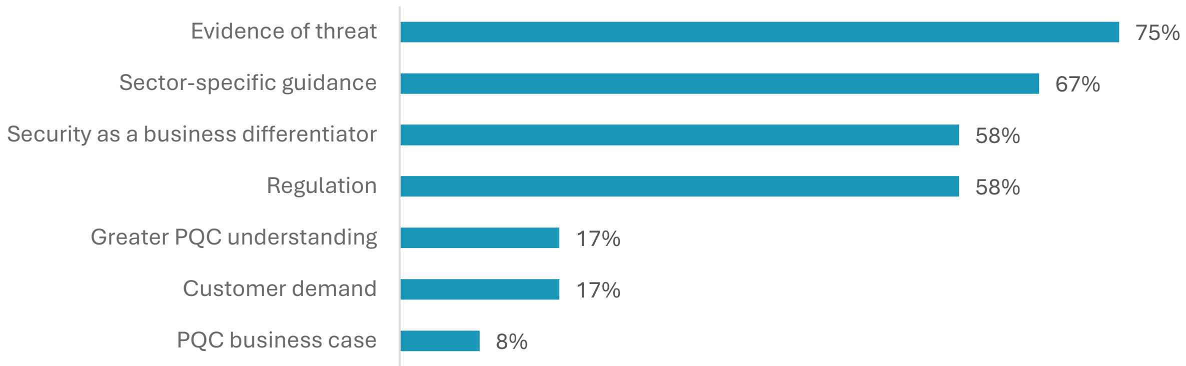
Note: n = 6 respondents. Respondents were asked to select their top 3 drivers. Chart shows % of respondents who chose the option as one of their top 3.

For the energy sector, the key drivers of PQC migration were customer demand (67%) and internal understanding of PQC (67%) (see Figure 4.31), suggesting that organisations are responding to external expectations while also prioritising knowledge building within their teams. Sector-specific guidance (50%) was another significant factor, indicating this would constitute another strong incentive for PQC migration. Regulatory requirements (33%), security as a business differentiator (33%), and evidence of quantum threats (33%) were secondary concerns, implying that while compliance and security benefits are recognised, they are not the primary motivators. The business case for PQC (17%) ranked the lowest, suggesting that financial justification is not a major factor in decision-making for energy firms, which are likely prioritising resilience and stakeholder expectations.

Finance sector

For the finance sector, the most significant driver of PQC adoption was evidence of quantum-enabled cyber threats (75%) (see Figure 4.32), suggesting that organisations are primarily motivated by the potential risks posed by quantum attacks. Sector-specific guidance (67%) and government or regulatory requirements (58%) also played a major role, indicating that financial institutions rely on clear external directives before committing to migration. The ability to use higher security levels as a business differentiator (58%) was another key factor, highlighting the competitive advantage of strong cyber security. Customer demand (17%) and internal understanding of PQC (17%) were much lower priorities, while a clear business case (8%) was the least influential factor, suggesting that financial institutions see PQC as a necessary precaution rather than a financially-driven decision.

Figure 4.32. Main PQC migration drivers for organisations in the finance sector top 3 (share of respondents)

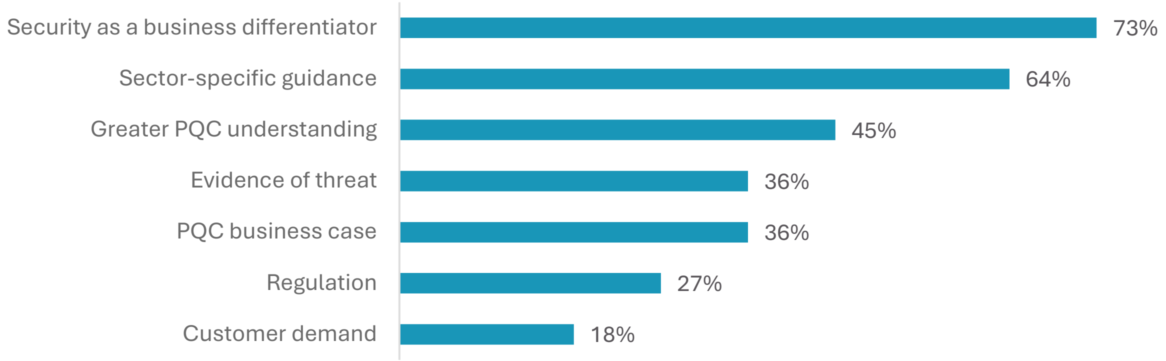


Note: n = 12 respondents. Respondents were asked to select their top 3 drivers. Chart shows % of respondents who chose the option as one of their top 3.

Healthcare sector

Healthcare's top driver of PQC adoption was the ability to use higher security levels as a business differentiator (73%) (see Figure 4.33), indicating that organisations see enhanced cyber security as a competitive advantage. Sector-specific guidance (64%) was also a key factor, suggesting that clearer regulatory direction would act as another strong incentive. Internal understanding of PQC (45%), evidence of quantum threats (36%) and PQC business case (36%) ranked moderately, while government mandates (27%) and customer demand (18%) were less influential, highlighting that regulatory pressure and consumer expectations are not primary motivators for PQC adoption in healthcare.

Figure 4.33. Main PQC migration drivers for organisations in the healthcare sector top 3 (share of respondents)

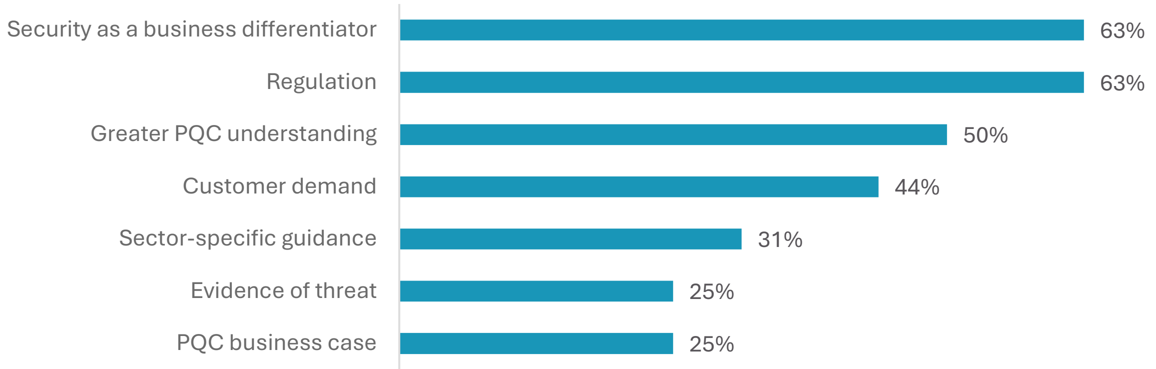


Note: n = 11 respondents. Respondents were asked to select their top 3 drivers. Chart shows % of respondents who chose the option as one of their top 3.

Telecoms sector

For the telecoms sector, regulatory requirements (63%) and security as a business differentiator (63%) were the top drivers of PQC adoption (see Figure 4.34), highlighting that both compliance pressures and competitive advantages are key motivators. Internal understanding of PQC (50%) and customer demand (44%) also played a role, suggesting a mix of internal and external motivations driving adoption. Sector-specific guidance (31%) and evidence of quantum threats (25%) ranked lower, indicating that telecoms companies are moving towards PQC based on compliance and market positioning rather than immediate cyber security risks. Although no specific guidance explicitly mandating PQC for telecoms exists, the Telecommunications, Security Code of Practice [37] contains multiple clauses about encryption. It also uses the phrase "effective encryption", thereby pushing the burden for knowing what "effective" means onto implementers. A clear business case (25%) was one of the least influential factors, suggesting that financial justification is not a primary incentive to adoption in this sector.

Figure 4.34. Main PQC migration drivers for organisations in the telecoms sector top 3 (share of respondents)

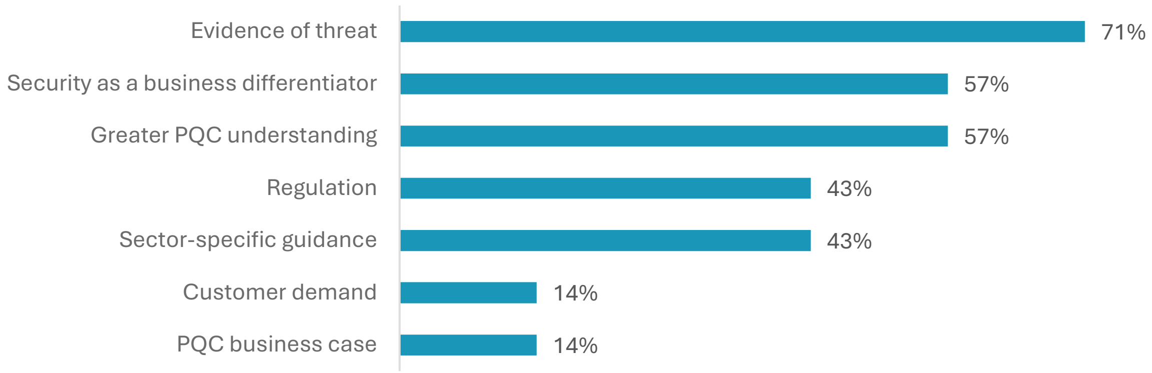


Note: n = 16 respondents. Respondents were asked to select their top 3 drivers. Chart shows % of respondents who chose the option as one of their top 3.

Transport sector

Transport's top driver of PQC adoption was greater evidence of quantum-enabled threats (71%) (see Figure 4.35), suggesting that organisations in this sector are highly responsive to tangible cyber security risks. Security as a business differentiator (57%) and internal understanding of PQC (57%) were also key motivators, indicating that both competitive positioning and knowledge-building play a significant role in adoption. Government regulations (43%) and sector-specific guidance (43%) were important but less dominant, while customer demand (14%) and a clear business case (14%) ranked lowest, implying that external pressure and financial justification are not primary factors driving PQC migration in transport.

Figure 4.35. Main PQC migration drivers for organisations in the transport sector top 3 (share of respondents)

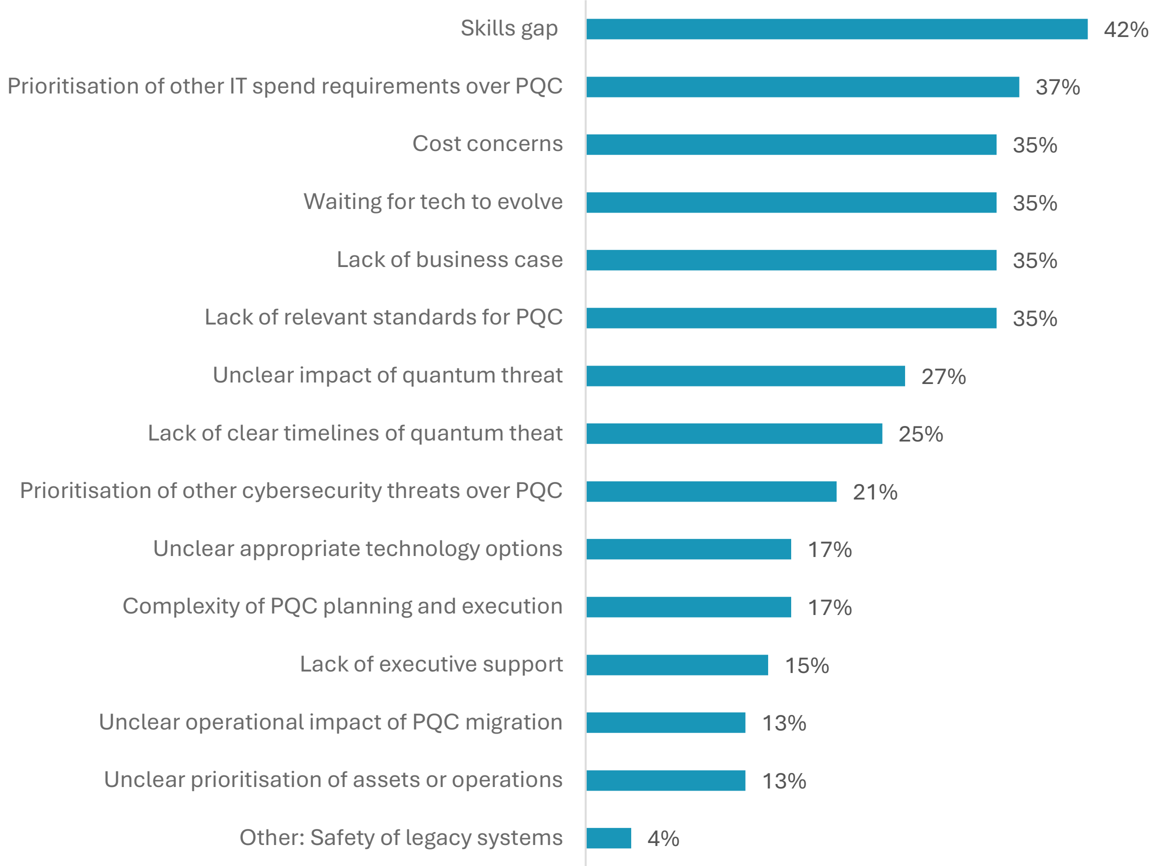


Note: n = 7 respondents. Respondents were asked to select their top 3 drivers. Chart shows % of respondents who chose the option as one of their top 3.

4.1.4 Challenges and blockers for PQC migration

We asked respondents to select their top 3 barriers to PQC migration. The skills gap (42%) was identified as the biggest barrier to PQC migration, with just under half of respondents selecting this option. Other significant challenges include the prioritisation of other IT spend requirements over PQC (37%) closely followed by four blockers, each chosen by 35% of respondents: cost concerns, waiting for tech to evolve, lack of business case and lack of relevant standards for PQC.

