





Organisational preparedness for post-quantum cybersecurity

Jukka Ahtiainen

Evdokimos Konstantinidis

Supervisor, Aristotle University of Thessaloniki

Date: 31.02.2026

Organisational preparedness for post-quantum cybersecurity

Jukka Ahtiainen

Evdokimos Konstantinidis

Supervisor, Aristotle University of Thessaloniki

Date: 31.02.2026

Acknowledgements

This thesis was completed under the supervision of Evdokimos Konstantinidis, whose guidance and feedback are gratefully acknowledged. The research was conducted in cooperation with Modirum Platforms which provided practical context for the study. A big thank you to my family for all the support and encouragement during the whole journey with ManagiDiTh.

The views expressed and conclusions drawn are those of the author alone. This study is for organisations, stay safe out there.

Abstract

Quantum computing introduces a fundamental shift in computational capability that challenges the long-term security assumptions of current cryptographic systems. While large-scale fault-tolerant quantum computers are not yet available, their foreseeable development creates a delayed but systemic cybersecurity risk for organisations that rely on classical public-key encryption. This risk is amplified by the harvest now, decrypt later model, in which encrypted data collected today may be exposed in the future.

The purpose of this thesis is to examine how organisations should prepare for quantum-safe cybersecurity and post-quantum cryptography from a strategic, regulatory, and organisational perspective. The study combines a structured literature review with an empirical survey conducted among cybersecurity professionals in Finland, with a particular focus on regulated and critical sectors.

The findings indicate that awareness of post-quantum cryptography exists but remains shallow, and that organisational preparedness is generally at an early stage. The most significant barriers identified are technological uncertainty, lack of skills, limited resources, and insufficient guidance. At the same time, regulatory developments and public investment signals suggest that post-quantum preparedness is increasingly becoming a governance and compliance expectation rather than a purely technical option.

This thesis concludes that effective preparation for quantum-safe cybersecurity requires early and structured action. Key measures include cryptographic inventory management, crypto-agile system design, hybrid cryptographic deployments, vendor readiness assessment, and documented transition planning. By integrating these measures into long-term security governance, organisations can reduce future exposure while remaining aligned with evolving regulatory and technological expectations.

Keywords: post-quantum cryptography; quantum-safe cybersecurity; organisational preparedness; cryptographic governance; regulatory compliance

Glossary

Advanced Encryption Standard (AES)

A symmetric encryption algorithm widely used for securing data in transit and at rest due to its efficiency and scalability.

Asymmetric encryption

A cryptographic method that uses a pair of keys (public and private) for secure communication, enabling encryption, authentication, and digital signatures without pre-shared secrets.

Coherence time

The duration during which a quantum system can maintain its quantum state before decoherence occurs, limiting the depth and reliability of quantum computations.

Cryptographic agility (crypto-agility)

The capability of an information system to rapidly switch cryptographic algorithms and protocols without requiring major system redesign.

Decoherence

The loss of quantum information caused by interaction with the environment, representing a key operational limitation and risk factor in quantum computing systems.

Entanglement

A quantum mechanical phenomenon where the states of two or more particles become correlated such that the state of one cannot be described independently of the others.

GDPR (General Data Protection Regulation)

A European Union regulation that sets requirements for protecting personal data through appropriate technical and organisational measures, including encryption.

Harvest Now, Decrypt Later (HNDL)

A threat model in which adversaries collect encrypted data today with the expectation that future quantum computing capabilities will enable its decryption.

Hybrid cryptography

An approach combining classical and post-quantum cryptographic algorithms to ensure security during the transition period to quantum-resistant systems.

Logical qubit

An error-corrected qubit constructed from multiple physical qubits to achieve reliable computation in fault-tolerant quantum systems.

NIS 2 Directive

An EU cybersecurity directive that mandates risk management, governance, and security controls for essential and important entities across critical sectors.

NIST (National Institute of Standards and Technology)

A U.S. standards body responsible for developing and standardising post-quantum cryptographic algorithms and migration guidance.

Post-Quantum Cryptography (PQC)

Cryptographic algorithms designed to be secure against both classical and quantum computing attacks, forming the basis of future secure communication systems.

Public Key Infrastructure (PKI)

A framework of technologies, policies, and procedures used to manage digital certificates and public-key encryption systems.

Quantum computing

A computational paradigm that uses quantum mechanical principles such as superposition and entanglement to perform calculations beyond classical capabilities for certain problem classes.

Quantum-safe cybersecurity

A cybersecurity approach that incorporates quantum-resistant cryptographic methods to ensure long-term data protection against quantum threats.

Qubit (quantum bit)

The fundamental unit of quantum information that can exist in multiple states simultaneously due to superposition.

RSA (Rivest–Shamir–Adleman)

A widely used public-key cryptographic algorithm based on integer factorization, vulnerable to quantum attacks via Shor's algorithm.

Shor's algorithm

A quantum algorithm capable of efficiently solving integer factorization and discrete logarithm problems, threatening classical public-key cryptography.

Superposition

A quantum property allowing a qubit to exist in multiple states simultaneously until measured.

Symmetric encryption

A cryptographic method that uses a single shared key for both encryption and decryption, known for efficiency in handling large data volumes.

Transmon qubits

Transmission-line shunted plasma oscillation qubits are a type of superconducting qubit designed to reduce sensitivity to charge noise, thereby improving coherence times and stability in quantum computing systems.

Index

Acknowledgements i
Abstract ii
Glossary iii
1. Introduction 1
2. Post-quantum cryptography 2
2.1 The implications of quantum computing 3
2.2 Why quantum era 5
2.3 Companies with quantum computers 6
2.4 Quantum computers 9
2.5 Quantum knowledge in Finland 10
2.6 Investment signals and strategic implications for PQC 12
3. Quantum theory 13
3.1 Quantum computing 14
3.2 Decoherence as an indicator of operational risk 14
3.3 Quantum physics 15
4. Quantum regulations 16
4.1 GDPR 16
4.1.1 GDPR's security requirements and the role of encryption 16
4.2 NIST and NIS 2 directive 17
4.3 EHDS 17
4.4 NIST with standardisation of PQC 18
4.5 NIS 2 directives scope and obligations 18
4.6 PQC threats under GDPR 19
4.7 Compliance strategies that bridge GDPR and PQC 20
5. Quantum era 21
6. Methodology of research survey 23
6.1 Survey method 23
6.2 Target group and scope 23
6.3 Changes to survey scope 24
6.4 Research survey questions 25
6.5 Results and analysis: Post-Quantum Cryptography (PQC) Readiness Survey 29
6.6 Research survey summary 37

7. Results 37
8. Conclusion 38
9. References 40
Annexes 44
Annex A 44
Annex B 49

Index of tables and figures

Index of Figures

Figure 1: 2.1 VTT-IQM-Q50-quantum-computer 2 by Peter Franco. 11
Figure 2: 6.1 Authors own work (2025) 29
Figure 3: 6.2 Authors own work (2025) 31
Figure 4: 6.3 Authors own work (2025) 33
Figure 5: 6.4 Authors own work (2025) 34
Figure 6: 6.5 Authors own work (2025) 35

Index of Tables

Table 1: 2.1 Organisations with superconductive quantum computer 7
Table 2: 2.2 Quantum computers 10

1. Introduction

The context of this study is shaped by the rapidly evolving landscape of post-quantum cryptography (PQC), where technological progress in quantum computing continues to challenge previously stable assumptions about cryptographic security. While earlier projections estimated that breaking widely used public-key encryption would require millions of physical qubits, recent developments in error correction, gate fidelity, and logical qubit optimisation suggest that the required threshold is steadily decreasing. Combined with continuous improvements in coherence times and system reliability indicates that the timeline for cryptographically relevant quantum capabilities may be shorter than previously assumed.

This evolving situation positions PQC not as a distant theoretical concern, but as an active strategic issue for organisations today. The uncertainty surrounding exact timelines does not reduce risk, it rather amplifies it. The relevance of PQC is directly tied to data longevity rather than immediate technological readiness.

This thesis is developed within the ManagiDiTH Master's programme, which emphasises the intersection of management, digital transformation, and technological innovation. Within this academic context, the study approaches PQC not solely as a technical cybersecurity problem, but as a multidisciplinary organisational challenge involving governance, risk management, regulatory compliance, and long-term strategic planning. The research reflects the programme's objective of bridging technological understanding with managerial decision-making in complex digital environments.

At the core of this study lies the role of data as a critical organisational asset. Organisations are fundamentally dependent on the confidentiality, integrity, and availability of data. Regardless of whether the sector is healthcare, finance, public administration, or other critical infrastructure. In sectors such as healthcare, where sensitive personal data may need to remain confidential for decades, the implications of quantum threats are particularly acute. However, the same underlying risk applies broadly across all domains that manage long-lived or high-value data.

In this context, PQC represents a paradigm shift in how organisations must approach data protection. The transition is no longer limited to technical upgrades of cryptographic algorithms but extends to organisational preparedness, architectural design, and strategic foresight. This thesis therefore positions itself at the intersection of technological evolution and organisational response, aiming to provide insight into how organisations can prepare for a future in which quantum computing reshapes the foundations of digital trust.

This study has made limited use of artificial intelligence (AI) tools to support the writing process, particularly in language refinement and translation. The AI tool ChatGPT was utilised to improve clarity, grammar, and readability, as well as to assist in translating content between Finnish and English.

In addition, AI-assisted support was used in a limited technical capacity to aid in the development of Python code for survey data handling and the generation of figures. The code was implemented and validated by the author using PyCharm, and all outputs were reviewed to ensure correctness and alignment with the research objectives. The use of AI was restricted to supportive linguistic and technical assistance. All substantive content, including research design, analysis, interpretations, and conclusions, remains the original work of the author. AI tools were not used to autonomously generate academic arguments or research findings.