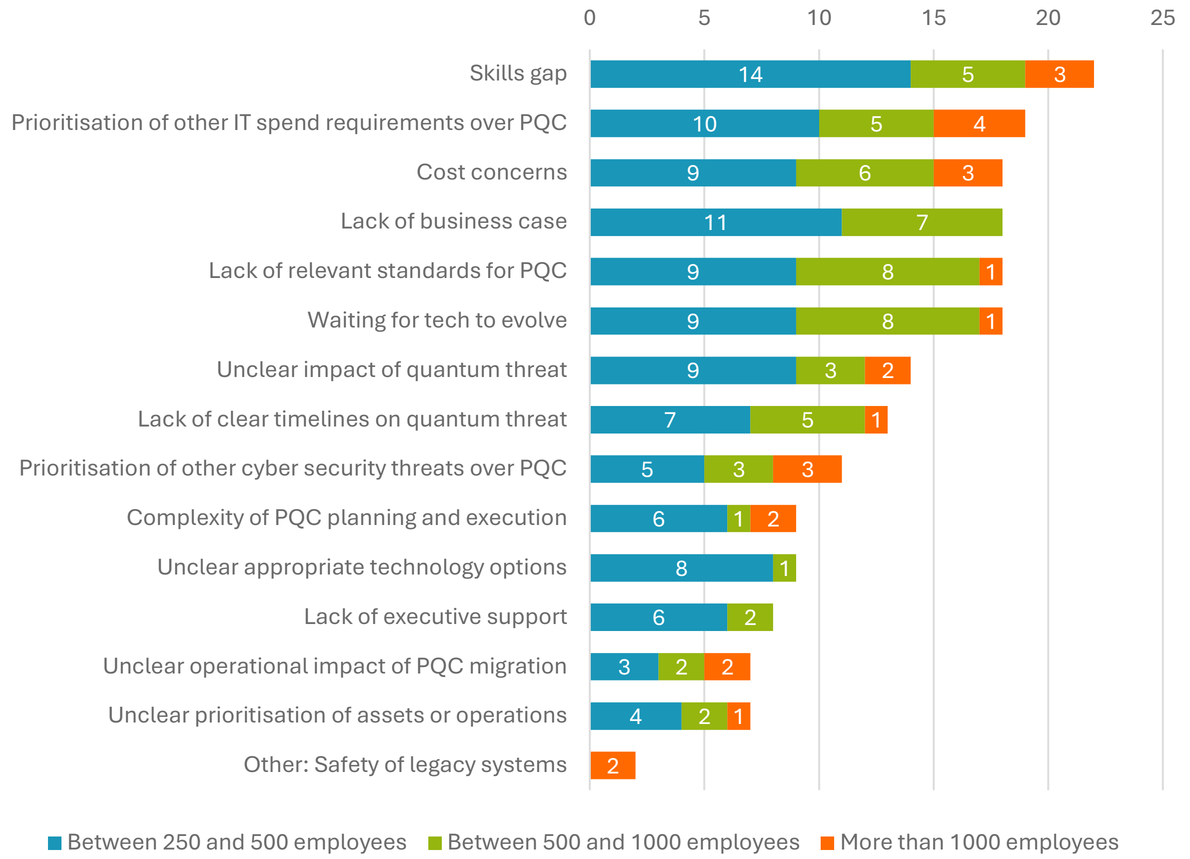
Figure 4.36. Main PQC migration blockers for organisations top 3 (share of respondents)



Note: n = 52 survey respondents. Respondents were asked to select which top 3 barriers are currently preventing or slowing down their organisation's migration to PQC.

We also analysed responses to this question by organisation size. Larger organisations (1000+ employees) identified the prioritisation of other IT spend requirements as the main barrier to PQC migration (57%). For medium organisations (between 500 and 1000 employees), the main barriers were the lack of relevant standards for PQC (53%) and waiting for technology to evolve (53%). Smaller companies (between 250 and 500 employees) identified the skills gap (47%) as their primary barrier, followed by lack of business case (37%) and the prioritisation of other IT spend requirements over PQC (33%).

Figure 4.37. Main PQC migration blockers for organisations, top 3 (count per organisation size)



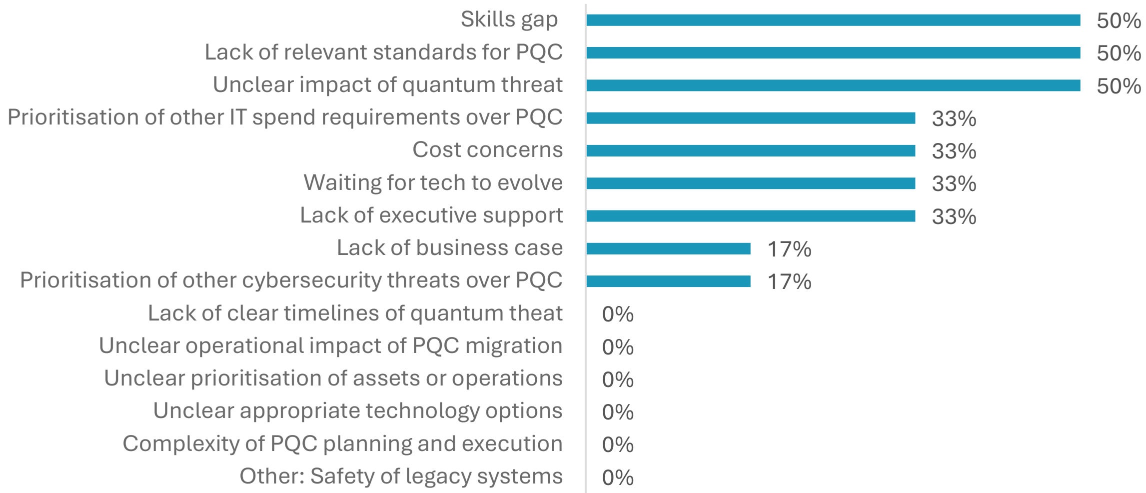
Note: n = 52 survey respondents. Respondents were asked to select which top 3 barriers are currently preventing or slowing down their organisation's migration to PQC.

Sector level analysis

Energy Sector

The following top 3 blockers to PQC migration were selected by 50% of energy survey respondents: skills gap, lack of relevant standards for PQC, and unclear impact on quantum threat (see Figure 4.38). This suggests that energy organisations are struggling to formulate the need for PQC migration and find the relevant experts capable of unfolding the complexity of migration. Four blockers followed the top 3, all of them selected by 33% of energy survey respondents: cost concerns, waiting for tech to evolve, lack of executive support, and lack of business case. Those seem to reveal difficulties in mapping out and planning for PQC migration based on the lack of knowledge reflected by the top 3 blockers.

Figure 4.38. Main PQC migration blockers for organisations in the energy sector, top 3 (share of respondents)

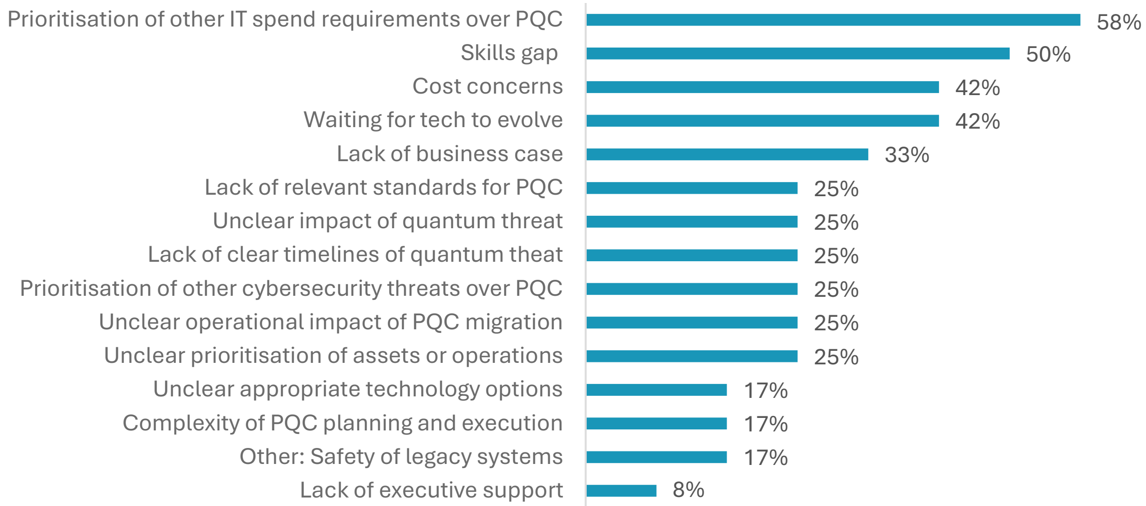


Note: n = 6 survey respondents. Respondents were asked which barriers are currently preventing or slowing down their organisation's migration to PQC.

Finance sector

According to 58% of financial organisations surveyed, the prioritisation of other IT spend requirements over PQC is the main blocker to the PQC migration (see Figure 4.39). This implies that organisations are struggling to articulate the need for initiating the PQC migration; perhaps because the threat is yet to materialise, unlike other cyber security threats that are currently impacting organisations. 50% of respondents reported a skills gap as the second main blocker for transitioning to PQC. Cost concerns and waiting for tech to evolve share the third position - supported by 42% of respondents.

Figure 4.39. Main PQC migration blockers for organisations in the finance sector, top 3 (share of respondents)

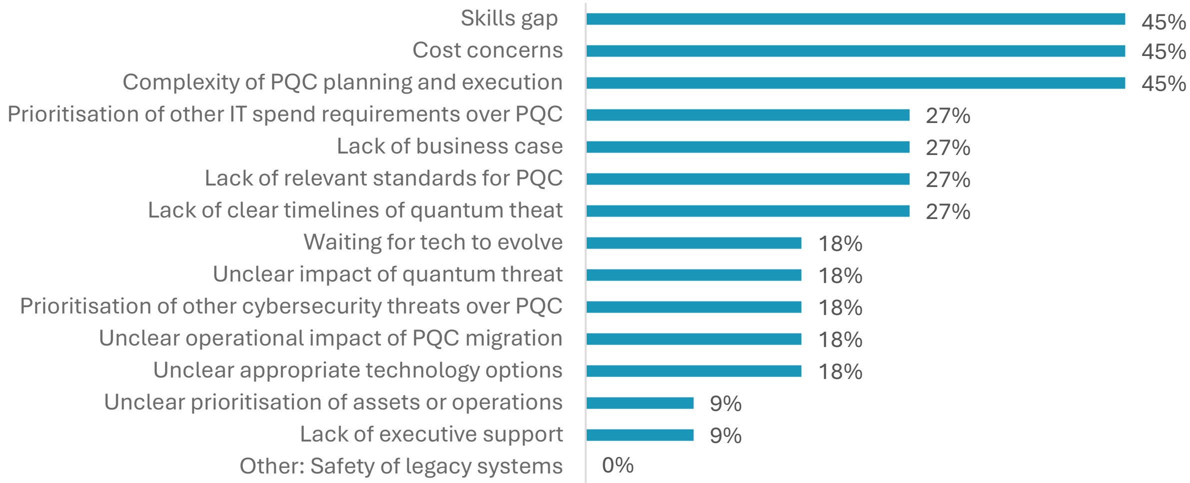


Note: n = 12 survey respondents. Respondents were asked which barriers are currently preventing or slowing down their organisation's migration to PQC.

Healthcare sector

45% of survey respondents in the healthcare sector identified the top 3 blockers as: skills gap, cost concerns, and complexity of PQC planning and execution (see Figure 4.40). This suggests that organisations are struggling to find people with expertise to unfold what the PQC migration requires, and therefore to develop and execute a migration plan. They are also aware of the significant investment required for the migration and are concerned about costs.

Figure 4.40. Main PQC migration blockers for organisations in the healthcare sector, top 3 (share of respondents)

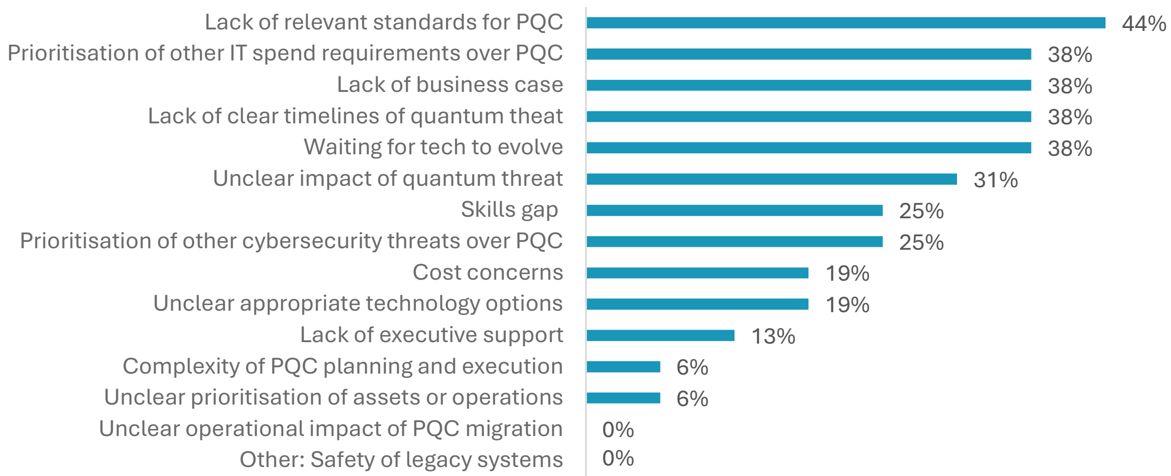


Note: n = 11 survey respondents. Respondents were asked which barriers are currently preventing or slowing down their organisation's migration to PQC.

Telecoms sector

44% of surveyed organisations in the telecoms sector highlighted the lack of relevant standards for PQC as the main challenge for the migration (see Figure 4.41). The following four blockers shared the second position, being cited by 38% of survey respondents: prioritisation of other IT spend requirements over PQC, lack of business case, lack of clear timelines of quantum threat, and waiting for tech to evolve. Organisations in this sector therefore appeared hesitant to transition to PQC without clear regulatory guidance, compelling financial incentives, or more developed technology.

Figure 4.41. Main PQC migration blockers for organisations in the telecoms sector, top 3 (share of respondents)

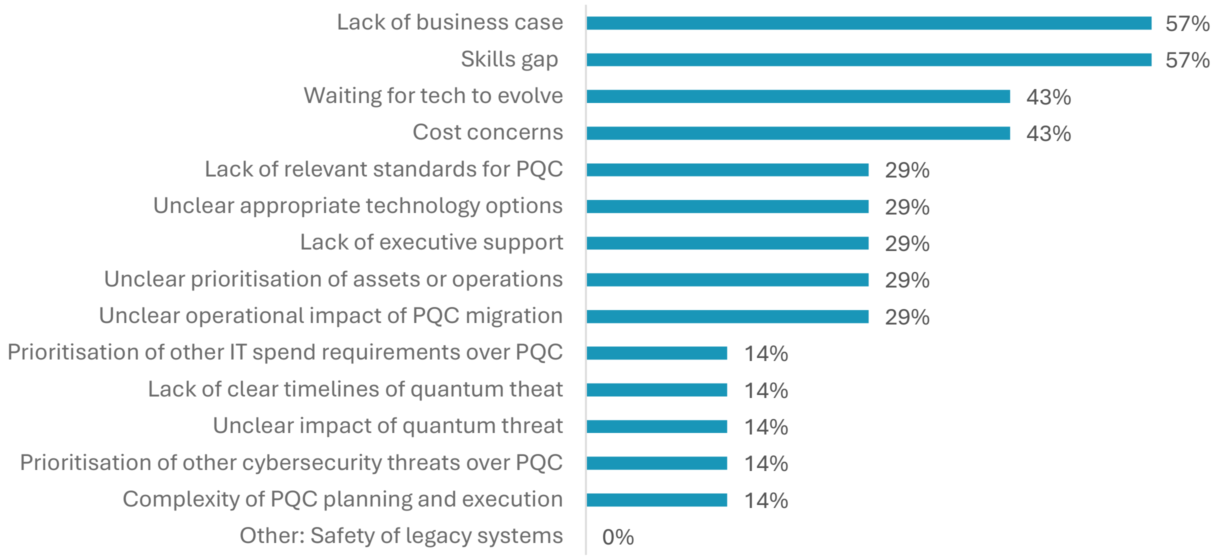


Note: n = 16 survey respondents. Respondents were asked which barriers are currently preventing or slowing down their organisation's migration to PQC.

Transport sector

Most surveyed organisations in the transport sector (57%) deemed the lack of business case and skills gap as the two primary blockers for the PQC transition (see Figure 4.42). This suggests that those organisations struggle to articulate the need for PQC migration in a way that makes sense for their business and find the relevant people to lead and execute it. Waiting for tech to evolve and cost concerns ranked as the next two blockers, both cited by 43% of respondents.

Figure 4.42. Main PQC migration blockers for organisations in the transport sector, top 3 (share of respondents)



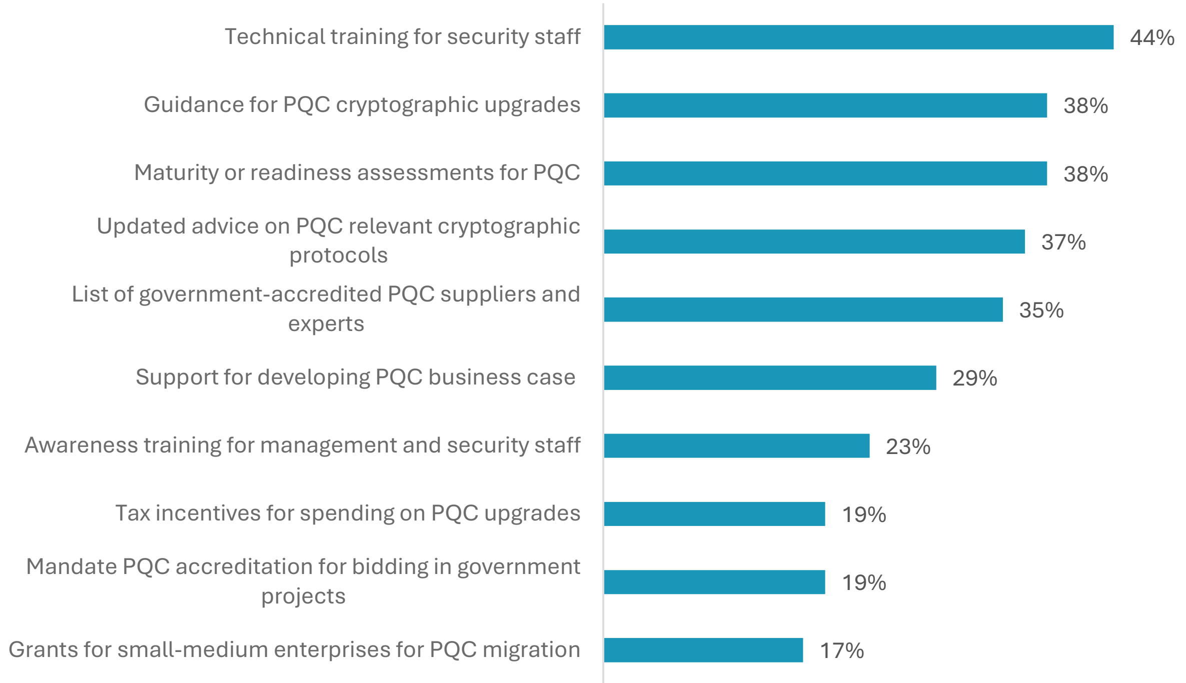
Note: n = 7 survey respondents. Respondents were asked which barriers are currently preventing or slowing down their organisation's migration to PQC.

4.1.5 Government measures to support organisations with PQC migration

The final survey questions focused on what type of support activities by government or regulators would be most valuable for CNI organisations. Once respondents selected their top 3 government measures, they were asked to elaborate in their selection through a free-text box. These answers can be found in Table 4.1.

Overall, the top 3 support activities judged to be most valuable were technical training for security staff, maturity or readiness assessments for PQC, and provision of guidance for how to approach cryptographic upgrades for PQC see (Figure 4.43).

Figure 4.43. Most important PQC migration support from government/regulators for organisations, top 3 (share of respondents)



Note: n = 52 survey respondents. Respondents were asked to select the top 3 areas in which the government could provide support to begin planning/deploying PQC migration.

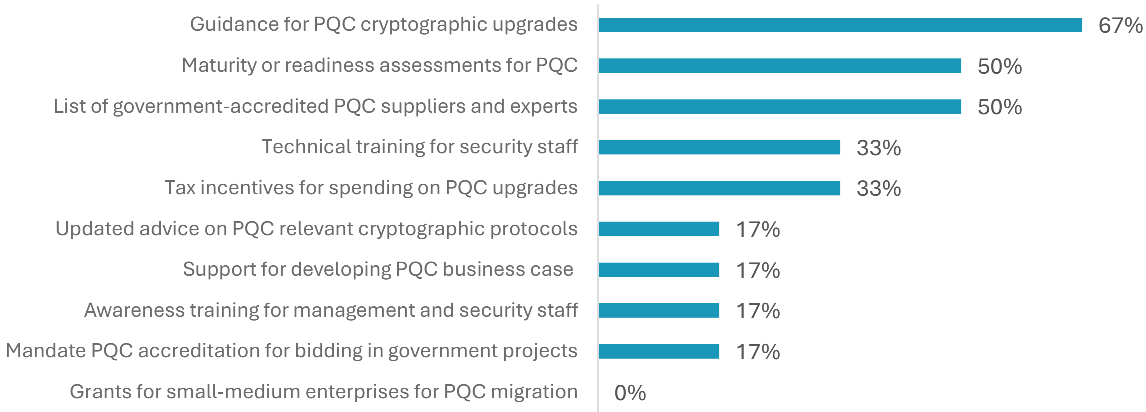
Sector-level analysis

Different sectors have distinct priorities for government and regulatory support. Telecoms and transport strongly prioritise technical training for security staff and awareness training for management, highlighting a need for workforce capability upskilling on PQC. Energy and finance request guidance on how to approach cryptographic updates, with a further ask from finance on maturity or readiness assessments and up-to-date regulatory advice, indicating a demand for clear evaluation frameworks and compliance guidance. Healthcare values guidance on PQC implementation and government-accredited PQC lists. Grants and tax incentives are of relatively limited interest for most sectors. Organisations surveyed primarily seek education, training, and structured assessments to ensure secure and effective PQC adoption.

Energy sector

In the energy sector, clear guidance on cryptographic upgrades for PQC (67%) was the most sought-after type of support from the government, highlighting a need for structured direction on implementation (see Figure 4.44). Additionally, 50% of respondents wanted a list of accredited PQC suppliers and experts, as well as maturity or readiness assessments, indicating that energy organisations are looking for both trusted resources and benchmarks to evaluate their preparedness.

Figure 4.44. Most important PQC migration support from government/regulators for organisations in the energy sector, top 3 (share of respondents)

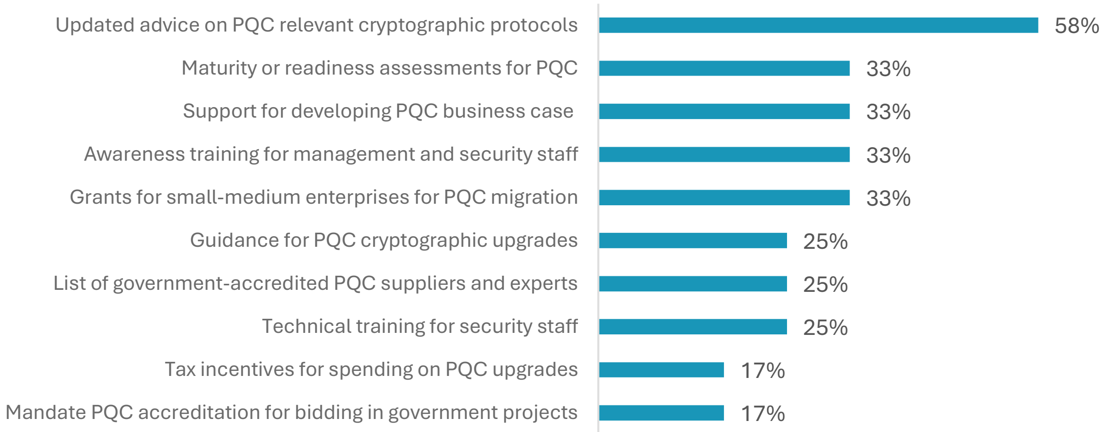


Note: n = 6 respondents. Respondents were asked to select the top 3 support activities they would like to see from government and regulators. The percentages represent the proportion of sector respondents who selected each option as one of their top 3 priorities.

Finance sector

In the finance sector, 58% of respondents prioritised up-to-date advice on specific cryptographic protocols relevant to PQC, indicating a strong need for technical guidance (see Figure 4.45). Awareness training for management and security staff, along with maturity or readiness assessments, were both valued by 33% of respondents, suggesting that financial institutions also recognise the importance of education and structured evaluation in their transition to PQC.

Figure 4.45. Most important PQC migration support from government/regulators for organisations in the finance sector, top 3 (share of respondents)

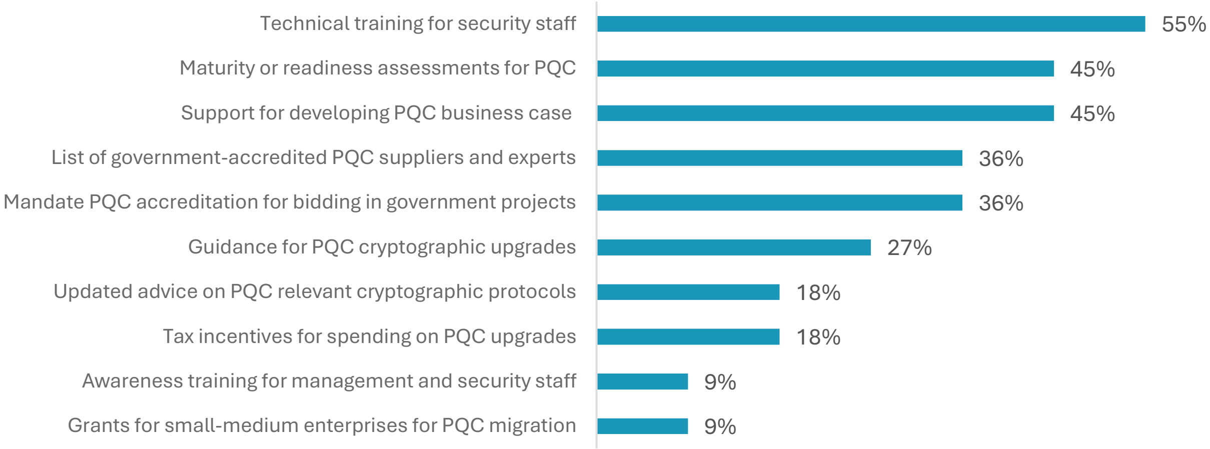


Note: n = 12 respondents. Respondents were asked to select the top 3 support activities they would like to see from government and regulators. The percentages represent the proportion of sector respondents who selected each option as one of their top 3 priorities.

Healthcare sector

In the healthcare sector, technical training for security staff was the most sought-after type of government support at 55%, indicating a strong need for skill development to manage PQC migration effectively (see Figure 4.46). Maturity or readiness assessments were also a priority for 45% of respondents, suggesting that organisations seek structured evaluations to measure their preparedness. Additionally, 45% highlighted the need for support in developing a clear business case or cost-benefit analysis for PQC migration, reflecting the sector's focus on financial justification and strategic planning.

Figure 4.46. Most important PQC migration support from government/regulators for organisations in the healthcare sector, top 3 (share of respondents)

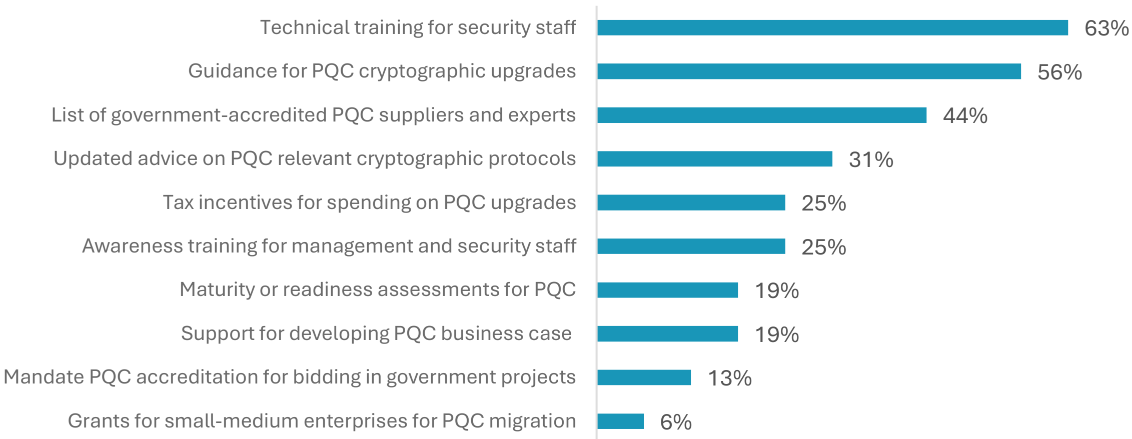


Note: n = 11 respondents. Respondents were asked to select the top 3 support activities they would like to see from government and regulators. The percentages represent the proportion of sector respondents who selected each option as one of their top 3 priorities.

Telecoms sector

In the telecoms sector, technical training for security staff (63%), guidance for PQC cryptographic upgrades (56%), and a list of government-accredited PQC suppliers and experts (44%) are the top 3 government measures that survey respondents would like to see. This suggests that, acknowledging their lack of PQC expertise, organisations seek training, cryptographic guidance, and recommended suppliers and experts to engage with.