2. Post-quantum cryptography

Quantum computing represents a fundamental shift in computational capability rather than a linear extension of existing technologies. Unlike classical computing, quantum systems exploit physical phenomena such as superposition and entanglement to process information in ways that can outperform classical computers for specific problem classes. While large-scale fault-tolerant quantum computers are not yet available, credible scientific progress has established that quantum computing poses foreseeable long-term implications for cybersecurity and data protection (Preskill, 2018; Mosca, 2018).

The relevance of quantum computing for organisations lies not in immediate operational disruption but in its impact on long-term security assumptions. Current cryptographic systems underpin digital trust across finance, public administration, healthcare, and critical infrastructure. Advances in quantum computing challenge the durability of these systems by altering the time horizon over which encrypted data can remain confidential. As a result, quantum computing introduces a delayed but systemic cybersecurity risk that organisations must address proactively rather than reactively (Mosca & Piani, 2023).

In the HNDL model, adversaries collect encrypted data today with the expectation that future quantum capabilities may enable decryption. This risk is especially relevant for organisations that process data with long-term sensitivity. The segments could include personal data, intellectual property, strategic communications, and state or industrial secrets. Even in the absence of immediate compromise, delayed exposure can result in regulatory, financial, and reputational consequences (Preskill, 2018; Mosca, 2018).

Regulatory and policy developments increasingly reflect this forward-looking risk assessment. In the European Union, cybersecurity and data protection frameworks emphasise the obligation to implement appropriate and state-of-the-art security measures. Recent policy initiatives explicitly acknowledge the need to prepare for cryptographic transition in response to quantum threats, even before quantum computers reach practical maturity. This positions post-quantum preparedness as a governance and compliance issue rather than a discretionary technical enhancement (European Commission, 2024).

In contrast to the EU, the United States has adopted a standards-driven approach that focuses on defining and publishing quantum-resistant cryptographic standards. The standard is allowing organisations flexibility in implementation timing. Through the National Institute of Standards and Technology (NIST), the U.S. model emphasises technical interoperability, migration guidance, and industry-led adoption. Despite these differences with EU, both regulatory approaches converge on a shared expectation that organisations should begin structured preparation for PQC. This work is based on foreseeable technological risk rather than confirmed attack capability (NIST, 2023; Mosca & Piani, 2023).

These developments taken together indicate that PQC is evolving into an actual compliance expectation. Organisations that delay preparation until quantum computers are operationally mature, risk misalignment with regulatory expectations. Prolonged migration timelines and increased exposure to legacy cryptographic dependencies are risks not to be taken lightly. Effective preparation therefore requires early integration of quantum risk into organisational strategy, security governance, and long-term investment planning rather than isolated technical experimentation. The following section examines how this transition is reflected in contemporary interpretations of state-of-the-art cybersecurity and organisational responsibility.

2.1 The implications of quantum computing

Key industry verticals that need to take mitigative cybersecurity steps are numerous. Banking and financial services have high data sensitivity and long-life value of data. Critical national infrastructures that provide essential systems, services or organisations that country relies on are particularly exposed due to the longevity and systemic importance of the data they process.

Healthcare infrastructure includes hospitals, emergency medical services, national health agencies, and pharmaceutical suppliers that deliver critical medical care and ensure continuity of public-health

functions (European Commission, 2020). Communications infrastructure consists of telecommunications providers, internet service operators, and satellite communication organisations that maintain essential digital and telecommunication connectivity (NCSC, 2023). Energy systems comprise organisations responsible for the generation, transmission, and distribution of power, including electricity grid operators, power-generation companies, oil and gas producers, pipelines, and refineries (CISA, 2023; NCSC, 2023). Water and wastewater infrastructure includes municipal water utilities and wastewater treatment facilities that ensure the safe provision, management, and disposal of water resources essential for public health (European Commission, 2020). Transportation infrastructure encompasses airports and air-traffic control services, rail network operators, major port authorities, and public transit agencies that enable national and international mobility (CISA, 2023). Financial infrastructure refers to central banks, major commercial banking institutions, and payment and clearing systems that underpin the stability and operation of the national economy (CISA, 2023). Government and public-service infrastructure comprise emergency services such as police, fire, and ambulance agencies. Also, national security and defence organisations and government data centers and administrative bodies that sustain state functionality (NCSC, 2023). Food and agriculture infrastructure includes organisations responsible for food production, processing, and distribution networks that support national food security (European Commission, 2020). Industrial and manufacturing infrastructure, recognized in some jurisdictions, incorporates chemical plants and facilities managing hazardous materials whose disruption could pose significant risks to human safety and the environment (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

The implications of quantum computing represent a qualitative shift rather than an incremental technological improvement. Unlike previous advances in computing power, quantum computing directly targets mathematical assumptions underpinning widely deployed public-key cryptographic systems. This creates a systemic risk that affects not only future data but also historically encrypted information with long-term value (Mosca, 2018).

Current academic discourse emphasizes that the quantum threat is not solely determined by the immediate availability of large-scale fault tolerant quantum computers, but by the asymmetry between data capture today and decryption capabilities in the future. This HNDL alters risk calculations for organisations responsible for sensitive or regulated data (Shor, 1997; Preskill, 2018). While full cryptographic relevant quantum computers, super conductive or other types, are not yet available, the consensus in recent literature is that organisations cannot rely on uncertainty in timelines as a security strategy. Risk exposure must be evaluated based on data longevity, adversary capability growth, and migration lead times for cryptographic infrastructure instead (Chen et al., 2016; Mosca, 2018).

Quantum risk for management is best understood as a strategic and compliance-driven issue rather than a purely technical one. Organisations that operate in regulated sectors face increasing pressure to demonstrate proactive risk management aligned with new directives embedded in cybersecurity and data protection frameworks. Consequently, quantum preparedness is emerging as a component of organisational resilience and long-term risk governance rather than an optional future enhancement (Preskill, 2018).

2.2 Why quantum era

The development of quantum computing marks a new technological era with the potential to reshape scientific discovery, industrial processes, and economic competitiveness. Unlike incremental improvements in classical computing, quantum computing introduces fundamentally new computational capabilities derived from quantum mechanical principles. These are superposition and entanglement. These capabilities enable certain classes of problems to be approached in ways that are practically impossible for classic computers.

The positive potential of quantum computing is often highlighted in relation to addressing complex global challenges. Quantum computational capability can be applied to environmental modelling, materials science, and chemical simulations that exceed the practical limits of classical digital computers (Bauer et al., 2020). Chemistry and materials research involve quantum-mechanical interactions that are extremely difficult to model accurately using classical methods. One frequently cited example is synthetic photosynthesis, which relies on quantum coherence and energy transfer processes that classical simulations can only approximate (Engel et al., 2007; Lambert et al., 2013). Quantum computers are theoretically well suited to such calculations and may, in the long term, contribute to advances in sustainable energy technologies and resource-efficient food production by enabling more accurate molecular and material design (Preskill, 2018).

Global corporations and governments have nevertheless initiated extensive quantum research programs. Some organisations possess the technical expertise to build and operate quantum hardware, while others invest strategically to secure early access, intellectual property, and human capital. Haste with quantum computing has been compared to historical technological races, such as the space race, where early participation conferred long-term strategic and geopolitical advantages.

From an organizational strategy perspective, investment in quantum technologies is increasingly interpreted as an option-value decision rather than an immediate productivity investment. Firms and public institutions allocate resources to quantum research not because near-term returns are

guaranteed, but because delayed entry could result in long-term competitive disadvantage if quantum advantage materializes in critical domains (Arute et al., 2019; Preskill, 2018).

At the same time, academic literature emphasizes the importance of distinguishing between three horizons of quantum value creation. These are demonstrated use cases (such as limited quantum simulations and optimization experiments), experimental prototypes with uncertain scalability, and long-term theoretical potential that may take decades to realize. Organisations that fail to make this distinction risk misallocating capital or adopting unrealistic expectations regarding return on investment (Preskill, 2018; Gyongyosi & Imre, 2019). Consequently, the strategic relevance of the quantum era for organisations lies not only in the promised societal benefits, but in prudent investment timing, capability building, and risk management towards PQC. Quantum readiness increasingly functions as a hedge against technological disruption. Early learning, ecosystem participation, and cryptographic preparedness may deliver resilience even if full quantum advantage remains distant (Preskill, 2018).

2.3 Companies with quantum computers

Public discussion of quantum computing progress frequently emphasizes qubit count as the primary indicator of technological advancement. While qubit scale is a visible and easily communicated milestone, academic literature consistently argues that qubit count alone is an insufficient metric for evaluating the real-world impact of quantum computers (Preskill, 2018; Gyongyosi & Imre, 2019). From a cybersecurity and post-quantum cryptography (PQC) perspective, the relevance of quantum hardware lies not in raw qubit numbers but in the system's ability to execute long, reliable, fault-tolerant computations. Consequently, organisational preparedness for the quantum era requires evaluation criteria that extend beyond headline hardware announcements.