Figure 4.47. Most important PQC migration support from government/regulators for organisations in the telecoms sector, top 3 (share of respondents)

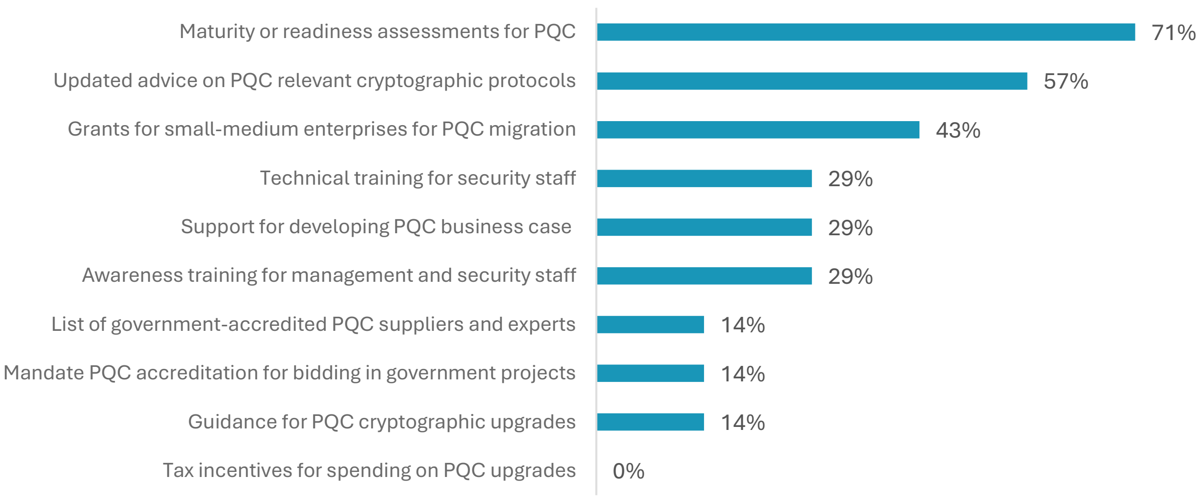


Note: n = 16 respondents. Respondents were asked to select the top 3 support activities they would like to see from government and regulators. The percentages represent the proportion of sector respondents who selected each option as one of their top 3 priorities.

Transport sector

In the transport sector, the most sought-after type of government support for PQC adoption is maturity or readiness assessments, with 71% of respondents seeking structured evaluations to guide their migration efforts (see Figure 4.48). It is recommended that evaluations should be performed against well-defined objectives, in a similar way to the NCSC CAF. Up-to-date advice on specific cryptographic protocols was also highly valued at 57%, indicating a need for clear technical guidance. Additionally, 43% highlighted the importance of grants for small- and medium-sized enterprises to support security improvements, suggesting that financial assistance could play a key role in accelerating PQC adoption within the sector.

Figure 4.48. Most important PQC migration support from government/regulators for organisations in the transport sector, top 3 (share of respondents)



Note: n = 7 respondents. Respondents were asked to select the top 3 support activities they would like to see from government and regulators. The percentages represent the proportion of sector respondents who selected each option as one of their top 3 priorities.

For each of the options selected for government help, survey respondents were asked to elaborate on their choice. Table 4.1 compiles all free-text answers from all respondents, grouped by type of support.

Table 4.1. Survey respondents' explanations of the type of PQC migration support they wish to see from government and regulators

Type of support	Answers from survey respondents
Technical training for security staff	• Offer certifications in PQC. • Provide hands-on training with real-world scenarios. • Support IT team with hands-on implementation of PQC. • Real-world scenarios, not just theory. • Hands-on workshops for security teams. • Hands-on training programs to upskill cyber security teams in implementing and managing PQC solutions effectively. • Training of our crypto team and how best to go about implementing various technologies.

Type of support	Answers from survey respondents
	• Enhance technical expertise to provide security staff with in-depth knowledge of PQC principles, algorithms, and implementation of best practices. • Technical training for security staff, crucial to ensure they can handle emerging threats effectively. • Provide technical training to enhance the work culture. • Technical instruction on post-quantum encryption methods. • Technical training for security staff is crucial. We need training on PQC implementation and integration with existing systems. This will ensure our security team can effectively deploy and manage PQC solutions. • Training that covers the integration of PQC into our existing security infrastructure, including firewalls and VPNs, is essential. • Conduct workshops on PQC implementation. • Cover PQC algorithm implementation. • Build in-house PQC expertise to lessen dependence on third-party vendors. • Improve the capacity to address cryptographic breaches as they occur. • Enhance responses to cyber risks. • Hands-on training covering PQC integration with existing systems, ideally with certification options. • Practical workshops, certification courses, and real-life case studies on PQC.
Awareness training for management and security staff	• Real-world examples tailored to energy sector threats. • Most helpful support would be developing customised training modules that cater to the specific needs and roles of management and security staff, focusing on telecoms-specific use cases and scenarios. • Executive training for employees. • Awareness training for management helps align security priorities and fosters a proactive culture. • Empower workforce with interactive PQC training solutions. • Training to use survey tools effectively. • Certification programs for PQC security expertise. • Make staff more aware of upcoming technologies • Equip security teams with the knowledge to successfully implement PQC migration. • Ensure everyone understands the value of PQC and their role in its implementation. • Provide government-funded consultancy for businesses new to PQC.

Type of support	Answers from survey respondents
List of government-accredited PQC suppliers and experts	• Easy access to guidance on PQC compliance would help companies transition smoothly without unnecessary roadblocks. • Enhance quality by collaborating with compliant PQC suppliers. • Provide a structured roadmap to streamline the PQC adoption process. • Reliable, vetted local partners. • Vetted reliable partners for our specific needs. • Provide reliable suppliers and minimise risks. • Ensure supply chain security. • Partnering with accredited suppliers is essential for secure and compliant cryptographic implementations. • Working with government-accredited suppliers and experts equips organisations with the tools and knowledge they need. • Specialising in cyber security for government agencies companies offers comprehensive PQC solutions. • Partners who understand our local challenges. • It would be great to have a clear, searchable database. Time is always a factor, and this would save us a lot of initial research. • Searchable database with healthcare-specific profiles and peer reviews would be most valuable. • A centralised and updated database of approved PQC vendors and service providers for reliable solutions. • Tailorable assessment tools that can be adapted to our specific logistics environment and needs. • Centre for Development of Telematics.
Maturity or readiness assessments for PQC	• Tools to evaluate preparedness and prioritise migration steps. • Readiness checks for smooth transition. • Tools or frameworks to evaluate current cryptographic systems and identify gaps. • Provide tools or frameworks to evaluate our current cryptographic systems and identify gaps in quantum readiness. • Support in evaluating current cryptographic systems and identifying gaps to prepare for PQC migration. • Assessments to identify gaps and improve PQC readiness. • A framework to evaluate risk infrastructure and compliance for assessing readiness for PQC implementation. • Tailorable assessment tools that can be adapted to our specific logistics environment and needs. • Develop a phased roadmap based on assessment findings.

Type of support	Answers from survey respondents
	• A clear, actionable report detailing our current gaps and vulnerabilities would be most helpful. We need to know where to focus our efforts. • I would need a clear report outlining gaps, focusing on NCSC alignment, and benchmarking against UK peers. • Clear reporting and recommendations. • Identify gaps in our infrastructure, processes, and staff expertise, allowing us to create a tailored roadmap for PQC implementation. • Identify vulnerabilities in current cryptosystems. • Assess gaps and guide organisations in migration planning. • Use survey tools effectively. • Being able to provide a PQC pack to commercial customers would allow greater understanding of the issues relating to PQC and quantum in general. • Support best practices and regulatory compliance. • Host a PQC innovation challenge with funding for winning solutions.
Up-to-date advice on specific cryptographic protocols relevant for PQC	• Clear standards on PQC algorithms and secure implementation. • Regular updates on PQC standards. • Regular updates on cryptographic protocols ensure our systems are ready for post-quantum challenges. • Regularly updated standards and recommendations for secure PQC adoption. • Regular updates on PQC standards to ensure secure adoption. • A government-backed list of recommended PQC protocols would help reduce uncertainty. • Security benchmarks for evaluating PQC encryption strength. • Process manual. • Clear, actionable guidance on which PQC algorithms and protocols to adopt, tailored to industry needs. • Cut through the jargon, give us direct action points. • Expert guidance would enable us to make informed decisions, ensuring the seamless integration of PQC solutions into our logistics services. • Data-driven solutions for superior quality. • Test frameworks for new algorithms. • Reduce risks of outdated encryption. • Hands-on workshops for practical PQC adoption. • Access to expert cryptographers, protocol-specific guidance, and implementation best practices. • Integrate security training as a requirement for IT staff promotions. • Save us time researching - help us know what everyone else is aiming for.

Type of support	Answers from survey respondents
Guidance on how to approach cryptographic upgrades for PQC	• Practical and step-by-step roadmap for seamless transition. • Clear, practical steps tailored to our systems. • Step-by-step guidance, focused on our critical infrastructure. • A step-by-step guide tailored to healthcare systems would be invaluable. We have specific regulatory requirements to consider. • Clear migration roadmaps to transition without business disruption. • Clear migration roadmap with risk assessment. • Publish step-by-step guides or best practices tailored to industries like transport and logistics to simplify migration planning. • Test PQC algorithms in controlled environments before roll-out. • Hybrid cryptography for phased PQC implementation. • Plans for industry-specific PQC adoption. • Technical whitepapers on integrating PQC into existing infrastructure. • Share risk assessments and mitigation strategies. • Identify public-key cryptography methods (e.g. RSA) that are susceptible to quantum attacks. • Spot long-term data that requires quantum-safe encryption now, such as government records and financial information. • Keep track of the upcoming phases of NIST's PQC selection process. • Implement clear regulatory expectations to avoid non-compliance issues. • Budgeting guidelines for PQC transition costs. • Ensure government contracts include funds for PQC upgrades. • Phased approach required to ensure smooth transition along with maintenance of security.
Mandating accredited PQC as a condition of bidding for new government-funded projects	• Saving money while enhancing quality feels like a win-win situation. • Mandatory PQC audits for bidders. This would ensure higher security standards in critical infrastructure projects. • Improve compliance with regulatory requirements. • Enforce compliance with recognised PQC standards. • Promote widespread adoption and enforce security consistency. • Establish clear guidelines and standards for accredited PQC solutions, aligned with telecoms industry standards and regulations. • Policy and regulatory support. • Support for building a business case helps justify the investment and align it with organisational goals. • This would ensure that our organisation and partners adhere to the highest security standards, protecting sensitive data and maintaining the integrity of our logistics services.

Type of support	Answers from survey respondents
Grants for small-medium enterprises to pursue security improvements (including PQC migration)	• Use survey tools effectively. • Financial support would be crucial for SMEs, as security upgrades can be costly. • Financial assistance would enable us to invest in new hardware and software that supports PQC, ensuring our systems are secure and compliant with emerging standards. • Tax incentives for security investments. • Easy-to-understand documentation outlining the requirements and qualifications for grant applications. • Encourage industry partnerships to subsidise PQC implementation costs. • It would be instrumental in supporting our organisation transition to PQC. Financial assistance would enable us to upgrade our infrastructure, invest in PQC solutions, and ensure the security of our logistics services. • As a financial institution, supporting our enterprise customers with a public-private wrapper on PQC would help us drive a future-looking improvement in cryptology across our large commercial customer base.
Support for developing a clear business case or cost-benefit analysis for PQC migration	• Budget allocation for implementation. • Post-implementation maintenance and support. • Practical cost-benefit insights. • Cost-benefit analysis. • Regulatory compliance benefiting from cost analysis. • ROI-focused reports on PQC implementation. • Business case templates, cost estimation guidance, benefit identification, and ROI analysis. • Offer templates, case studies, or financial models to help justify PQC migration to stakeholders. • Help in identifying critical assets that justify PQC investment. • Guidance on how to raise the priority against other threats perceived as more imminent. • By receiving support for developing a clear business case, we can make informed decisions about PQC migration, prioritise resource allocation, and ensure that our security investments align with our organisational goals. • Template or framework that demonstrates the ROI of PQC, especially in mitigating potential data breaches, would be very useful. • Templates or guidelines to justify investment and prioritise PQC migration. • Organise cross-industry training sessions for knowledge sharing. • Tax breaks would motivate organisations to allocate resources towards post-quantum readiness.

Type of support	Answers from survey respondents
Tax incentives for spending on PQC upgrades	• Reduce taxable income with PQC hardware upgrades. • The cost of crypto agility is high and being able to have a tax incentive will aid prioritisation. • Monitor policy updates for new PQC-related tax incentives. • A simple breakdown of eligible expenses would be helpful. Navigating tax codes can be confusing, and we need clarity. • Establish clear eligibility criteria for tax incentives; ensure that telecoms organisations understand the requirements and can plan accordingly. • Tax benefits would accelerate adoption by offsetting initial implementation expenses. • Encourage faster upgrades with less cost. • Align corporate priorities with national security and compliance requirements.

5. Conclusions and recommendations

The overall picture for PQC migration is one of a problem that is perceived by UK critical national infrastructure players as significant, but not yet a high priority for investment. The following recommendations focus on how government and regulators can help raise the profile of the problem and address some of the most critical barriers to progress. Please note that these recommendations are based on the authors' views, which have in turn been informed by input and feedback from the interviews, and have also taken into account the findings of the survey. Where relevant, we have indicated where a given recommendation was directly suggested by interviewees.

5.1 Recommendations for government and regulators

1. **Address uncertainty around PQC timelines, by collating and sharing informed estimates for the Q-Day (timeframe for a likely quantum-enabled attack) for commonly-used cryptographic algorithms.**

Uncertainty around when a cryptographically relevant quantum computer will emerge (see Figure 2.5) is significant, and makes planning difficult. Any estimate of when quantum computers will become cryptographically relevant is challenging, as it relies on speculations about an extremely complex and fast-moving technology. Collating estimates from professional bodies and academic reports would, at a minimum, provide organisations with the resources they need to identify a timeline that they have confidence in.

2. **Develop and disseminate a clear, single source of guidance for PQC migration – this could be provided at a central level by the NCSC, but also needs a clear sector-level overlay to address the specific context and complexities of each CNI sector**

Resources on the threat should be pulled into a clear guidance document for industry, that brings together some of the separate NCSC reports and other strategies into a single reference document. This should emphasise the importance of cryptography for achieving organisational goals, the need to invest to protect information from quantum computers, and the business case for PQC migration. More sector-specific step-by-step guides to PQC migration would also be useful.

3. **Produce guidance and disseminate information specifically targeted at board members and other senior management-level stakeholders.**

This should emphasise the importance of cryptography for achieving organisational goals, the need to invest to protect information from quantum computers, and the business case for PQC migration. Many of the barriers to adoption highlighted in the interviews and survey are rooted in difficulties articulating the cost-benefit analysis to economic stakeholders (see Figure 4.36). These challenges include prioritising spend, cost concerns, lack of a business case, and prioritisation of other cyber security threats over PQC. Previous efforts to engage with industry have focused on technical specialists, but as an organisational issue, advice should also be targeted at senior leaders.

4. **Work with industry and academia to develop training for organisations looking to upskill their staff. Couple this with development of a formal register or certification, to allow industry to recognise quality support.**

The most frequently cited barrier to migration (see Figure 4.36) was the skills gap. Unsurprisingly, this was accompanies by several explicit requests from organisations we interviewed, for support to overcome this barrier. Specific asks included technical training, guidance on PQC upgrades, and accreditation schemes (see Figure 4.43).