A critical factor in this evaluation is the error rate of quantum operations. Physical qubits, particularly in superconducting architectures, are inherently noisy meaning that each quantum gate introduces errors which accumulate rapidly during computation. Contemporary research on fault-tolerant quantum computing demonstrates that cryptographically relevant attacks, such as breaking RSA using Shor's algorithm, require extremely low logical error rates that can only be achieved through substantial quantum error correction overhead (Gambetta et al., 2015; Preskill, 2018). Recent experimental and theoretical studies indicate that achieving a single error-suppressed logical qubit typically requires on the order of hundreds to thousands of physical superconducting qubits, depending on

target fidelity and code distance (Google Quantum AI, 2023; Terhal, 2013). Updated resource estimates further show that the feasibility of quantum attacks on public-key cryptography is dominated by the cost of constructing and maintaining logical qubits rather than by raw physical qubit counts alone (Sohn et. al., 2019). As a result, quantum processors with thousands of physical qubits pose an immediate threat to classical encryption (HNDL) and represent incremental progress toward future cryptographic capability. For organisations assessing PQC urgency, trends in error reduction and logical qubit scaling are therefore more informative indicators of risk than headline qubit numbers alone (Mosca & Piani, 2023).

Table 1: 2.1 Organisations with superconductive quantum computer

NAME	Producer	Qubits
Condor	IBM	1121
Jiuzhang	China	76
Bristlecone	Google	72
50-qubit QC	IQM with VTT	50
Tangle Lake	Intel	49

These companies are known and involved with quantum computers 2025. IBM is aiming openly towards one million qubits quantum computer.

Contemporary quantum systems exhibit steadily improving coherence times, particularly in superconducting qubit architectures; however, these improvements remain insufficient for sustained execution of cryptographically relevant workloads without extensive error correction. Recent experimental results demonstrate that transmon qubits can achieve energy relaxation and dephasing times in the range of hundreds of microseconds, with isolated demonstrations approaching the millisecond regime under highly controlled laboratory conditions (Gambetta et al., 2015; Google quantum AI, 2023). While these advances represent significant progress compared to earlier generations of superconducting qubits, academic analyses emphasize that such coherence durations still constrain circuit depth and limit the feasibility of executing long, complex algorithms required for breaking modern public-key cryptography (Sohn et. al., 2019). In practice, cryptographically relevant quantum computations would require coherence times that can be sustained across large numbers of logical qubits operating in parallel, a capability that remains far beyond current experimental systems. Consequently, although improving coherence trends signal technological momentum, they do not yet translate into an immediate quantum threat to classical encryption. For organisations assessing post-quantum cryptography (PQC) readiness, coherence time developments should therefore be

interpreted as early indicators of long-term risk evolution rather than evidence of near-term cryptographic vulnerability (Mosca & Piani, 2023).

High gate fidelity is essential for reducing cumulative errors and enabling effective error correction. Recent experiments have demonstrated record single-qubit fidelities (up to 99.998%), which significantly reduce the resource overhead for fault-tolerant implementations (MIT researchers, 2025). Control methods such as geometric gates achieving fidelities above 99% further confirm that improvements in fidelity contribute more to practical capability than simple increases in qubit count (Zhou et al., 2025). Real-world analyses of multi-qubit gate implementations demonstrate how noise and fidelity trade-offs affect error rates in hardware (AbuGhanem, 2025), and comprehensive frameworks link fidelity directly to computational cost and effective circuit performance (Kechedzhi et al., 2024). Sustained improvements in these metrics are therefore key early indicators of accelerating quantum maturity and inform organisational PQC readiness more reliably than speculative trends.

Beyond hardware performance, ecosystem maturity plays a decisive role in translating quantum computing capability into real-world impact. Ecosystem maturity encompasses software development frameworks, compiler optimizations, cloud-based access models, benchmarking standards, and the availability of skilled personnel (Gyongyosi & Imre, 2019). Firms positioning themselves as quantum platform providers invest heavily in these ecosystems to enable experimentation and accelerate learning across user communities. In contrast, other organisations pursue quantum hardware primarily as a signal of research leadership or national technological capability. From a strategic management perspective, this distinction matters. Platform-oriented strategies accelerate applied knowledge diffusion and potential risk exposure, while research-oriented approaches may serve national innovation policy objectives without immediate cryptographic consequences (Preskill, 2018).

Taken together, these dimensions illustrate why organisational preparation for PQC cannot be based on isolated technological metrics or promotional claims. Quantum computing capability emerges from the convergence of hardware reliability, software ecosystems, and sustained institutional investment. Companies and governments that lead across these dimensions influence not only future computational advantage but also the timeline over which classical cryptographic systems may become obsolete. For organisations responsible for protecting long-lived sensitive data, understanding these metrics supports rational investment decisions and phased PQC adoption. In this context, quantum hardware development functions as a strategic early-warning signal for cybersecurity planning, reinforcing the need for proactive, metrics-driven preparation for the post-quantum era (Mosca, 2018; Chen et al., 2016).

2.4 Quantum computers

Multiple technological approaches are currently being pursued to realize practical quantum computers. Dominant hardware architecture has not yet emerged. This diversity reflects both the early stage of the field and the significant engineering challenges associated with scaling quantum systems while maintaining acceptable error rates. Unlike classical computers, quantum computers are inherently probabilistic and error-prone, meaning that computational reliability depends on sophisticated error correction rather than perfect physical operation. As a result, progress in quantum computing is better understood through improvements in error mitigation, coherence, and control fidelity than through raw qubit counts alone (Preskill, 2018; Gyongyosi & Imre, 2019).

Superconducting quantum computers are currently the most widely deployed platform among large technology companies. These systems use superconducting circuits operated at cryogenic temperatures to implement qubits with fast gate speeds and strong integration with existing semiconductor fabrication processes. Their primary limitation lies in relatively short coherence times and comparatively high error rates, which demands substantial quantum error correction in the end. Empirical studies indicate that thousands of physical superconducting qubits may be required to realize a single fault-tolerant logical qubit suitable for cryptographically relevant workloads (Google quantum AI, 2023; Gambetta et al., 2015). From a PQC perspective, superconducting platforms are therefore advancing rapidly in scale but remain constrained by reliability rather than qubit quantity.

Ion trap quantum computers employ charged atoms confined and manipulated using electromagnetic fields. These systems are known for significantly longer coherence times and high gate fidelities compared to superconducting qubits, which reduces certain error correction requirements (Preskill, 2018). However, ion trap systems typically suffer from slower gate operations and scalability challenges related to control complexity and physical layout. As a result, while ion traps demonstrate superior stability at small scales, their path toward large-scale, fault-tolerant quantum computing remains uncertain. For organisations monitoring PQC risk, ion traps illustrate that long coherence alone does not directly translate into near-term cryptographic capability.

Photonic and silicon photonic quantum computers represent an alternative approach focused on using photons as qubits that often operate at room temperatures. These architectures offer potential advantages in scalability and integration with optical communication infrastructure. Also reduced sensitivity to thermal noise makes these quantum computers more fault tolerant. (Flamini, Spagnolo, & Sciarrino, 2018). However, challenges related to deterministic photon generation, loss, and two-

qubit gate implementation remain significant. At present, photonic systems are primarily experimental, and their implications for PQC timelines are long-term rather than immediate.

Topological quantum computers aim to encode qubits in exotic quantum states that are expected to be more resistant to local noise. This property could reduce the amount of error correction required for reliable computation. The concept is considered attractive from an error correction perspective, but scalable topological quantum computers have not yet been demonstrated. Current experimental work focuses on validating basic measurement and control mechanisms needed to form a topological qubit. Recent peer reviewed studies report progress in semiconductor and superconductor devices that support these quantum states. Yet these results represent early technical milestones rather than proof of large-scale fault tolerant quantum computation (Microsoft Azure Quantum, 2025). As a result, topological quantum computing should be viewed as a long-term research direction rather than a practical technology. From an organisational PQC planning perspective, topological qubits do not represent a near-term driver of cryptographically relevant quantum risk and should instead be treated as part of a distant technology horizon (Nayak et al., 2008; Preskill, 2018; Fu & Li, 2024).

Quantum annealers, such as those developed by D-Wave, differ fundamentally from universal, gate-based quantum computers. These systems are designed to solve specific optimization problems rather than to execute general quantum algorithms such as Shor's algorithm. As a result, quantum annealers are not considered capable of breaking public-key cryptography and do not contribute directly to PQC risk (Preskill, 2018). Their existence nonetheless highlights the fragmentation of the quantum computing landscape and the importance of distinguishing between quantum technologies with cryptographic relevance and those without.

Table 2: 2.2 Quantum computers

Superconducting Quantum Computer	Ion Trap Quantum Computer	Photonic Quantum Computers	Silicon Photonic Computers	Topological Quantum Computers	D-Wave Quantum Computers

2.5 Quantum knowledge in Finland

The joint development project between VTT and IQM has successfully concluded after four years. This resulted Finland's first 50-qubit superconducting quantum computer. Initiated in 2020 with €20.7 million in government funding, the project aimed to strengthen national expertise in quantum computing and to support the adoption of quantum technologies in both research and industrial contexts. During the project, 5- and 50-qubit quantum computers were developed. Most recent system

positions Finland as a European frontrunner in the field of superconducting quantum technologies. As part of the development process, an intermediate 20-qubit device was first constructed and later upgraded into a fully functioning 50-qubit system, reflecting substantial progress in domestic quantum hardware capabilities (VTT, 2025).

The significance of the new quantum computer is substantial for national technological advancement as well as for industrial applications. The system enables the development of novel algorithms and computational methods in areas such as simulation, optimization, artificial intelligence, and materials modeling. VTT and IQM contributed complementary technological expertise throughout the collaboration, and the resulting quantum computer is widely accessible to researchers and companies. Its availability is expected to accelerate scientific breakthroughs while also supporting the emergence of practical applications across Finnish industry (VTT, 2025). Super computers and classical quantum computing systems (hybrids) together with quantum computers might be the first steps towards useable power to discover new findings in computer owners' own industry segment.



Figure 1: 2.1 VTT-IQM-Q50-quantum-computer 2 by Peter Franco.

2.6 Investment signals and strategic implications for PQC

Investment patterns in quantum technologies provide important strategic signals for organisations planning post-quantum cryptography transitions. Public funding and venture capital pursue fundamentally different objectives. This distinction helps explain why progress toward quantum capability continues despite uncertainty around near-term commercial returns. Public funding is primarily aimed at building long-term national capability, scientific infrastructure, and technological sovereignty. Governments justify sustained investment in quantum research and infrastructure based on resilience and security considerations rather than immediate profitability, which signals that quantum capability development is viewed as a strategic necessity rather than an optional innovation (European Commission, 2024; OECD, 2025).

This logic is evident in large-scale public investment programs in the United States and China. In the United States, the National Quantum Initiative coordinates multi-agency federal funding to support research, infrastructure, and technology transfer with the explicit objective of maintaining long-term technological leadership (Quantum.gov, 2023). In China, quantum technology development is widely described as government-led and aligned with state strategic priorities, with national programmes designed to build long-term capability rather than near-term commercial returns (Paglieri et al., 2025). Policy-level analysis also notes that China has announced multi-billion-dollar investment commitments for quantum infrastructure, including major national laboratory capacity, reflecting a sustained state-driven approach to capability development (Organisation for Economic Co-operation and Development, 2025). The implication for organisations is that progress toward cryptographically relevant quantum capability will be driven by strategic state priorities. Even in the absence of clear short-term market demand, reducing the viability of prolonged “wait and see” approaches to post-quantum preparedness (Mosca & Piani, 2023).

Venture capital investment follows a different logic and plays a complementary role. Private investors focus on scalable business models, shorter time horizons, and technologies that can generate value before fault-tolerant quantum computers become available. Venture funding has concentrated as a result on quantum software, cloud access platforms, control systems, and hybrid architectures that integrate quantum processors into existing computing environments (OECD, 2025). This activity is strategically significant for PQC because it accelerates the availability of migration tools, cryptographic agility solutions, and supporting services that lower organisational barriers to PQC adoption (Chen et al., 2016; NIST, 2023).

The Finnish quantum program illustrates how investment signals are not solely a function of absolute funding levels. Even with modest investments compared with the scale of major economies, this joint VTT and IQM case demonstrates that targeted objectives and ecosystem integration can convert limited funding into credible capability (VTT, 2025). For organisational decision-makers, the lesson is that post-quantum preparedness does not depend on matching global hardware investment levels, but on aligning strategy, infrastructure, and cryptographic transition planning with observable technological and policy trajectories (European Commission, 2024; Mosca, 2018).

3. Quantum theory

Quantum theory represents one of the most significant shifts in scientific understanding since the development of classical mechanics. Emerging in the early twentieth century, quantum mechanics challenged long-standing assumptions about determinism and the nature of physical reality. Early contributors such as Planck, Einstein, and Bohr demonstrated that energy is quantified and that particles exhibit behaviors that cannot be explained using classical physics alone (Nielsen & Chuang, 2010). These foundational discoveries paved the way for a new theoretical framework capable of describing phenomena at the atomic and subatomic scales.

A key feature of quantum mechanics is the probabilistic nature of physical systems. Rather than possessing definite properties independent of observation, quantum systems exist in superpositions as multiple possible states simultaneously, until measured (Griffiths, 2017). This principle revolutionized scientific perspectives on measurement, uncertainty, and the limits of human knowledge. Moreover, the concept of entanglement, in which the states of two particles become inseparably correlated, challenged classical notions of locality and suggested that quantum information can exhibit nonclassical correlations across distances (Einstein, 1935).

In recent decades, quantum theory has expanded beyond foundational physics into emerging technologies such as quantum computing, quantum communication, and quantum sensing. Quantum computers use quantum bits called qubits. Qubits are capable of superposition and entanglement to perform certain computations more efficiently than classical machines (Preskill, 2018). These advances indicate that quantum principles not only deepen our understanding of nature but also hold transformative potential for future technological landscapes.

3.1 Quantum computing

Quantum computers use physical quantum bits. Qubits enable superposition and entanglement. The number of qubits in any quantum computer does not indicate directly the usable computational power. Qubits are highly sensitive to environmental disturbance and cannot be scaled as is without introducing control complexity and substantial error (Preskill, 2018; Gyongyosi & Imre, 2019). For decision-makers this distinction matters because increased qubit counts do not directly translate into operational capability. The urgency to assess cryptographic transition does not come from headlines about qubit figures. Organisations should monitor system reliability metrics, error correction progress and logical qubit stability (Mosca, 2018; Mosca & Piani, 2023). Present superconducting quantum computers have qubits under 1150 and looking ahead. Quantum computer physical qubits don't need to be in millions scale to solve new algorithms or break cyber encryptions. Advanced Encryption Standard (AES) 126-bit encryption can be breakable by the end of year 2029. AES-126 is still common and weak encryption within companies (Jäppinen, 2025).

3.2 Decoherence as an indicator of operational risk

Decoherence represents operational instability. It is about quantum information loss due to interaction with the surrounding environment. It is an unavoidable phenomenon that limits the depth and duration of quantum computation (Zurek, 2003; Preskill, 2018). Short coherence times determine how long a quantum computer can perform meaningful calculations in superconductive states before quantum state collapses and the calculations continue at classical speed. It's vital to recognize the different quantum technologies that have different decoherence states. Organisations that evaluate potential quantum use cases or assess future cryptographic threats, decoherence therefore translates into execution risk. Quantum computers with short coherence times require heavier error correction and tighter environmental control, which in turn increase capital expenditure and operational overhead (Sohn et. al., 2019)

In practical terms, decoherence helps explain why most organisations access quantum systems through cloud-based services rather than on-premises installations. Centralized cloud delivery allows providers to absorb hardware fragility and operational risk, while customers interact with quantum resources at an abstracted level. For organisations this reinforces the expectation that early quantum capability will be consumed as a service rather than owned as physical infrastructure (Preskill, 2018; OECD, 2025).

3.3 Quantum physics

Quantum physics describes the world at the subatomic level, offering a framework fundamentally different from classical interpretations. It proposes that radiation is quantized, meaning it is divided into discrete packets known as quanta, each operating with its own characteristic frequency, wavelength, and energy. Researchers in the field have demonstrated that subatomic particles behave in ways that differ profoundly from the phenomena observed in the macroscopic world familiar to us, challenging long-held assumptions about the nature of physical reality (Challoner, 2025).

In addition to advances in fundamental quantum research and hardware development, an important question concerns when quantum computers are likely to become genuinely useful for society and in what ways they will complement existing computational technologies. Although fully error-corrected quantum computers remain a long-term goal, practical quantum devices are already beginning to offer value in highly specialized computational tasks (Preskill, 2018). Their impact is expected to emerge gradually as hybrid models are adopted, in which quantum processors work alongside classical high-performance computing systems. These hybrid computational approaches are becoming increasingly common in both research settings and industry because they allow quantum devices to handle specific subproblems while supercomputers manage large-scale numerical workloads, thereby combining the strengths of both technologies (Bauer et al., 2020).

Quantum computers are not expected to become consumer products for private households or everyday users. Instead, they are expected to function primarily through cloud-based services, like current models used to access high performance computing infrastructures. This model enables organisations, researchers, and companies to utilize quantum resources without maintaining the highly specialized cryogenic and electromagnetic environments required to operate quantum hardware (IBM Research, 2023). For instance, several technology providers already offer access to quantum processors through cloud platforms with subscription-based or monthly usage models, allowing users to experiment with quantum algorithms in controlled and scalable environments (Arute et al., 2019).

Furthermore, quantum computers may offer significant advantages in energy efficiency when compared with traditional supercomputers. Although cryogenic support systems require highly specialized cooling. Quantum processors themselves can execute certain types of computation using substantially less energy than classical computers (Gyongyosi & Imre, 2019). Some assessments indicate that, for specific computational tasks, quantum devices may operate with orders of magnitude lower energy consumption. This is an important factor for the sustainability of future high-performance computing strategies. As quantum technologies continue to mature, their integration with existing

supercomputing infrastructures may therefore enhance computational capabilities while simultaneously contributing to broader environmental and economic benefits (Preskill, 2018).

4. Quantum regulations

Many parties are rushing with new regulations concerning quantum era. International regulation frameworks guide the governments and companies all together. Setting standards creates a set of rules for quantum to be conducted fairly and responsibly in organisations. Regulations also support ethical use and new innovations for quantum with organisations like GDPR, NIST, WHO and many directives and privacy laws.

4.1 GDPR

The European Union's General Data Protection Regulation (GDPR) has become the global benchmark for data privacy. GDPR set out obligations for controllers and processors to protect personal data through appropriate technical and organisational measures (GDPR, 2018, art. 32). While the GDPR was drafted before the full rise of quantum computing as a mainstream policy issue, its open-ended "state of the art" clause means that organisations must continually reassess their security practices considering emerging threats. The impending advent of large-scale quantum computers represents precisely such a disruptive development.

Quantum computers have the potential to undermine today's cryptographic foundations that expose encrypted personal data to retrospective compromise. In this context, the transition to PQC is not merely a technical migration. It is a regulatory requirement tied directly to GDPR's integrity and confidentiality principles (European Data Protection Board [EDPB], n.d.). This paper explores the intersection of GDPR and PQC, demonstrating why organisations subject to GDPR should integrate PQC into compliance strategies.

4.1.1 GDPR's security requirements and the role of encryption

GDPR embeds two fundamental principles. The integrity and confidentiality of personal data (GDPR, 2018, art. 5). To operate these, Article 32 requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (GDPR, 2018). Importantly, GDPR highlights encryption as an example of such a measure.