5. **Publish a list of intensive training courses that can get technical employees up to speed on PQC and cryptographic migration.**

The most frequently cited barrier to migration is the skills gap (see Figure 4.36). The estimated timescales for the emergence of cryptographically relevant quantum computers mean that long-term skill creation strategies (such as the creation of degree-level courses, or embedding cryptographic skills into existing degree programs) may not move fast enough to filter through to the organisations that need those skills (though ensuring that the UK has access to those skills in general should certainly be considered, as they are extremely valuable.) Professional certifications and dedicated short courses may be more appropriate, if industry is able to find the funds to pay for them. Professionals who would benefit from a deeper understanding of cryptography include IT security leads, secure software developers and architects. Smaller organisations that do not have a consistent need for cryptography skills may consider teaming with consultants and academics; the NCSC's proposal to establish a PQC Consultant Accreditation Scheme should support those stakeholders.

6. **Establish a network of PQC working groups, at a cross-sector and sector-specific level. The groups should involve academia, government or regulators, industry and standards bodies. These should share best practice and encourage collaboration on PQC migration.**

Our interviewees highlighted this as a key area where government could help. In energy, finance, and telecoms, interview respondents mentioned the benefits of collaborative groups who explored issues around PQC, shared best practice, and where appropriate, produced standards. This is particularly important for sectors where inter-organisational communication is critical to the success of the sector, meaning that no single organisation can fully migrate in isolation. Similarly, regulators called for PQC groups to help with the collection and dissemination of information about the quantum threat. Standards bodies should be invited to participate in these working groups to ensure that standardisation can be documented and shared where valuable. Sectors that appear to be ahead of the curve, such as energy, finance, and telecoms, should be encouraged to share challenges and solutions. Opportunities to learn from specialists in other countries that are proactively tackling this problem (such as the US, Singapore, and South Korea) should also be harnessed.

7. **Ensure that the need for quantum-safe products is clearly articulated as an opportunity for technical suppliers, and help to drive development of a vendor ecosystem.**

Most businesses will be highly reliant on the technology supply chain to support their PQC migration. The majority of their cryptographic material is managed by software-as-a-service vendors, or by smaller software suppliers (including suppliers of cyber physical systems such as PLCs or other low-level controllers and sensing devices). Actively managing the migration to PQC requires working with software suppliers to ensure that their strategy will deliver quantum-safe solutions, in a timeline that works.

One possible activity for government and/or regulators could be providing opportunities for the supply chain to engage in PQC forums or events. Another could be providing estimates of addressable PQC market size for organisations selling PQC-ready equipment and software, to encourage development of an ecosystem of quantum-safe suppliers. Government can also support end user organisations that need to actively manage their software supply chain – for example by providing guidelines on setting goals for their suppliers and monitoring progress.

8. **Provide guidance and advice on scoping exactly what activities will be required for PQC migration.**

This should include identifying what skills and resources those activities need, and advising on how to judge the scale of the investment required. Expected migration timelines should be presented alongside the estimated timeframe for a cryptographically relevant quantum computer to emerge. Regulators are in a strong position to contextualise this advice, and ensure that sector-specific considerations are reflected in their dissemination of this information.

An effective PQC migration may be a multi-year effort, requiring funding and management throughout. The most effective strategy to reduce total cost of ownership is one that targets exactly which assets require attention (i.e. understanding where cryptography is used, avoiding systems that do not use quantum-vulnerable cryptography, and prioritising algorithms that are the most vulnerable) and works to a timescale that avoids expensive reactive upgrades in response to the emergence of practical, quantum-enabled attacks. This needs careful planning and estimation. Balancing asset lifetime against the estimated emergence of a cryptographically relevant quantum computer is in line with advice from Mosca's Inequality Theorem [38].

9. **Highlight the risks associated with adopting PQC, as well as the risks of not adopting it, so that organisations can make informed choices and manage risks appropriately**.

Much of the technical advice available to industry encourages organisations to identify where their cryptographic assets are. This entails understanding the software assets that implement cryptography, the location and ownership of keys, and the location and ownership of digital certificates. But whilst this is a good first step, it is not sufficient by itself. Organisations should also build an understanding of the purpose of the cryptography in context, and explicitly record constraints that could be broken by injudicious deployment of PQC algorithms. Factors to consider include usability (i.e. could the PQC implementation introduce unacceptable delay?), control stability (i.e. could the PQC implementation introduce latency or increase network traffic to unacceptable levels for controllers?) and scalability (i.e. could the storage of longer signatures or the additional data transfer required per handshake introduce technical performance issues in the system?). Selecting the incorrect algorithm for a given task (e.g. trying to use a signature to protect the confidentiality of a message) is also to be avoided. NCSC has already released some guidance on when to use different algorithm types.

10. **Build a communications and dissemination plan to reach out to the wider ecosystem in order to achieve the above objectives**

Migrating to PQC is not a challenge that can be wholly tackled by government. Private investment and expertise are essential to making progress. But government has an opportunity to bring key players together, inform strategy, and prevent expensive rework.

11. **Consider when and how best to take specific regulatory action to mandate PQC migration (e.g., by a certain date).**

While this may seem an obvious way to drive migration, the research conducted for this study indicates that most UK CNI organisations are still far from ready to start on the journey. Given the complexities of planning for and deploying PQC, industry interviewees – who contributed several of the above recommendations – indicated that it would be valuable to action some of the suggestions above, prior to taking regulatory action. Several interviewees also emphasised the importance of developing policy and regulation on PQC collaboratively with regulated organisations, to ensure that regulations are practical and achievable. This desire was echoed by regulators themselves, who felt that they were in a good position to translate high-level PQC guidance from the NCSC and government into the language of their stakeholders, and to provide relevant sector-specific context.

6. References

[1] NIST, "NIST releases first 3 finalized Post-Quantum Encryption standards," Aug 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[2] Capgemini, "TechnoVision: Top 5 Tech Trends to Watch in 2025," Nov 2024. [Online]. Available: https://www.capgemini.com/news/press-releases/technovision-top-5-tech-trends-to-watch-in-2025/.

[3] Capgemini, "Y2Q: A journey to quantum safe cryptography," 2023. [Online]. Available: https://prod.ucwe.capgemini.com/wp-content/uploads/2023/10/D38710-2023-Quantum-Projects-ODS-Support-October-2023-v3.pdf.

[4] NIST, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," Apr 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf.

[5] Capgemini, "New quantum safe cryptographic standards future proofing financial security in the quantum age," Sep 2024. [Online]. Available: https://www.capgemini.com/insights/expert-perspectives/new-quantum-safe-cryptographic-standards-future-proofing-financial-security-in-the-quantum-age/.

[6] H. Ma, S. Pan, Y. Gao, J. He, Y. Zhao and Y. Jin, "Vulnerable PQC against Side Channel Analysis - A Case Study on Kyber," in *2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2022.

[7] NIST, "Intro to Side-chanel security of NIST PQC standards," 2023. [Online]. Available: https://www.nist.gov/video/intro-side-channel-security-nist-pqc-standards.

[8] Europol, "Quantum Safe Financial Forum," May 2024. [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff.

[9] Q. S. F. Forum, "A call to action," Feb 2025. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf.

[10] B. f. I. Settlements, "Project Leap: Quantum-proofing the financial system," Jan 2024. [Online]. Available: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.

[11] E. P. A. Asia, "EPAA Press Release WG-QSC," Apr 2024. [Online]. Available: https://emergingpaymentsasia.org/wp-content/uploads/2024/04/25-April-EPAA-Press-Release-WG-QSC.pdf.

[12] HSBC, "HSBC pilots quantum-safe technology for tokenised gold," Sep 2024. [Online]. Available: https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc-pilots-quantum-safe-technology-for-tokenised-gold.

[13] Vodafone, "GSMA, IBM and Vodafone establish Post-Quantum Telco Network Taskforce," Sep 2022. [Online]. Available: https://www.vodafone.com/news/technology/post-quantum-telco-network-taskforce.

[14] A. Quantum, "Ampliphae, HPE Athonet and Arqit deliver Quantum-Safe Private 5G using Symmetric Key Agreement," Jan 2024. [Online]. Available: https://arqit.uk/press-releases/ampliphae-hpe-athonet-and-arqit-deliver-quantum-safe-private-5g-using-symmetric-key-agreement?utm_source=substack&utm_medium=email.

[15] Vodafone, "Vodafone tests Quantum-safe business network with upgraded smartphones," Jul 2023. [Online]. Available: https://www.vodafone.com/news/technology/vodafone-tests-quantum-safe-business-network-upgraded-smartphones.

[16] C. Consultants, "Energy network security for the good of society in a post-quantum world," Apr 2024. [Online]. Available: https://www.cambridgeconsultants.com/societal-energy-network-security-in-a-post-quantum-world/.

[17] N. C. S. C. (UK), "Preparing for Quantum-Safe Cryptography," Nov 2020. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

[18] N. C. S. C. (UK), "Next steps in preparing for post-quantum cryptography," Aug 2024. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.

[19] U. National Cyber Security Centre, "Post-quantum cryptography, NCSC Annual Review 2024," Dec 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-04/post-quantum-cryptography.

[20] U. N. C. S. Centre, "Timelines for migration to post-quantum cryptography," Mar 2025. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[21] U. National Cyber Security Center, "Market incentives and the future of technology security, NCSC Annual Review 2024," Dec 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-03/market-incentives.

[22] N. S. Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," Sep 2022. [Online]. Available: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

[23] U. Congress, "Quantum Computing Cybersecurity Preparedness Act," Dec 2022. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/7535/text.

[24] G. o. Canada, "Preparing your organization for the quantum threat to cryptography," Jan 2025. [Online]. Available: https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.

[25] E. Commission, "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography," Apr 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[26] F. O. f. I. S. Germany, "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography," Dec 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3.

[27] G. Federal Office for Information Security, "Quantum-safe cryptography – Fundamentals, Current developments and Recommendations," May 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6.

[28] F. C. A. (ANSSI), "ANSSI views on the Post-Quantum Cryptography transition," Dec 2023. [Online]. Available: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.

[29] T. a. C. W. &. Informatica, “PQChoiceAssistant,” [Online]. Available: https://tno.github.io/PQChoiceAssistant/.

[30] C. A. a. N. O. f. A. S. R. Unit Weerbaarheid, “The PQC Migration Handbook,” Dec 2024. [Online]. Available: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf.

[31] K. P.-Q. Cryptography, “SMAUG-T & HAETAE,” Jan 2025. [Online]. Available: https://kpqc.cryptolab.co.kr/.

[32] M. A. o. Singapore, “Advisory on addressing the cybersecurity risks associated with Quantum,” Feb 2024. [Online]. Available: https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf.

[33] A. S. Directorate, “Guidelines for cryptography,” Dec 2024. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography.

[34] Gartner, “Begin Transitioning to Post-Quantum Cryptography Now,” 2024. [Online]. Available: https://www.gartner.com/en/articles/post-quantum-cryptography.

[35] Global Risk Institute, “Quantum Threat Timeline Report 2024,” Global Risk Institute, 2024.

[36] B. Flyvbjerg and A. Budzier, “Why Your IT Project May Be Riskier Than You Think,” Harvard Business Review, 2011.

[37] C. M. &. S. Department for Digital, “Telecommunications Security Code of Practice,” 2022. [Online]. Available: https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf.

[38] M. Mosca, “Cybersecurity in an era with quantum computers: will we be ready?,” *Cryptography ePrint Archive,* 2015.

[39] Capgemini, “Top tech trends of 2025,” Jan 2025. [Online]. Available: https://www.capgemini.com/wp-content/uploads/2025/02/Top-Tech-Trends-2025_Report_v7.pdf.

[40] C. R. Institute, “Quantum technologies: How to prepare your organization for a quantum advantage now,” Apr 2022. [Online]. Available: https://www.capgemini.com/wp-content/uploads/2022/04/Final-Web-Version-Quantum-Technologies.pdf.

[41] NIST, “What Is Post-Quantum Cryptography?,” Dec 2024. [Online]. Available: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.

[42] NIST, “Module-lattice-based key-encapsulation mechanism standard,” Aug 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf.

[43] NIST, “Module-Lattice-Based Digital Signature Standard,” Aug 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf.

[44] NIST, “Stateless Hash-Based Digital Signature,” Aug 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf.

[45] M. Mosca, “Cybersecurity in an era with quantum computers: will we be ready?,” 2015. [Online]. Available: https://eprint.iacr.org/2015/1075.pdf.

[46] NIST, “Report on Post-Quantum Cryptography,” Apr 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.

[47] Capgemini, “How should organizations respond to NIST’s announcement of the first batch of quantum-resistant cryptographic algorithms?,” Sep 2022. [Online]. Available: https://www.capgemini.com/us-en/insights/expert-perspectives/how-should-organizations-respond-to-nists-announcement-of-the-first-batch-of-quantum-resistant-cryptographic-algorithms/.

[48] N. c. s. c. (NCSC), “Cyber chiefs unveil new roadmap for post-quantum cryptography migration,” 2025. [Online]. Available: https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled.

Appendices

Appendix A: *Terms and definitions*

Table A. 1. Terms and definitions used in this report for quantum technology analysis

Term	Definition
Quantum computer	The term “quantum computer” describes a collection of technologies that use principles of quantum mechanics to store and process information.
Cryptographically relevant quantum computer	For a quantum computer to be “cryptographically relevant” it must be able to undermine the security of cryptographic functions such as encryption, hashing, or digitally signing data for relevant key sizes. In the case of asymmetric encryption, the quantum computer must be capable of calculating the private key from a public key, for key lengths that are in common use.
Quantum algorithm	A quantum algorithm is a description of a process to be run on a quantum computer that tackles a specific problem.
Qubit	The most basic unit of information representation within a quantum computer. Similar to the binary digit (or “bit”) in a classical computer, except it is capable of being in a state of superposition representing both 0 and 1 at the same time.
Quantum error correction	Quantum error correction is a collection of techniques that focus on restoring the representation of information in a quantum computer to a desired state after it has been perturbed away from that state by unwanted physical effects in the system. This contrasts with other attempts to make quantum computers more resilient, such as efforts to prevent the errors from occurring in the first place. Quantum error correction plays a significant role in the journey towards a cryptographically relevant quantum computer, as common techniques such as qubit redundancy (aggregating multiple physical qubits to represent a single "logical qubit") impair efforts to build quantum computers at scale.
Q-Day	For a given cryptographic algorithm, and key length, Q-Day is the date when a cryptographically relevant quantum computer becomes available to an adversary.
‘Harvest-now-decrypt-later’ attack	A strategy where attackers collect and store encrypted data now, with the intention of decrypting it in the future when more advanced decryption technologies, such as quantum computing, become available. This approach poses a significant threat because any system using traditional asymmetric cryptography to transmit data that will still be of tactical relevance to an attacker in several years’ time, can be intercepted now. This vulnerability remains until PQC migration is complete.
Digital certificates	A digital certificate is an electronic document used to prove the authenticity of a user, device, server, or website. It leverages Public Key Infrastructure (PKI) to securely exchange data over the internet. Digital certificates contain a public key and the identity of the certificate holder, and they are issued by trusted third parties known as Certificate Authorities (CAs). These certificates enable secure communication by allowing two parties to trust each other's identities, with the CA vouching for them.