The regulation does not mandate specific cryptographic algorithms. Still regulation obliges organisations to consider latest technology, implementation cost, processing nature, and risk severity when

determining security controls (GDPR, n.d.). This open-textured standard is intentional, enabling GDPR to remain technologically neutral and ready to bend when needed. This standard is ready to evolve as new threats emerge.

The European Data Protection Board has consistently emphasized that encryption is a primary tool for ensuring confidentiality and should be deployed where feasible. Particularly for cross-border data transfers and sensitive processing activities (EDPB, n.d.). From this perspective, PQC naturally fits as the logical next step in encryption's evolution.

4.2 NIST and NIS 2 directive

Quantum computing introduces a disruptive challenge to cybersecurity by undermining classical cryptographic schemes such as RSA, ECDSA, and elliptic curve Diffie-Hellman. To mitigate this risk, both the United States and the European Union are advancing frameworks for post-quantum cryptography (PQC). NIST is standardising quantum-resistant algorithms, while in the EU the NIS 2 directive (Directive (EU) 2022/2555) mandates improved cyber-risk management across critical sectors (Council of the European Union & European Parliament, 2022). Together, these initiatives reflect a global movement to prepare for the quantum era.

4.3 EHDS

The European Health Data Space Regulation (EHDS) entered into force in March 2025. EHDS established a common legal framework for accessing and sharing electronic health data across the European Union (European Union, 2025). The regulation mandates the use of secure processing environments, health data access bodies, and harmonised infrastructure components. These are to support both primary and secondary uses of health data.

Although the regulation places strong emphasis on secure data handling, interoperability, and governance, it does not currently mandate PQC standards as part of its technical requirements. Instead, detailed technical guidance and implementation specifications are still under development. These may shape how organisations operationalise secure processing environments under the EHDS framework (TEHDAS2 Joint Action, 2025).

At the same time EU-funded initiatives such as the QUANTUM project demonstrate an increasing policy. Policy focuses on data quality, governance, and trusted data ecosystems within the EHDS context. These initiatives signal a broader regulatory trajectory. In which advanced security practices are

likely to become integral to organisational compliance and risk management in the health sector. Including future cryptographic requirements (European Commission, 2024).

4.4 NIST with standardisation of PQC

NIST launched its Post-Quantum Cryptography project to identify, evaluate, and standardize cryptographic algorithms resilient to quantum attacks (NIST, n.d.-a). After multiple rounds of competition, NIST announced its first standards in 2024, finalising ML-KEM for key encapsulation and ML-DSA / SLH-DSA for digital signatures, published as FIPS 203–205 (NIST, 2024). More recently, in March 2025, HQC was selected as a fifth algorithm for encryption as a backup option (NIST, 2025).

Beyond standardization, NIST has issued guidance for migration. For example, NIST IR 8547 outlines best practices for transition strategies, emphasising hybrid cryptographic approaches, risk assessment, and lifecycle planning (NIST, 2023). Organisations are urged to prepare early, adopting hybrid classical–quantum schemes during the transition phase while ensuring interoperability (NIST, 2025).

NIST's recommendations highlight several priorities. Firstly, hybrid deployment prefers to use PQC in tandem with classical methods during migration to full PQC (NIST, 2023). Secondly there are the performance trade-offs that are about larger key sizes and computational overhead for quantum computers to struggle with (Utimaco, 2024). Third pick is about security assurance. By monitoring new analytic results and maintaining conservative margins. (NIST, n.d.-a) Lastly deprecation roadmap. By preparing for gradual phase-out of PQC algorithms (AppViewX, 2024). These requirements reflect a proactive stance, encouraging organisations to begin pilots and integrate PQC readiness into procurement and risk governance.

4.5 NIS 2 directives scope and obligations

In the Europe, the NIS 2 Directive significantly broadens cybersecurity obligations for both essential and important entities (Council of the European Union & European Parliament, 2022). It requires technical and organisational controls including risk management, incident reporting, supply chain security, and governance oversight (NiS2 directive, 2022). Member States must transpose NIS 2 into national law by October 2024, after which organisations will be directly accountable (Entrust, 2023).

While NIS 2 does not explicitly mention PQC, it emphasizes latest cybersecurity practices. Analysts interpret this as implying that PQC readiness may become expected under NIS 2, particularly for critical infrastructure (NIS2 directive, 2022) The European Commission has also published a Coordinated PQC Roadmap recommending that Member States begin transitions by 2026, with critical systems

migrated no later than 2030 (European Commission, 2024). This urges member states and critical operators to begin adopting hybrid classical-PQC schemes. This policy trajectory makes it increasingly likely that GDPR enforcement authorities will interpret PQC readiness as part of appropriate measures. Or in other words, compulsory for organisations.

Integrating PQC into NIS 2 compliance

Organisations facing NIS 2 obligations should integrate PQC planning into compliance strategies. This may include conducting cryptographic inventories, piloting hybrid algorithms, requiring vendor support for PQC, and aligning governance frameworks with EU-level roadmaps (ENISA, 2023). Documenting these steps provides evidence of suitable and the right kind measures, strengthening both compliance and resilience.

The combined force of NIST's PQC standardisation and the NIS 2 directive's regulatory mandate points toward a future where PQC adoption is both a technical necessity and a legal expectation. Even if not explicitly required, aligning NIS 2 compliance with PQC migration allows organisations to safeguard critical operations and prepare for the disruptive power of quantum computing.

4.6 PQC threats under GDPR

Quantum computing poses a dual threat to GDPR compliance. Algorithms such as Shor's can solve the integer factorization and discrete logarithm problems underlying RSA and elliptic curve cryptography (NIST, n.d.). This means data encrypted with today's widely deployed systems could be decrypted almost instantly on a sufficiently powerful quantum computer.

Secondly is the mentioned harvest now, decrypt later (HNDL) model compounds risk. This is an urgent risk of data confidentiality. Adversary that can intercept and store encrypted data means harm on global scale without precaution. Data that has a long lifetime or high value is under threat. Just to wait until quantum resources are mature to decrypt it (Encryption Consulting, 2024). This model is especially relevant to GDPR, given that many categories of personal data must be stored for years or decades. Health records, financial data, or government archives encrypted with classical methods could be exposed retroactively, undermining GDPR's confidentiality principle (HashiCorp, 2025).

ENISA, the EU's cybersecurity agency, has echoed these concerns. ENISA published guidance on quantum-readiness and highlighting PQC migration as a strategic priority (KBI Media, 2024). Together, these developments suggest that GDPR compliance and PQC migration are converging paths particularly in Public Key Infrastructure (PKI) systems, TLS libraries, and hardware security modules.

4.7 Compliance strategies that bridge GDPR and PQC

Organisations seeking to align GDPR obligations with PQC can consider a structured approach. Cryptographic planning and risk assessment about GDPR's accountability principle requires controllers to document processing operations and associated risks (GDPR, 2018, art. 30). Extending this to cryptography, organisations should plan how and where encryption is applied. Algorithms noted, key lengths, and certificate lifecycles. This assessment allows prioritisation of systems most exposed to quantum threats, such as those storing long lifetime data (HashiCorp, 2025).

NIST recommends hybrid cryptography schemes that combine classical and PQC algorithms during transition (NIST, 2023). This dual protection demonstrates to regulators that controllers are adopting proportionate, forward-looking measures. Under GDPR, this could evidence compliance with the "appropriate technical measures" obligation (GDPR, n.d.).

GDPR emphasize ongoing accountability. Systems should therefore be architected for agility and upgradeability. The ability to swap cryptographic primitives without fundamental redesign (ICO, 2023). Crypto-agile infrastructures ensure that future PQC improvements can be adopted seamlessly, limiting risk of non-compliance. Also, the agile rollback feature is important to implement in planning.

Governance and documentation are for Senior management that are accountable for GDPR compliance (GDPR, 2018, art. 24). Documenting PQC migration strategies, risk assessments, and testing plans strengthens governance evidence and provides demonstrable compliance.

Quantum research and EU policy are dynamic by nature. Organisations must monitor guidance from the European Commission (ENISA) and National data protection authorities (European Commission, 2024). Such monitoring ensures ongoing alignment with GDPR's evolving "state of the art" standard with regulatory and documentation.

The integration of PQC into GDPR compliance presents several challenges. Costs, redo work with algorithms, legacy systems and political ambiguous enforcement with cross border operations. PQC algorithms such as lattice-based KEMs typically require larger key sizes, leading to increased bandwidth and processing costs (NIST, 2025). The uncertainty in cryptanalysis with PQC can produce redo work because PQC is relatively young. Algorithms standardized today may tomorrow prove weak, raising compliance risks if adopted prematurely (NIST, 2025). Legacy Systems and embedded platforms may lack upgrade paths that complicates PQC rollout across entire infrastructures. GDPRs ambiguous enforcement currently does not mandate PQC explicitly. However, supervisory authorities

may interpret the “state of the art” clause expansively, especially considering commission roadmaps (European Commission, 2024).

To mitigate these challenges, regulators should issue explicit PQC guidance under GDPR. Also, the new ISO standard for PQC can framework the setup for organisations that align with the Commission’s 2024 roadmap. Organisations should adopt phased strategies that combine hybrid deployments with governance and IT partners’ oversight. This ensures crypto agility for future updates.

GDPR’s technological neutrality ensures its relevance across decades, but this same neutrality requires proactive interpretation by controllers. The emergence of quantum computing means that classical encryption will not remain “state of the art” anymore. To satisfy GDPR’s obligations for confidentiality, integrity, and accountability (CIA), organisations must therefore instantly prepare for PQC. Adoption of PQC is not merely a technical upgrade. It is a compliance obligation rooted in GDPR’s core principles. Organisations can both prove their security and demonstrate regulatory diligence with these steps. Organisations should conduct cryptographic planning, deploy hybrid schemes, build crypto-agile infrastructures, and monitor regulatory guidance. As EU policy increasingly emphasizes quantum readiness, PQC will become the natural standard for GDPR compliance in the quantum era.

5. Quantum era

Modern cryptographic systems rely on both symmetric and asymmetric encryption, which serve complementary roles. Symmetric encryption uses a single shared secret key for both encryption and decryption. It is computationally efficient and well suited for protecting large volumes of data in transit and at rest. Algorithms such as the AES are therefore widely used across governmental, industrial, and commercial systems (Diffie & Hellman, 1976; IBM, 2025). Symmetric encryption remains a core component of secure digital systems because of its speed, scalability, and operational efficiency.

Asymmetric encryption relies on a pair of mathematically related keys. A public key is used for encryption, while a private key is used for decryption. This structure enables secure key exchange, digital signatures, and authentication without the need to share a secret key in advance. Widely deployed asymmetric systems such as RSA, elliptic curve cryptography, and Diffie Hellman rely on mathematical problems that are difficult for classical computers to solve within a practical timeframe (Diffie & Hellman, 1976).

The emergence of quantum computing fundamentally changes this assumption. Shor's algorithm demonstrates that a sufficiently powerful quantum computer could efficiently solve the mathematical problems that underpin classical asymmetric cryptography. This would render RSA, elliptic curve cryptography, and classical Diffie Hellman insecure once large-scale fault tolerant quantum computers become available (Shor, 1997; Preskill, 2018). While such systems do not yet exist, the risk is considered foreseeable rather than hypothetical, particularly for data with long confidentiality requirements.

This risk is amplified by the HNDL model in the future when quantum capabilities mature. Because encrypted data can retain value for many years, organisations cannot rely solely on current cryptographic strength. Planning for cryptographic transition is therefore required well before quantum computers reach practical attack capability (Chen et al., 2016; Mosca, 2018).

In response to this challenge, the cryptographic community has developed PQC. These algorithms are designed to resist attacks from both classical and quantum computers and are based on alternative mathematical assumptions. The NIST has standardised a first set of post quantum algorithms to support long term transition. These include ML KEM for key establishment, ML DSA as the primary digital signature scheme, SLH DSA as a conservative hash-based alternative, FN DSA for constrained environments, and HQC as a backup key encapsulation mechanism to support algorithmic diversity (NIST, 2024; NIST, 2025).

The transition to post-quantum cryptography will affect a wide range of digital services. Secure web communications, virtual private networks, cloud authentication systems, financial services, and governmental communication platforms all depend on public key cryptography and will require migration to quantum-resistant alternatives. To manage this transition safely, hybrid cryptographic approaches are already being recommended to preserve security and interoperability during the migration period while reducing implementation risk (Chen et al., 2016; National Institute of Standards and Technology, 2023).

From an organisational perspective, symmetric encryption remains largely resistant to quantum attacks when sufficiently strong key lengths are used. In contrast, traditional asymmetric systems face structural vulnerabilities in the quantum era. The adoption of PQC is therefore not a theoretical exercise, but a practical requirement for maintaining confidentiality, integrity, and availability. Trust in digital systems over the coming decades need to be robust. The challenge is no longer whether post quantum cryptography will be needed, but how and when it should be implemented as part of long-term cybersecurity governance. One way to deal with PQC can be with PQC itself.

6. Methodology of research survey

This research study investigates emerging changes in Post-Quantum Cryptography (PQC) and their implications for information security within the Finnish health and social care (SOTE) sector. The purpose of the research is to assess awareness, preparedness, and perceived challenges that organisations may face in adapting to PQC technologies as part of broader cybersecurity frameworks.

The study is supervised by Evdokimos Konstantinidis from the University of Thessaloniki.
The data collection method chosen is an anonymous online survey, distributed to a limited group of professionals responsible for information security management within Finnish healthcare and social service organisations. After the first phase. The research surveys scope was widened to professional cybersecurity groups in Finland.

This approach was selected to obtain practical, experience-based insights from individuals who directly influence cybersecurity preparedness and compliance decisions at the organisational level.

6.1 Survey method

The survey was designed and implemented using Microsoft Forms (MS Forms) due to its accessibility, ease of use, and secure data handling features. Respondents receive the survey link by email from ISCTE Lisbon Univ., accompanied by a concise introduction message explaining the purpose of the research, its academic background, and the assurance of anonymity.

Email distribution was intentionally chosen to establish trust and ensure that potential respondents understand that the study is legitimate, ethical, and academically motivated. Study was made in Finnish for the audiences and clear understanding of the questions. The estimated completion time of approximately three minutes supports higher response likelihood among busy professionals and respects their valuable time.

The survey consists of seven structured questions with both multiple-choice and open-ended options to allow for quantitative and qualitative insights.

6.2 Target group and scope

First the target group comprised information security officers, IT managers, and cybersecurity specialists working in Finland’s health and social care sector (SOTE).

This group was selected because they are directly involved in implementing and maintaining data protection measures, managing compliance with the NIS Directive, and responding to new regulatory and technological challenges, including quantum-safe cryptography.

The survey research was deliberately limited to a small, focused sample (initially 21 invited respondents). Finland has 21 welfare areas, and each has one responsible “inhouse” Chief Information Security Officer. The goal is to obtain high-quality, expert-level feedback that provides depth rather than broad statistical representation. A future phase could expand the study to a wider national sample once the initial patterns and challenges are identified.

6.3 Changes to survey scope

With a total of one response from welfare areas (21), the survey had to be published to several other groups to reach some responses to ongoing research survey. After 2 months the change of scope dropped health and social care IT personnel only out and was made available to four closed professional cybersecurity groups in Finland. Study was ultimately published into two closed WhatsApp groups that have 899 IT security experts in total. Survey was also published into two closed cybersecurity groups in LinkedIn with 1800 members. From these groups the total number of responses rose to 29. The original survey was made in Finnish. This English translation was never used as is.

The research survey was planned to open on 10 September 2025, and the final reminder for the social and healthcare organizations was sent on 7 November 2025. Despite these efforts, the number of responses received remained at zero. Identifying the correct email addresses for potential respondents proved considerably more challenging than initially anticipated, partly because contact information for cybersecurity officers was often not publicly available. As a result, locating appropriate recipients required manual investigation, including phone calls and systematic examination of organizational websites. Eventually, general cybersecurity contact addresses were identified, although reaching specific individuals remained difficult.

An additional complication emerged when messages sent from the university domain (formatted as firstname.lastname@iscte-iul.pt) were systematically quarantined in at least one security-sensitive organization. This issue prevented the survey invitations from reaching the intended recipients and significantly limited the feasibility of collecting data as originally planned. Consequently, the scope of the study required reassessment and subsequent refinement to align with the data that could realistically be obtained under these constraints. The study is subject to limitations related to sample size and data collection constraints. The results should therefore be interpreted as indicative rather than

statistically generalisable, while still providing valuable exploratory insights into organisational preparedness.

6.4 Research survey questions

The question concerning the respondent's job role is justified because organisational position influences exposure to cybersecurity responsibilities and is known to shape security awareness and decision-making capabilities, which studies on organisational cybersecurity behaviour, have demonstrated (Parsons et al., 2014).

What is your job role? (Select from the options or provide your own)

Information Security Officer

Information Security Specialist

IT Specialist

Chief Information Security Officer (CISO) / Director of Information Security

Senior Cybersecurity Specialist

Manager / Supervisor

Chief Information Officer (CIO) Head of IT Management

The second question about the industry sector is warranted because sectoral differences in regulatory environments, risk landscapes and technology dependence strongly affect cybersecurity readiness and adoption of emerging technologies, as sector-based security research has shown (Mellado et al., 2010).

What is your industry sector? (Select the sector in which you primarily work or provide your own)

Finance

Public Sector

Public Administration

Education

Education Sector

Consumer Products

Agriculture, Forestry and Food Sector

Service Sector

Banking and Finance

Defence

Health and Social Care Sector

Industry and Manufacturing

Information and Communications Technology (ICT) Sector

State Government

The third question regarding prior awareness of quantum-safe security is essential because awareness is a foundational predictor of adoption about willingness. This represents a key component of security culture, as highlighted in empirical studies on emerging cybersecurity technologies (Rogers, 2003).

Have you heard about quantum safe security (Post-Quantum Cryptography, PQC)?

Yes, I am well familiar with the topic

Yes, somewhat familiar

Yes, I have heard of it but have not examined it in detail

I have not heard about the topic

I don't know

Other

The fourth question about whether the organisations have a formal PQC plan is appropriate because strategic preparedness and business planning that are central determinants of successful security transitions, as demonstrated in research on proactive cybersecurity governance and organisational resilience (Björck et al., 2015).

Does your organization have a plan regarding PQC?

Yes plan completed and in use

Yes plan in progress

Not yet but discussions ongoing

No plan

Other

Fifth question on dependence on vulnerable encryption is justified because current reliance on classical cryptographic schemes determines the urgency of migration and aligns with studies that asses systemic cryptographic risk under future quantum threats (Mosca, 2018).

How would you assess your current systems' dependency on encryption methods that could be broken by quantum computers?

Fairly dependent

Highly dependent multiple critical systems

Minimal dependence

I don't know

The sixth question on obstacles to PQC adoption is academically supported because identifying perceived organisational barriers provides insight into capability gaps, resource constraints and innovation resistance. All these are widely recognized factors in cybersecurity change processes (Renaud, 2016).