Post-quantum certificates	Post-quantum certificates are digital certificates designed to be secure against the potential threats posed by quantum computers. These certificates use cryptographic algorithms that are resistant to quantum attacks, ensuring that the data they protect remains secure even if quantum computers become capable of breaking current encryption methods.

Table A. 2. List of acronyms

Acronym	Definition
AIVD	General Intelligence and Security Service (The Netherlands)
ANSI	American National Standards Institute
ANSSI	French Cyber security Agency
AP+	Asia Pacific Plus
ASD	Australian Signals Directorate
BSI	Federal Office of Information Security (Germany)
CAF	Cyber Assessment Framework
CCN	National Cryptology Center (Spain)
CISA	Cyber security and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMMC	Cyber security Maturity Model Certification
CNI	Critical National Infrastructure
CNSA	Commercial National Security Algorithm
CSA	Cyber security Advisory
CTO	Chief Technology Officer
CWI	Centrum Wiskunde & Informatica (The Netherlands)
DSIT	Department for Science, Innovation and Technology
EC3	European Cybercrime Centre
ESO	Electricity System Operator
ETSI	European Telecommunications Standards Institute

FIPS	Federal Information Processing Standards
GCHQ	Government Communications Headquarters
HAETAE	Hybrid Algorithm for Elliptic Curve and Traditional Encryption
HNDL	Harvest-now-decrypt-later
IP	Intellectual Property
IT/OT	Information Technology/Operational Technology
KpqC	Korean Post-Quantum Cryptography
ML-DSA	Module-Lattice Digital Signature Algorithm
ML-KEM	Module-Lattice Key Encapsulation Mechanism
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NQCC	National Quantum Computing Centre
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QSFF	Quantum Safe Financial Forum
RFC	Request for Comments
RoI	Return on Investment
RSA	Rivest-Shamir-Adleman
SMAUG-T	Secure Modular Arithmetic for Universal Group-Theoretic Transformations
SME	Small and Medium-sized Enterprises
TNO	Dutch Organization for Applied Scientific Research
UKRI	UK Research and Innovation
UN	United Nations

VCs	Venture Capitalists
VP	Vice President
VPN	Virtual Private Network

Table A. 3. Terms and definitions used in this report for analysis and discussion of interviews and survey responses

Term	Definition
Sector	Industry sectors covered in this report are **energy, transport, healthcare, telecoms, and finance**.
Organisation type	**'Industry practitioners'** – refers to companies from the five target sectors that are end-users of cyber security for critical national infrastructure. '**Regulators'** refers to organisations that enforce and implement policies and regulations for their sector for their sector, but which do not belong to a government agency. '**Academia'** refers to universities and research centres with experts in quantum computing, post-quantum cryptography, etc.
Interview type	We categorised an interviewee or survey respondent's 'interview type' as '**End User'** (if they primarily offered views of cyber security and PQC approaches in their own organisation), or '**Ecosystem**' (if they primarily offered views about their sector or the wider UK – i.e. regulators, academia). The questions asked to these two groups varied slightly, to capture the different viewpoints of end-users/practitioners and respondents who could take a broader view of the market. Note that these two categories have some overlap. Specifically, some End User organisation interviewees were unable or unwilling to comment on their own organisation's PQC approach or strategy; in such cases we incorporated their responses into Ecosystem view analyses. Some interviewees shared views on both their own organisation and their sector or the wider UK 'Ecosystem'.
Interviewee role	We categorised interviewees as either **'Technical**' or '**Managerial**', depending on the nature of their role and level of technical expertise. The interview questions asked to these two groups varied slightly; specifically, we did not ask detailed technical questions to the Managerial interviewees.
Interviewee job title	**'CISO'** refers to interviewees that have a technical role at a board level. It includes CISOs and CTOs. **'Head of department'** refers to directors, people with direct influence over their organisation's cyber security or budget holders in the cyber security space. It does not include people from the executive board. **'Cyber security expert'** refers to interviewees with deep technical expertise on cyber security because they are closer to implementation than strategy. **'Advisor'** refers to interviewees that focus on high-level cyber security aspects and provide advice to their own or other organisations. **'Professor'** refers to academic interviewees.

Appendix B: *Supporting technical information*

Quantum computing and its use cases

Quantum computers are based on the principles of quantum physics, utilising superposition, entanglement, and interference to address complex computational problems. The fundamental unit of quantum computing is the qubit (quantum bit), which differs from a classical bit. Unlike a classical bit, which exists exclusively in the state of binary “0” or “1”, a qubit can exist in a quantum state of “0”, “1”, or a superposition of states “0” and “1” – i.e. at the same time. Quantum computers leverage these phenomena to perform computations in a fundamentally different manner from classical computers. This results in a significant acceleration of computational processes, an increase in accuracy, and the ability to address problems that are unsolvable by classical computers.

Quantum computers have the potential to achieve exponential speed-ups for specific problem types, surpassing the capabilities of classical computers. The applications of quantum computing are extensive (see Figure 1), including areas such as drug simulation, material science, aerodynamic modelling, supply chain optimisation and financial modelling, among others. The application domains where quantum computers are anticipated to provide substantial value can be broadly categorised into three main areas: optimisation, simulation, and machine learning. A Capgemini report [39] highlighted that by 2030, quantum computing is expected to transform areas such as cryptography, drug discovery, and climate modelling.

Figure B. 1. Leading quantum computing use cases being tested by industry

Financial Services	Life Sciences	Chemicals	Aerospace	Automotive
• Risk management • Dynamic portfolio management • Derivatives pricing • Fraud detection	• Biological target identification • Compound lead identification and optimization • Drug target interactions • Disease diagnosis • Clinical trial optimization	• Modelling and optimization of chemical reactions • Battery manufacturing • Molecular simulation and discovery	• Air traffic control • Airplane design optimization • Optimize fleet, crew, fuel, etc. • Cargo loading optimization • Supply chain optimization	• Traffic flow management • Car design optimization • Crash simulation • Battery manufacturing • Industrial efficiency • Supply chain optimization

Source: Capgemini Research Institute [40]

Shortcomings of classical cryptography

Current cryptographic algorithms provide the necessary security based on the complexity of certain mathematical problems (such as integer prime factorisation, which is practically infeasible for classical computers to solve). However, a sufficiently advanced quantum computer using Shor’s algorithm could perform this factorisation within hours. This capability poses a significant threat to asymmetric public key cryptographic systems, such as RSA (named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman) and Elliptic Curve Cryptography (ECC), which are integral to securing communications and digital signature applications. Additionally, Grover’s algorithm, another quantum algorithm, could potentially compromise symmetric key cryptographic systems like Advanced Encryption Standard (AES), which is crucial for protecting sensitive data.

While classical cryptography depends on the difficulty of integer factorisation or discrete logarithms, post-quantum cryptography relies on problems like lattice-based, hash-based, and multivariate polynomial equations that are tough even for quantum computers to solve.

‘Harvest-now-decrypt-later’ attacks

Organisations with data having a longer shelf life are vulnerable to ‘harvest-now-decrypt-later’ (HNDL) [41] attacks where threat actors can access currently encrypted data and then decrypt it later when they have access to powerful quantum computers. Such data include personally identifiable information, industrial trade secrets, personal health information, and sensitive justice system information. With the aid of quantum computing technology, cybercriminals could potentially decrypt private keys, allowing them to create or manipulate digital documents along with their digital signatures. This could involve a variety of sensitive information, including audit records and legal documents that depend on encrypted messaging.

This potential threat requires the adoption of post-quantum cryptography (PQC), whose algorithms are designed using classical methodologies, and are expected to withstand quantum attacks and integrate into existing infrastructures without needing specialised hardware.

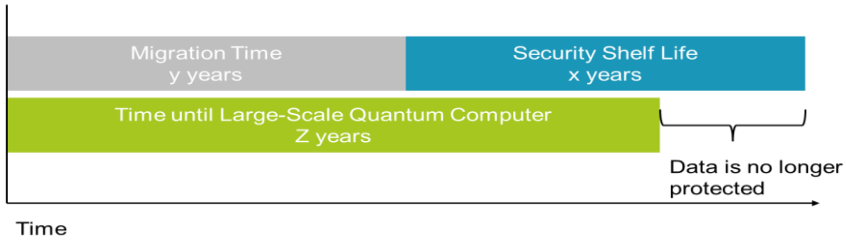
Impact of quantum computers on encryption protocols

- **Asymmetric cryptography no longer secure:** Asymmetric algorithms such as Diffie-Hellman (Merkel), Rivest, Shamir, Adleman (RSA), and Elliptic Curve Cryptography (ECC) are used in HTTPS, PKI, digital signatures, Wi-Fi protection, smartcards, hardware tokens, banking networks, cryptocurrencies, and most VPNs. Shor’s algorithm (and its variants) is a quantum algorithm that can potentially solve mathematical problems in a matter of hours that were thought to be computationally infeasible on traditional computers. These include problems whose complexity is a core assumption of asymmetric cryptography, as they allow the private key (the key that is used to decrypt messages) to be calculated from the public key (the key that is shared so others can encrypt messages). This means that a large-scale quantum computer capable of running Shor’s algorithm is likely to break traditional asymmetric cryptography used for encryption and digital signatures. Preparing early is crucial, as post-quantum validation technology needs to be implemented in advance.
- **Symmetric cryptography weakened:** Quantum computers are expected to weaken traditional symmetric encryption as well. Using Grover's algorithm, a brute force attack on AES-128 could be performed in as little as 2^{64} operations. This reduces AES-128's security to be equivalent to that of a 64-bit key today. AES 256 is considered secure, since even with quantum computers, performing 2^{128} operations to break ciphers is not feasible at present.
- **Hash functions are weakened:** Grover’s algorithm also theoretically speeds up the generation of “hash collisions” (identifying an input value that produces the same output as a legitimate input value). As a result, longer hashes that increase the number of output possibilities are recommended.
- **Asymmetric is the most pressing challenge:** The problems posed by Shor’s algorithm to asymmetric cryptography are far more serious [3, 4] than the minor speed-ups for brute force attacks offered by Grover’s algorithm against symmetric cryptography and hash functions.

Assessing the threat

To assess the threat that quantum computers pose on systems, products, and applications, Michele Mosca’s theorem (see below) can be used.

Figure B. 2. Michele Mosca's theorem to assess the quantum threat



If the time data must stay secure (x) and the time to upgrade to cryptographic systems that are quantum-safe (y) exceeds the time before quantum computers can break cryptography (z), then organisations will not be able to protect their assets against quantum attacks for the years required. The purpose of the theorem is to provide an estimate of how much time organisations need to transition to quantum-safe security protocols.

The Y2Q cyber security threat

The Y2K (Year 2000) bug, also known as the Millennium bug, stemmed from the practice of using two-digit year formats in computer programs to save memory. As the year 2000 approached, this created fears of widespread system failures, prompting global efforts to update software. Similarly, the Y2Q (year to quantum) problem refers to the potential threat posed by quantum computers, which could break current cryptographic systems and wreak havoc on government and enterprise security.

Both Y2K and Y2Q have similarities due to their potential global impact on computing and communication systems. Also for both, the technical complexity of the problems means that there is uncertainty around the level of impact that could manifest, and a need for skilled engineers to implement a resolution. But the differences between Y2Q and Y2K are more significant. Y2K had a definitive deadline and an internal problem with a one-time fix, whereas Y2Q's threat from quantum computers is uncertain, external, and requires ongoing analysis and upgrades based on system vulnerabilities and data criticality. Y2K's potential damage was immediately noticeable, while Y2Q's impacts might be delayed and less visible.

Y2Q presents more uncertainties and greater complexity than Y2K, requiring long-term solutions. Standard bodies and private organisations are developing solutions to address the Y2Q problem, focusing on PQC and Quantum Key Distribution (QKD). Quantum key distribution is an application of quantum physics to enhance security.

NIST encryption standards

Three encryption standards were introduced by NIST in 2024 to resist quantum computer attacks:

- **ML-KEM** (modular lattice key encapsulation mechanism (FIPS 203) [42] based on CRYSTALS-Kyber): A general-purpose encryption suitable for securing data in transit across various applications.
- **ML-DSA** (modular lattice digital signature algorithm (FIPS 204) [43] based on CRYSTALS-Dilithium): A general-purpose lattice-based algorithm for general-purpose digital signature protocols.

  SLH-DSA (stateless hash-based digital signature algorithm (FIPS 205) [44] based on SPHINCS+): Designed for digital signatures based on a different mathematical approach than ML-DSA, primarily as a backup to ML-DSA.

Appendix C: *Interview methodology details*

We conducted 21 semi-structured interviews with a mix of industry end-users of cyber security and broader ecosystem players, including regulators from each of the target sectors. The breakdown of respondents is shown in Table C. 1:

Table C. 1 Number of interviews performed by sector and interview type

Sector	No. of end user interviews	No. of ecosystem interviews	No. of interviews that fitted both categories
Energy	2	0	1 (regulator)
Transport	2	0	1 (regulator)
Healthcare	2	0	1 (regulator)
Telecoms	1	2	1 (regulator)
Finance	2	0	1 (regulator)
Academia + industry association	0	5	0

C.1 Interview respondent recruitment approach and criteria

Interview targets were recruited through the professional networks of the Cambridge Consultants and Capgemini project team, as well as through referrals from DSIT. Potential interviewees were informed that they would be participating in a study conducted on behalf of DSIT, with the goal of understanding PQC awareness and readiness, migration drivers and blockers, and ideas on potentially useful support or interventions from government. Interviewees were told that participation would be anonymous, and that analysis would be conducted by sector.

We used the following criteria for recruiting interviewees:

1. Organisation location: Based in the UK, or with a UK branch large enough to require a UK-based IT/cyber security team.
2. Sector: Focus on CNI organisations across five market sectors: energy, healthcare, finance, telecoms, and transport. In addition, we reached out to cyber security ecosystem players (academics and relevant sector regulators).
3. Organisation type: Private and public companies, regulatory bodies, and academia. While regulators for the relevant sectors were explicitly targeted, other government bodies were out of scope (the NHS was, however, considered in scope for healthcare). Organisations needed to be either significant end-users of cyber security themselves, or important players in the overall quantum and/or cyber security ecosystem.
4. Candidate role: Senior-level role related to cyber security strategy or implementation, within their organisation or sector. For academics, their focus area needed to include quantum computers or post-quantum cryptography.
5. Organisation size: More than 250 employees. We judged it unlikely that smaller companies would currently be incorporating quantum threats into their short- and medium-term strategies, and therefore excluded them.

C.2 Interview methodology

Interviews were conducted via videocall. The length was 45-60 minutes.

We created two sets of guidance questions for the interview programme: one for industry end-users, and another for ecosystem stakeholders. The full set of questions can be found at the end of this Appendix. The questions for both groups are broadly similar, but take into account the broader perspective of the ecosystem players for that group, and conversely the specific insight on their own cyber security strategy that industry end-users could provide.