What are the biggest obstacles you see for adopting PQC in your organization? (Select the most relevant/s max 5.)

Technological uncertainty solutions still in progress

Lack of management or decision making support

No significant obstacles

Lack of resources time or money

Lack of skills or training

Lack of guidelines and standards

Technology vendor support and solution compatibility especially considering some legacy technologies

Prioritization of development tasks

Legacy systems compatibility requirements

We expect service providers to deliver secure services including PQC capabilities if needed

Complexity of technology environment

The matter is not seen as urgent enough to require prioritization

The seventh question regarding the importance of PQC readiness relative to other cybersecurity needs is about prioritization influences resource allocation. Strategic direction and perceived importance have been shown to predict organisational adoption behavior in security domains (Ifinedo, 2013).

How important do you consider developing PQC readiness compared to other cybersecurity or health and social care sector requirements?

As very important, high priority

Important, but not the most urgent

As a medium requirement

As a rather minor requirement

Not important right now

I don’t know

The eight question about preferred forms of external support is warranted for governmental guidance, capacity building measures and regulatory clarity that have been found to significantly influence adoption of advanced cybersecurity practices. Particularly in public-sector and highly regulated environments (Bade et al., 2019).

How would you like to see authorities or national actors supporting the PQC transition within health and social care organizations?

Clear guidance and standards

Training and skills development

Funding support or project financing

Shared pilots and peer networks

Providing technical expert assistance

Other

In addition to the dominant barriers, a small number of respondents mentioned more context-specific challenges related to legacy systems, vendor dependencies, prioritization constraints, and perceived urgency. While these factors were not widely shared, they highlight the heterogeneity of organizational contexts in which PQC adoption decisions are made.

6.5 Results and analysis: Post-Quantum Cryptography (PQC) Readiness Survey

These results and figures are made with Python code script print-out.

1. Awareness of PQC

Have you heard about quantum safe security (Post-Quantum Cryptography, PQC)?

Number of valid responses: 29

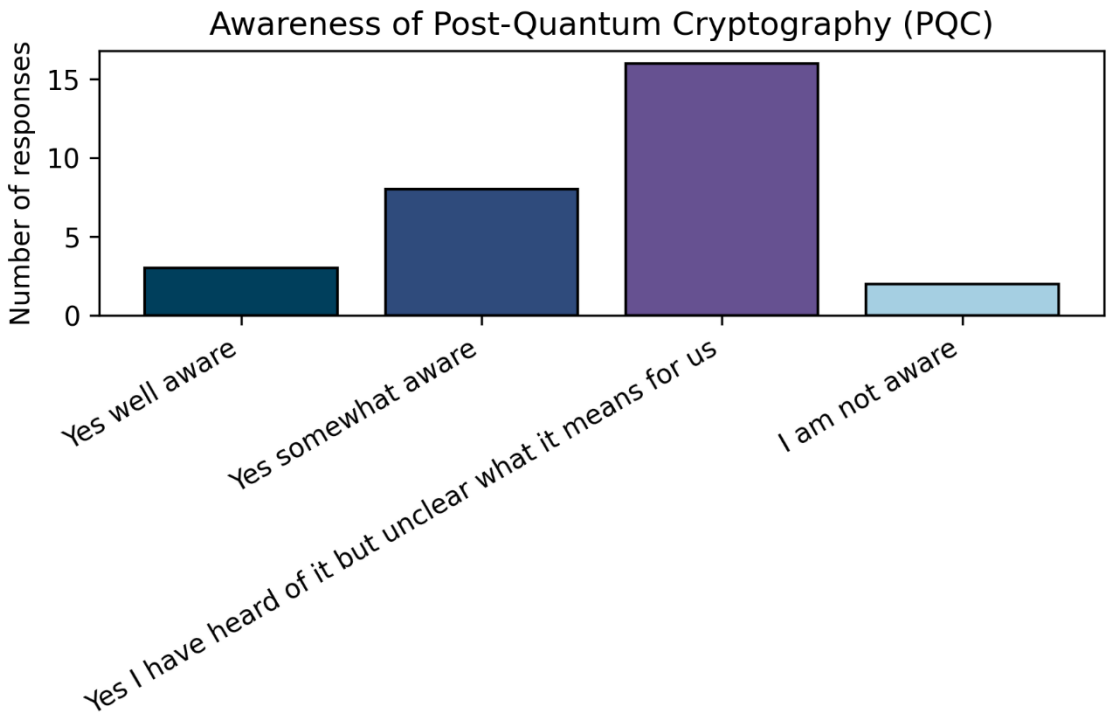


Figure 2: 6.1 Authors own work (2025)

Response distribution:

- Yes I have heard of it but unclear what it means for us: 16 (55.2%)
- Yes somewhat aware: 8 (27.6%)
- Yes well aware: 3 (10.3%)
- I am not aware: 2 (6.9%)

Interpretation:

The dominant category is 'Yes I have heard of it but unclear what it means for us' (55.2%), indicating a relatively concentrated pattern in this item.

2. Job role profile

What is your job role? (Select from the options or provide your own)

Number of valid responses: 29

Response distribution:

- Information Security Officer: 12 (41.4%)
- IT Specialist: 5 (17.2%)
- Manager / Supervisor: 5 (17.2%)
- Information Security Specialist: 3 (10.3%)
- Chief Information Security Officer (CISO) / Director of Information Security: 1 (3.4%)
- Senior Cybersecurity Specialist: 1 (3.4%)
- Chief Information Officer (CIO) Head of IT Management: 1 (3.4%)
- Code 8 (label not defined): 1 (3.4%)

Interpretation:

The dominant category is 'Information Security Officer' (41.4%), indicating a relatively concentrated pattern in this item.

3. Dependency on quantum-vulnerable encryption

How would you assess your current systems' dependency on encryption methods that could be broken by quantum computers?

Number of valid responses: 29

Descriptive statistics:

- Mean: 2.31
- Median: 2
- Standard deviation: 1.05
- Quartiles (Q1, Q2, Q3): (1.5, 2, 3.0)

Methodological note: The mean value is reported as a descriptive summary indicator. As the response scale is ordinal, the mean should be interpreted directionally rather than as a precise measurement.

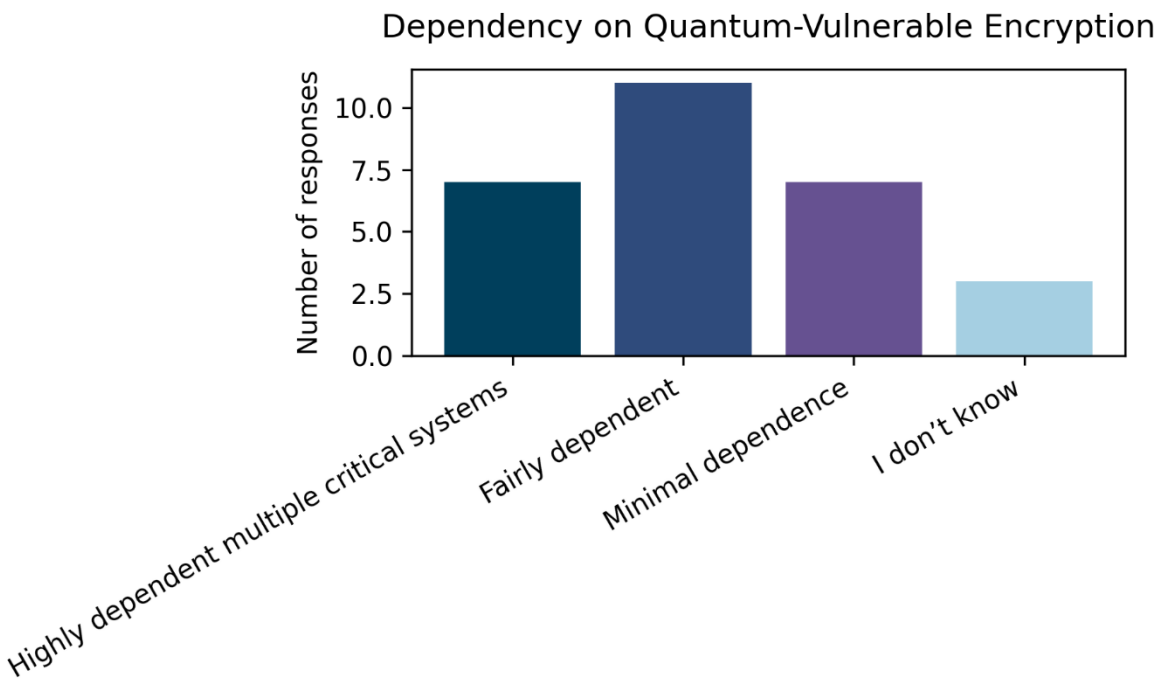


Figure 3: 6.2 Authors own work (2025)

Response distribution (ordered low → high):

- Highly dependent multiple critical systems: 7 (24.1%)
- Fairly dependent: 11 (37.9%)
- Minimal dependence: 7 (24.1%)
- I don’t know: 3 (10.3%)
- Code 5 (label not defined): 1 (3.4%)

Interpretation:

The most common response is 'Fairly dependent' (37.9%). The mean of 2.31 suggests responses lean toward the lower end of the scale.

4. Importance of PQC readiness

How important do you consider developing PQC readiness compared to other cybersecurity or health and social care sector requirements?