Each interview was conducted by a PQC expert from Cambridge Consultants or Capgemini, and a notetaker. Interviews were conducted using a semi-structured approach to enable open discussion and flow of conversation. Since the purpose of the interviews was to generate insight rather than to enable robust statistical analysis of responses, interviewers were free to mix the order of questions, to probe further on responses if appropriate, and to skip questions if respondents were unable to answer. For industry end-users, if the interviewee was classified as a 'managerial' rather than a technical respondent, then the more technical questions were skipped.

To facilitate the notetaking and analysis tasks, an automatic transcript was generated for each interview after the interviewee consented to it. Interviewees were told that this was solely for the purpose of ensuring clarity of notes and would not be shared more widely.

C.3 Interview analysis approach

We divided the analysis of the interviews into three different levels:

1. **Interview notes** – The note-taker of the interview summarised the different answers of the interview guide, anonymising the content but ensuring it reflected the interviewee's views.
2. **Sector analysis** – All the interview analysis was captured in the same document, which allowed for easy filtering and comparisons between interviewees of the same sector or profile. We included this analysis in Section 3 of this report.
3. **Overall analysis** – The different interview questions were aligned with the four objectives of this report. At this stage we distilled the main messages shared by the interviewees for each the overarching objectives, comparing between sectors and also contrasting with the survey insights. We captured this analysis in Section 2.

C.4 Interview questions

We used two sets of questions for the interviews, depending on the view shared by the interviewee. The first set of questions was for 'end-user' and the second one for 'ecosystem' stakeholders. The differences between the two sets were minimal to ensure subsequent comparison. Both sets had questions classified as 'Technical' or 'Both'. If the interviewee had a good level of technical knowledge, all the questions were considered. If the interviewee was not aware of the technical details, technical questions were excluded.

Based on our initial interviews, we proposed to adjust the original questions as follows:

1. Remove Q2[3] – Our interviewers felt this question was not providing any critical additional insight beyond what is already covered in other questions, and that all interviewees work for organisations where digital assets are extensive, so this question could be deleted.

[3] Original question 2: What role do digital assets [e.g. software and applications, data, websites] play in your organisation?

2. Remove Q6[4] – As the interviews were not conducted under NDA, this question was too specific for interviewees to feel comfortable answering it, and we did not feel it necessary for useful analysis of PQC strategies.
3. Add a new question (after the original Q5) to address barriers relating specifically to understanding the organisation's current security situation:
   a. "Are there any particular barriers that might make doing an inventory of cryptography challenging for your organisation?" [Prompt: e.g. software supply chains are complex or not known, our cyber security is managed by third party providers, etc.]
4. Rephrase Q11 to focus on the interviewee's knowledge of the types of attack that quantum computers can enable:
   a. Original question: "What type of security problems do you think your organisation could suffer if you were subjected to a quantum-enabled cyber attack? Do you have a good sense of which of these would be highest-risk or highest priority for you?"
   b. Updated question: "Are you aware of what types of cyber attacks quantum computers can enable, and/or which types of cryptography are most at risk?"

'End-user' Interview Questions

Table C. 1. Final set of questions used for 'end-user' interviews.

Area	No.	Respondent type	Pilot questions
1 – Role and organisation	Q1	Both	Can you please share some background on your department and role, as these relate to responsibility for your organisation's cyber security strategy?
1 – Role and organisation	Q2	Both	DELETED *
1 – Role and organisation	Q3	Technical	For how many years do you need to ensure that your digital assets are kept secure? Could you specify the type of assets?
2 – PQC Knowledge and awareness	Q4	Both	Are you familiar with any specific digital security/cyber security goals (or priorities) that your organisation has? If so, what are the most important ones?
2 – PQC Knowledge and awareness	Q5	Technical	Are you aware of the type(s) of cryptography your company uses for cyber security, and where? [prompt: asymmetric vs asymmetric; asymmetric authentication; RSA]
2 – PQC Knowledge and awareness	Q6	Both	Are there any particular barriers that might make doing an inventory of cryptography challenging for your organisation?

[4] Original question 6: What was your latest major IT upgrade? How long was the migration planned to last? How long did it actually take?

Area	No.	Respondent type	Pilot questions
2 – PQC Knowledge and awareness	Q7	Both	How do you think the risk posed by quantum computers compares to other cyber risks your organisation is managing today? Why?
2 – PQC Knowledge and awareness	Q8	Technical	How do you think the level of risk posed by quantum computers will change in 5-10-30 years' time in comparison to other cyber risks?
2 – PQC Knowledge and awareness	Q9	Both	How much do you know about the impact of quantum computing development on cyber security?
2 – PQC Knowledge and awareness	Q10	Both	Are you aware of any PQC advice or resources? If yes, Which ones?
2 – PQC Knowledge and awareness	Q11	Both	Are you aware of what types of cyber attacks quantum computers can enable, and/or which types of cryptography are most at risk?
2 – PQC Knowledge and awareness	Q12	Both	In your opinion, when do you think quantum computers would constitute a real threat and why?
2 – PQC Knowledge and awareness	Q13	Both	Has your organisation already started exploring or planning for using post-quantum cryptography (PQC)? • If yes, please specify: - Have you started your PQC migration journey? [If no, follow up] When do you expect to start? - What are your next steps? - How long do you think it will take you to migrate to PQC? - What is the expected level of effort required? - Which team(s) will be part of the migration? - Could you give the order of magnitude on the estimated total cost of the migration? - How much of a priority is this? • If no, - How soon would you expect to start planning? [prompt answer: 1 year, 3 years, 5+ years, unsure]

Area	No.	Respondent type	Pilot questions
3 – Migration drivers and incentives	Q14	Both	• If the organisation is already migrating - What are the main factors driving your organisation to start planning for or executing on your PQC migration? • If organisation is not migrating yet - In your opinion, what would be the most compelling reason or driver that would push your organisation to embark on a PQC migration?
4 – Blockers and barriers	Q15	Both	Are any particular barriers currently preventing or slowing down your organisation's planning for or migration to PQC? If so, what are the main one(s)?
4 – Blockers and barriers	Q16	Technical	Are you aware of any specific technical barriers to transitioning your organisation to PQC?
4 – Blockers and barriers	Q17	Both	What sort of non-technical barriers are you aware of?
5 – Government and regulatory interventions	Q18	Both	Are you currently receiving guidance on PQC migration from any of the following: Government or regulators? Industry associations? External consultants? Cyber security technology provider(s)?
5 – Government and regulatory interventions	Q19	Both	What would be most helpful from regulators or government, to encourage, enable or support your organisation in preparing for the transition to PQC? [e.g., more information about threat, training, assessments, software tools, compliance regulation, etc]
6 – Additional comments	Q20	Both	Do you have any further comments or questions that you would like to share with us?

'Ecosystem interview' questions

This set of questions was created after updating the 'End-User' interview questions.

Table C. 2. Set of questions used for 'Ecosystem' interviews.

Area	No.	Respondent type	Programme Questions
1 – Role and organisation	Q1	Both	Can you please share some background on your department and role? Could you elaborate on how your research impacts security decisions in other organisations?

Area	No.	Respondent type	Programme Questions
	Q2		DELETED
1 – Role and organisation	Q3	Technical	How does the lifetime of an asset influence its requirements for cryptography?
2 – PQC Knowledge and awareness	Q4	Both	What security goals are supported by cryptography?
2 – PQC Knowledge and awareness	Q5	Technical	Do you have an opinion on how well industrial organisations understand what cryptography they are using and where?
2 – PQC Knowledge and awareness	Q6	Both	Are there any particular barriers that might make doing an inventory of cryptography challenging for an organisation?
2 – PQC Knowledge and awareness	Q7	Both	How do you think the risk posed by quantum computers compares to other cyber risks that organisations face today? Why?
2 – PQC Knowledge and awareness	Q8	Technical	How do you think the level of risk posed by quantum computers will change in 5-10-30 years' time in comparison to other cyber risks?
2 – PQC Knowledge and awareness	Q9	Both	How much do you know about the impact of quantum computing development on cyber security?
2 – PQC Knowledge and awareness	Q10	Both	Are you aware of any PQC advice or resources? If yes, Which ones?
2 – PQC Knowledge and awareness	Q11	Both	Are you aware of what types of cyber attacks quantum computers can enable, and/or which types of cryptography are most at risk?
2 – PQC Knowledge and awareness	Q12	Both	In your opinion, when do you think quantum computers would constitute a real threat and why?

Area	No.	Respondent type	Programme Questions
2 – PQC Knowledge and awareness	Q13	Both	How soon should an organisation start exploring post-quantum cryptography? - What should their first steps be? - How long do you think it will take an organisation to migrate to PQC? - What is the expected level of effort required? - Which team(s) should be part of the migration? - Could you give the order of magnitude on the estimated total cost of the migration? - How much of a priority is this?
3 – Migration drivers and incentives	Q14	Both	What are the main factors driving your organisation to start planning for or executing on your PQC migration?
4 – Blockers and barriers	Q15	Both	What do you believe are the principal barriers to migrating to PQC?
4 – Blockers and barriers	Q16	Technical	Are you aware of any specific technical barriers to transitioning to PQC?
4 – Blockers and barriers	Q17	Both	What sort of non-technical barriers are you aware of?
5 – Government and regulatory interventions	Q18	Both	What role should academia take in supporting organisations in their migration to PQC?
5 – Government and regulatory interventions	Q19	Both	What would be most helpful from regulators or government, to encourage, enable or support the transition to PQC? [e.g., more information about threat, training, assessments, software tools, compliance regulation, etc]
6 – Additional comments	Q20	Both	Do you have any further comments or questions that you would like to share with us?

Appendix D: *Online survey methodology details*

D.1 Respondent recruitment approach and criteria

The survey was sent to 1293 survey candidates after they passed the pre-screening process applied by our third-party partner, 133 completed it. Of these, 53 were screened out automatically due to not meeting key criteria (see below) but were asked to complete one question on PQC awareness, which we have analysed separately from the rest of the data. The rest (80) completed the full survey; 28 of them were eliminated due to quality issues, which left 52 good, qualified responses.

A third-party survey recruitment firm was used to identify and pre-screen respondents, and to send out the link to the survey. In addition, we recruited a small number of survey targets through the project team's professional network and referrals from DSIT.

We followed similar criteria to those applied for recruiting interview respondents:

1. Organisation location: Respondents must work in an organisation based in the UK, or which has a UK branch large enough to require an UK-based IT/cyber security team.
2. Organisation sector: We targeted five CNI market sectors: energy, transport, telecoms, healthcare, and finance.
3. Organisation type: Private and public companies in the above sectors.
4. Organisation size: Candidate must work in an organisation with more than 250 employees. It is unlikely that smaller companies are currently incorporating quantum threats into their short- and medium-term strategies.
5. Respondent role: Must hold a senior-level role related to cyber security strategy or implementation, within their organisation or sector.
6. Respondent level of PQC familiarity: Must be at least slightly familiar.
7. Responsibilities: Has influence on cyber security strategy, purchasing decisions or deployment.

The survey logic was designed to automatically screen out respondents who did **not** meet the above criteria.

D.2 Respondents breakdown by sector

Table D. 1. Number of respondents at different stages of the survey process, by sector.

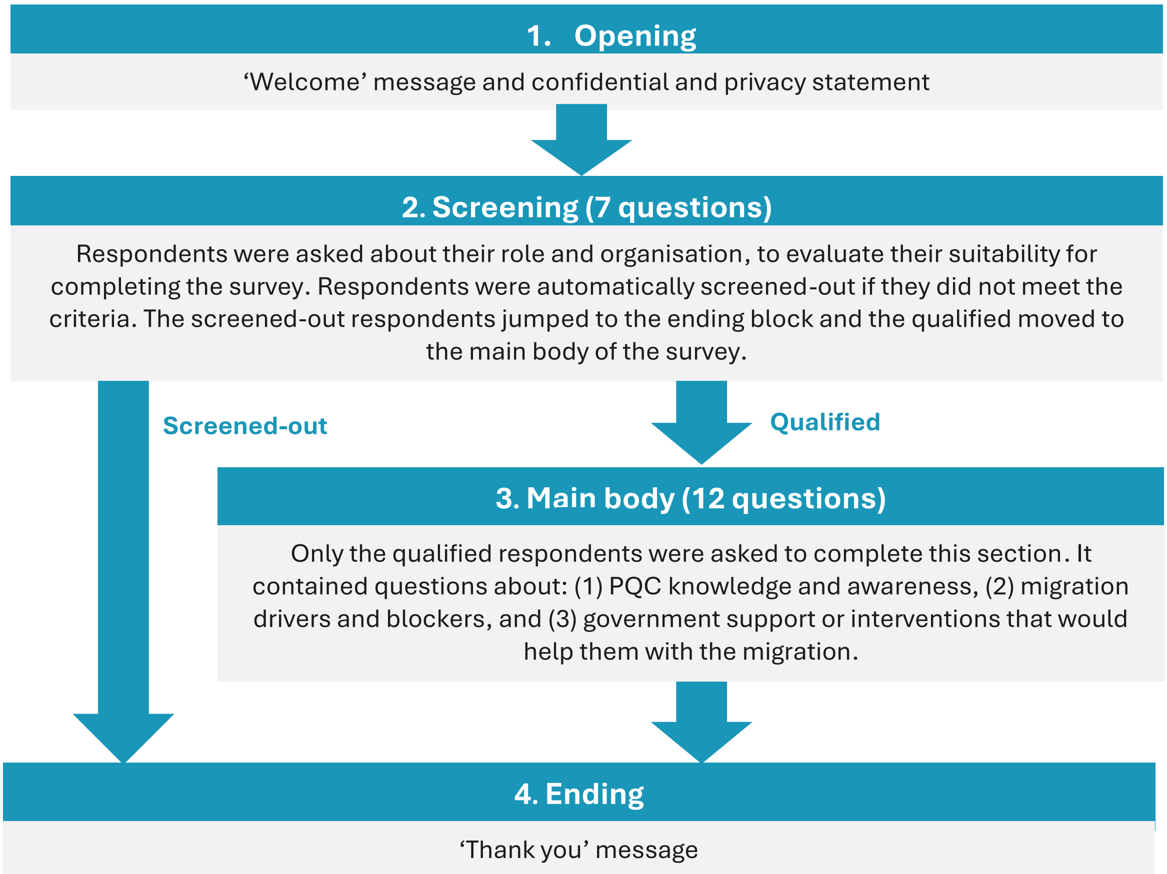
	Total number of responses	'qualified' Completed full survey and passed quality control	'screened-out' Screened out but completed awareness question	'eliminated' Completed full survey but were eliminated due to quality issues
Total	**133**	**52**	**53**	**28**
Energy	13	6	5	2
Transport	15	7	5	3
Telecoms	29	16	5	8
Healthcare	19	4	4	11
Finance	29	7	10	12
Other	28	0	27	1

Note: Table shows number of responses in each category

D.3 Survey methodology and design

The survey was developed using the Qualtrics platform and administered via an online link. The survey had 19 questions, of which 7 were screening questions and 12 were main insight questions. Most questions were closed multiple-choice questions. We also included one open text question on what type of PQC-related government interventions the respondent felt would be most helpful. Time to complete the survey was estimated at 10-15 minutes.

We designed the survey to have four main parts:



D.4 Survey analysis approach

Once the responses were collected, we performed a quality control on the "qualified" ones. The quality control measures applied included:

- Ensuring time to complete survey is in line with our expectations (e.g. a very fast complete time means the respondent was likely answering at random so the response should be excluded).
- Ensuring the IP address indicates respondent is UK-based.
- Ensuring responses are not simply 'first choice selected' only (e.g. respondent just chooses (a), (a), (a), (a), etc.).
- Ensuring human-like behaviour with reCAPTCHA.

The survey questions were also tied to the four overarching objectives of this report.

Each question was analysed individually and by sector, only for the 52 qualified responses that also met the quality criteria. One exception was made on the question *"How many years do you believe you have before a quantum computer could enable a cyber attack against your organisation's systems?"*, which was submitted to every respondent independently of the automatic screening. We did not include the bad quality responses in our analysis.

We presented the main findings through graphs or tables with an accompanying explanatory text. Our analysis included comparisons between sectors to identify the similarities and differences between them.

We also applied different views (not just sector-related) for those questions that could bring interesting insights, including:

- Role (e.g. board vs. non-board respondents)
- Organisation size (e.g. small-medium-large)
- Influence over budget or cyber security strategy (e.g. no influence vs. influence)
- Familiarity with PQC (e.g. moderately-very-extremely familiar)

D.5 Cryptographic maturity framework

Our survey included a question to assess organisations' cryptographic maturity based on 7 statements. For each statement, respondents were asked to select whether they applied to their organisations given four predetermined answers:

- Yes
- To some extent
- No
- Unsure

We created a framework that allowed us to compare the different sectors based on the responses received. Since every sector received a different number of responses, we calculated the percentage of respondents that selected each of the options for each of the statements by sector. Table D. 2 contains an example for the finance sector.

Table D. 2. Responses received for the finance sector in %

Statement	Yes [Y_x]	To some extent [T_x]	No [N_x]	Unsure [U_x]	Score [S_x]
1-We know where our sensitive data is stored	42%	58%	0%	0%	71%
2-We know how long our data needs to be stored and secured for	75%	17%	0%	8%	79%
3-We have a mostly complete inventory of where our organisation uses cryptography	25%	67%	0%	8%	54%
4-We have a team of internal staff with cryptographic skills	50%	42%	0%	8%	67%
5-We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of "banned" algorithms that cannot be introduced	67%	25%	0%	8%	75%
6-Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations	58%	42%	0%	0%	79%

7-Our senior management understands how cryptography contributes to our organisational goals and business strategy	50%	42%	8%	0%	635

A single score was then calculated per statement using formula (1). This is called the statement score s_x, where x symbolises the statement number.

$$(1)\ S_x = Y_x + 0.5T_x - N_x - 0.5U_x$$

S_x: *Statement score*

Y_x: *Percentage of 'Yes' responses for statement x*

T_x: *Percentage of 'To some extent' responses for statement x*

N_x: *Percentage of 'No' responses for statement x*

U_x: *Percentage of 'Unsure' responses for statement x*

Then, our experts assessed and ranked the different statements from 1 (early step in PQC journey or easy to accomplish) to 4 (later step in PQC journey or difficult to accomplish). These ranking positions were used to weigh the different statements, so that the sum of all the weights was 100%.

Table D. 3. Weights for cryptographic maturity statements.

Statement	Rank	Weight [W_x]
1-We know where our sensitive data is stored	1	6%
2-We know how long our data needs to be stored and secured for	2	11%
3-We have a mostly complete inventory of where our organisation uses cryptography	3	17%
4-We have a team of internal staff with cryptographic skills	3	17%
5-We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of "banned" algorithms that cannot be introduced	4	22%
6-Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations	4	22%
7-Our senior management understands how cryptography contributes to our organisational goals and business strategy	1	6%

Finally, all statements were weighed and added together to obtain the sector maturity score following formula (2)

$$(2)\ M_s = 10\sum_{x=1}^{7} S_x W_x$$

M_s: *Maturity score for sector 's'*

S_x: *Statement score*

W_x: *Statement weight*

Table D. 4. Maturity score for the five CNI sectors

Sector	Maturity score
Energy	7.9
Finance	7.1
Healthcare	6.6
Telecoms	5.9
Transport	6.3

D.6 Survey questions

Part 1: Opening

Q1.1 **Organisational readiness for post-quantum cryptography migration**

Cambridge Consultants has been commissioned by the UK Department for Science, Innovation and Technology (DSIT) to undertake a survey of UK organisations regarding their awareness of and plans for future cyber security, specifically relating to the need for post-quantum cryptography (PQC) migration. This survey will take approximately 10 minutes. Survey participation is anonymous, however organisations will be grouped by sector for the purpose of analysis. The survey aims to capture information about:

1. Knowledge and awareness of UK organisations about PQC migration.
2. PQC migration drivers and blockers that UK organisations are experiencing.
3. Potential services, guidance and regulatory support that could support UK organisations in migrating to PQC. The findings will inform the steps that the UK government will consider to support the transition in a way that best enables different sectors and organisations.

Confidentiality and Privacy Statement

Your privacy is important to us. All responses you provide in this survey will be kept strictly confidential. The data collected will be used solely for research purposes and will be anonymised to ensure that no personal identifiers are linked to your responses. Only authorised personnel will have access to the data and it will be stored securely. Your participation is voluntary and you may withdraw at any time without any consequences.

***By clicking NEXT, I understand the confidentiality and privacy statement and agree to participate in this survey**

Part 2: Screening questions

Q2.1 Which of the following describes your organisation?

Select one

- Academic institution
- Energy infrastructure owner, network operator or services provider
- Financial institution
- Government body or regulatory agency
- Healthcare provider (NHS or private)
- Telecommunications /IT services or infrastructure provider
- Transport and/or logistics services or infrastructure provider
- Other ____

Q2.2 What is the name of the organisation you work for? (Response is optional)

Note: This information will remain completely confidential and will only be used for purposes of ensuring appropriate segmentation of responses

____

Q2.3 What is the size of your organisation?
Select one

- Less than 250 employees
- Between 250 and 500 employees
- Between 500 and 1000 employees
- Between 1000 and 5000 employees
- More than 5000 employees

Q2.4 What is your role within the organisation?
Select the option that best describes your role

- CEO/COO
- Chief Information Officer/Chief Data Officer/CISO
- Head/Director of IT
- Head/Director of Cyber security
- Head/Director of Data/Data Security
- Head of Strategy/Planning/Innovation
- Other technical senior management (Director level or above)
- Non-technical senior management (Director-level or above)
- Other ____

Q2.5 What is the relevance of your role to your organisation's cyber security strategy?
Select one

- Direct budget holder for cyber security for overall organisation
- Direct budget holder for cyber security for a specific division/department/asset class
- Strategic planner for cyber security
- Influencer for cyber security but not direct budget holder/planner
- Implementer of cyber security solutions but no direct influence on strategy/purchasing
- No influence on cyber security strategy, purchasing decisions or deployment

Q2.6 How familiar are you with concepts or technologies relating to post-quantum cyber security?
Select one

- Not familiar at all
- Slightly familiar: I am aware of its existence
- Moderately familiar: I have some technical knowledge in this area
- Very familiar: I have deep technical knowledge in this area
- Extremely familiar/active practitioner: I contribute to the development of this area via research papers, thought leadership reports, etc.

Q2.7 How many years do you believe you have before a quantum computer could enable a cyber attack against your organisation's systems?

Select one

- Less than 5 years
- Between 5 and 10 years
- Between 10 and 20 years
- More than 20 years
- Unsure

Part 3: Body of survey

Q3.1 Which sources do you currently consult or follow, for information on quantum cyber security matters?

Select all that apply

- ☐ News websites and magazines. (e.g. Wired, Forbes, Popular science)
- ☐ Blogs and personal websites (e.g. Krebs on security, Cryptogram)
- ☐ Tech News and community forums (e.g. Ars Technica, hacker News, Bleeping computer)
- ☐ Conferences (e.g. Black Hat, DEF CON, RSA Conference)
- ☐ Academic journals (e.g. Journal of cyber security, IEEE Transactions on information forensics and security)
- ☐ Guidance from public organisations and public schemes (National Cyber Security Centre, Cyber Aware, Cyber Essentials)
- ☐ Other: ______________________________
- ☐ ⨂None

Q3.2 Which of the below best describes how your organisation currently plans for and provides cyber security, for your digital assets?

Select one option in each row

	Fully done by our in-house team	Partially outsourced to vendor or consultant	Fully outsourced to vendor or consultant	Unsure
Cyber security planning and strategy	7.	8.	9.	10.
Cyber security deployment, ongoing management and updates	11.	12.	13.	14.

Q3.3 Which of the following are the most important cyber security goals for your organisation? Select your top 3

- ☐ Protect security of e-commerce transactions
- ☐ Protect our intellectual property
- ☐ Ensure data protection and privacy for customers
- ☐ Ensure data protection and privacy for our staff
- ☐ Ensure continuity of operations
- ☐ Prevent cyber attacks having a safety impact on operations and/or customers
- ☐ Prevent cyber attacks having a negative environmental impact
- ☐ Comply with regulation
- ☐ Protect the reputation of our organization
- ☐ Ensure integrity of our data

Q3.4 Do the following statements about cryptographic maturity apply to your organisation? Select an answer for each statement.

	No	To some extent	Yes	Unsure
We know where our sensitive data is stored	•	•	•	•
We know how long our data needs to be stored and secured for	•	•	•	•
We have a mostly complete inventory of where our organisation uses cryptography	•	•	•	•
We have a team of internal staff with cryptographic skills	•	•	•	•
We maintain a list of acceptable cryptographic algorithms/key lengths to use, and of “banned” algorithms that cannot be introduced	•	•	•	•
Our approach to vulnerability management includes assessing our cryptographic libraries to ensure that we are using secure implementations	•	•	•	•
Our senior management understands how cryptography contributes to our organisational goals and business strategy	•	•	•	•

Q3.5 Which of the following best characterises the current status of your organisation's migration towards post-quantum cryptography (PQC)?
Note: 'Migration journey' means the process of migrating all cyber security to be resilient to attacks enabled by quantum computers
Select one

- Not started and not considering right now
- Aware, but not ready to start
- Actively developing a strategy, but have not yet started executing on it
- Migration of our cryptography is already underway
- Migration complete – we have migrated all systems and are fully ready

Q3.6 How soon do you expect to start planning your PQC migration journey?
Note: 'Migration journey' means the process of migrating all cyber security to be resilient to attacks enabled by quantum computers
Select one

- Within the next 12 months
- 1-3 years from now
- 3-5 years from now
- 5-10 years from now
- 10+ years from now
- Unsure

Q3.7 How long do you think it will take your organisation to complete your PQC migration journey, once you start?
Note: 'Migration journey' means the process of migrating all cyber security to be resilient to attacks enabled by quantum computers
Select one

- Less than 1 year
- Between 1 and 3 years
- Between 3 and 5 years
- More than 5 years
- Unsure

Q4.1 What are the most important drivers for your organisation to start planning for or deploying a PQC migration strategy?
Note: Migration journey means the act of migrating all cyber security to be resilient to attacks performed by quantum computers
Select your top 3

- ☐ Government or regulator requirements / Legislative mandates
- ☐ Customer demand
- ☐ Sector- or Industry-specific guidance or requirements
- ☐ Ability to use higher levels of security as a business differentiator
- ☐ More significant evidence of the threat (e.g., reports of successful quantum-enabled cyber attacks)
- ☐ Greater understanding of PQC within your organisation
- ☐ A clear business case for PQC in our organisation
- ☐ Other ______________________________

Q5.1 What barriers are currently preventing or slowing down your organisation's PQC migration? Note: Migration journey means the act of migrating all cyber security to be resilient to attacks performed by quantum computers
Select all that apply

- ☐ Lack of clarity on impact of quantum threat
- ☐ Lack of clarity on timelines for quantum threat
- ☐ Low priority vs mitigating other cyber security threats
- ☐ Low priority vs other IT spend requirements
- ☐ Cost concerns
- ☐ Unclear on operational impact of undertaking a migration
- ☐ Unclear on relevant standards for PQC
- ☐ Unclear on appropriate technology options
- ☐ Lack of executive support
- ☐ Waiting for tech to evolve
- ☐ Planning and execution are too complex
- ☐ Unclear which assets or operations should be prioritised
- ☐ Skills gap in our IT/cyber security team
- ☐ Lack of business case or cost-benefit analysis
- ☐ Other: ______________________________

Q5.2 From the barriers you previously selected, which is the **most significant** one?
Select one

- Lack of clarity on impact of quantum threat
- Lack of clarity on timelines for quantum threat
- Low priority vs mitigating other cyber security threats
- Low priority vs other IT spend requirements
- Cost concerns
- Unclear on operational impact of undertaking a migration
- Unclear on relevant standards for PQC
- Unclear on appropriate technology options
- Lack of executive support
- Waiting for tech to evolve
- Planning and execution are too complex
- Unclear which assets or operations should be prioritised
- Skills gap in our IT/cyber security team
- Lack of business case or cost-benefit analysis
- Other: ____

Q6.1 What are the most important activities you'd like to see from government or regulators, to support your organisation's transition to PQC?
Select your top 3

☐ Technical training for security staff
☐ Awareness training for management and security staff
☐ List of government-accredited PQC suppliers and experts
☐ Maturity or readiness assessments for PQC
☐ Up-to-date advice on specific cryptographic protocols relevant for PQC
☐ Guidance on how to approach cryptographic upgrades for PQC
☐ Mandating accredited PQC as a condition of bidding for new government-funded projects
☐ Grants for small-medium enterprises to pursue security improvements (including PQC migration)
☐ Support for developing a clear business case or cost-benefit analysis for PQC migration
☐ Tax incentives for spending on PQC upgrades
☐ Other ____

Q6.2 Could you please elaborate on what type of support would be most helpful, for your top choices?
Write your answer

- Technical training for security staff ______________________________
- Awareness training for management and security staff
  ____
- List of government-accredited PQC suppliers and experts
  ____
- Maturity or readiness assessments for PQC
  ____
- Up-to-date advice on specific cryptographic protocols relevant for PQC
  ____
- Guidance on how to approach cryptographic upgrades for PQC
  ____
- Mandating accredited PQC as a condition of bidding for new government-funded projects
  ____
- Grants for small-medium enterprises to pursue security improvements (including PQC migration)
  ____
- Support for developing a clear business case or cost-benefit analysis for PQC migration
  ____
- Tax incentives for spending on PQC upgrades
  ____
- Other ______________________________

Part 4: Ending

You have reached the end of the survey. Thank you for your time in completing it.