Number of valid responses: 29

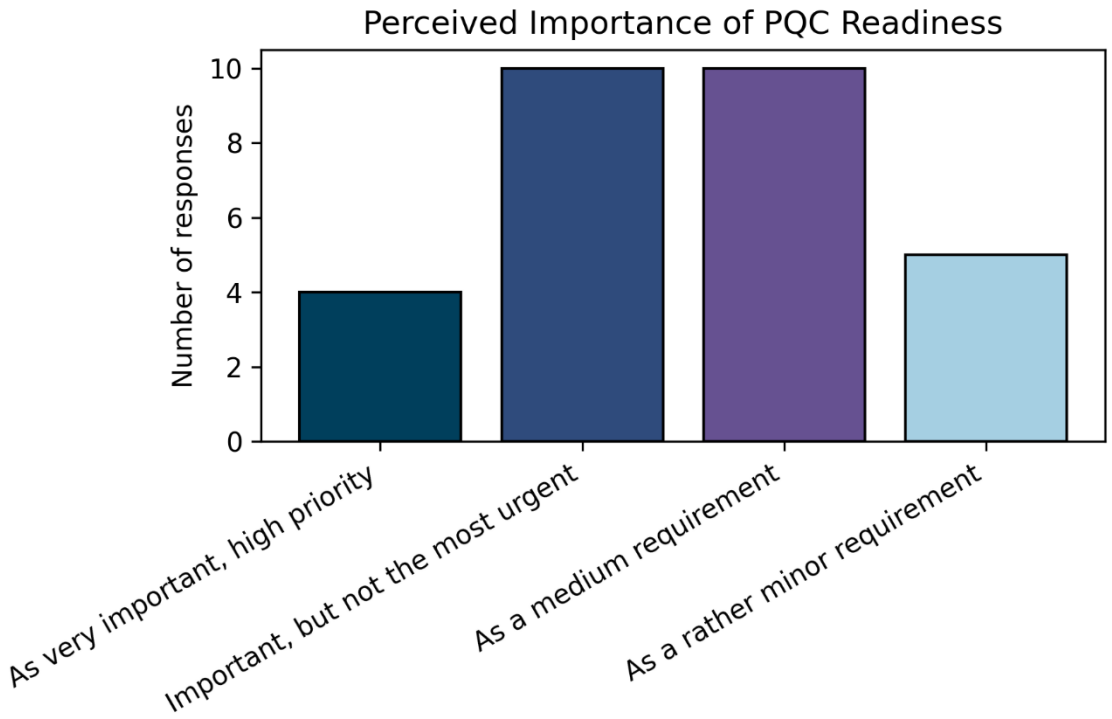


Figure 4: 6.3 Authors own work (2025)

Descriptive statistics:

- Mean: 2.55
- Median: 3
- Standard deviation: 0.93
- Quartiles (Q1, Q2, Q3): (2.0, 3, 3.0)

Methodological note: The mean value is reported as a descriptive summary indicator. As the response scale is ordinal, the mean should be interpreted directionally rather than as a precise measurement.

Response distribution (ordered low → high):

- As very important, high priority: 4 (13.8%)
- Important, but not the most urgent: 10 (34.5%)
- As a medium requirement: 10 (34.5%)

- As a rather minor requirement: 5 (17.2%)

Interpretation:

The most common response is 'As a medium requirement' (34.5%). The mean of 2.55 suggests responses lean toward the higher end of the scale.

5. Organizational Barriers to PQC Adoption

What are the biggest obstacles you see for adopting PQC in your organization? (Select the most relevant)

All respondents selected at least one obstacle, yielding a total of 73 obstacle mentions.



Figure 5: 6.4 Authors own work (2025)

Ranked obstacles (long-tail grouped):

- Technological uncertainty solutions still in progress: 15 (20.5%)
- Lack of resources, time or money: 15 (20.5%)

- Lack of skills or training: 14 (19.2%)
- Lack of guidelines and standards: 13 (17.8%)
- Lack of management or decision-making support: 8 (11.0%)
- Other context-specific obstacles (aggregated): 8 (11.0%)

Interpretation:

The leading barriers are concentrated around 'Technological uncertainty solutions still in progress', 'Lack of resources time or money', 'Lack of skills or training'. This suggests that capability, resourcing, and uncertainty factors dominate over niche technical constraints.



Figure 6: 6.5 Authors own work (2025)

Research survey analysis

Understanding how health and social care organisations prepare for emerging cryptographic requirements has become increasingly important as quantum technologies evolve. Post-Quantum Cryptography (PQC) is expected to reshape how critical sectors secure sensitive information, yet little empirical data exists on how organisations perceive this transition. This survey-based study provides a basic view of awareness, readiness, and perceived challenges related to PQC within Finland's health and social care sector. Although the findings are not statistically generalizable due to a limited number of respondents, they offer an early snapshot of professional perspectives and contribute to the growing discourse on quantum-safe cybersecurity.

Methodological overview

The study utilized an anonymous online survey developed with Microsoft Forms and disseminated through email and professional cybersecurity groups. The survey sought input from individuals who hold direct responsibility for information security management within the Finnish SOTE sector, including Chief Information Security Officers, IT managers, and cybersecurity specialists. The initial target sample consisted of 21 welfare area CISOs. After receiving only one response, the survey distribution was expanded to closed WhatsApp professional groups and LinkedIn cybersecurity communities, ultimately resulting in 29 completed responses.

The survey comprised seven structured questions integrating multiple-choice and open-ended formats. This mixed-methods structure allowed the generation of both quantitative indicators and qualitative reflections, consistent with basic research traditions.

Data analysis strategy

Data analysis was performed using descriptive statistical techniques to identify broad patterns across responses. Open-ended answers underwent thematic analysis, enabling the identification of recurrent ideas, perceived obstacles, and contextual explanations that enrich the quantitative findings. As this study is exploration in scope, the analysis emphasizes conceptual insights rather than generalizable statistical conclusions.

Because the total number of responses (n = 29) is well below what is typically required for statistically valid sector-wide claims, the results should be interpreted as indicative phenomena rather than representative facts. This limitation is discussed explicitly in the interpretation of findings.

6.6 Research survey summary

This basic study offers an early look at how Finnish health and social care professionals understand and prepare for the transition to post-quantum cryptography. While the limited sample size restricts generalizability, the findings highlight important themes, including uneven awareness levels, early-stage organisational planning, and a possible need for national guidance and resources. These insights set the foundation for more comprehensive future research and support the ongoing conversation about quantum-safe cybersecurity in critical public-sector environments. As the importance of PQC continues to rise, understanding practitioner perspectives will remain essential for guiding national preparation and policy development.

7. Results

This chapter summarises the key findings of the Post Quantum Cryptography readiness survey. The survey received 29 valid responses. Most respondents worked in information security or IT roles. Information Security Officers formed the largest group at 41.4 percent. This means the results reflect an operational security viewpoint rather than a purely executive viewpoint.

Awareness of post quantum cryptography was present but shallow. Most respondents had heard of quantum safe security but did not understand what it means for their organisation. This group represented 55.2 percent of responses. A smaller share reported being somewhat aware at 27.6 percent. Only 10.3 percent reported being aware. A minority of 6.9 percent were not aware.

Organisations reported meaningful dependence on encryption methods that could become vulnerable in the quantum era. The most common response was dependent at 37.9 percent. A further 24.1 percent reported high dependence across multiple critical systems. Another 24.1 percent reported minimal dependence. Around 10.3 percent did not know their level of dependence. This indicates that visibility into cryptographic exposure is still incomplete.

Post quantum readiness was generally seen as relevant but not yet treated as the most urgent cybersecurity issue. The most common responses were important but not the most urgent at 34.5 percent and a medium requirement at 34.5 percent. Only 13.8 percent rated it as a very important high priority. This suggests that PQC is acknowledged but competes with other immediate security and sector requirements.

The most frequently reported barriers were practical and organisational. Respondents most often selected technological uncertainty and lack of proven solutions. Lack of resources and lack of skills

were also among the leading barriers. Lack of guidelines and standards was another common barrier. Lack of management support was reported less frequently but still present. Overall, the barriers indicate that uncertainty, resourcing, and capability gaps dominate over purely technical obstacles.

Respondents also indicated a need for external support to enable progress. The most requested forms of support were clear guidance and standards, training and skills development, and technical expert assistance. Funding support and shared pilots were also mentioned. This points to a readiness model where national guidance, vendor maturity, and coordinated migration support are important drivers of organisational action.

8. Conclusion

This thesis examined organisational preparedness for post-quantum cybersecurity in response to the foreseeable impact of quantum computing on existing cryptographic systems. The central finding is that quantum computing represents a delayed but systemic cybersecurity risk rather than an immediate technical disruption. Encrypted data with long-term value is already exposed through the harvest now, decrypt later threat model (HNDL). HNDL shifts cybersecurity planning from short-term incident response toward long-term strategic risk management.

Post-quantum cryptography (PQC) is not a future technical upgrade but an emerging governance and compliance challenge. Regulatory frameworks in both the European Union and the United States increasingly signal that cryptographic resilience must be maintained against foreseeable technological developments. Even where PQC is not yet explicitly mandated, expectations around “state of the art” security practices are evolving in a way that makes delayed preparation increasingly difficult to justify.

The analysis of quantum computing technologies demonstrated that headline metrics such as qubit counts do not translate directly into cryptographically relevant capability. Instead, error rates, coherence times, logical qubit construction, and ecosystem maturity determine when quantum computers will pose practical risks to classical public-key cryptography. This reinforces for organisations the need to base decisions on risk indicators and migration timelines rather than speculative predictions or marketing claims.

The research survey conducted within Finnish professional cybersecurity communities revealed that awareness of post-quantum cryptography exists but remains shallow. Most organisations acknowledge relevance but do not yet treat PQC as a high-priority initiative. The primary barriers

identified were technological uncertainty, lack of skills, limited resources, and insufficient guidance. These findings suggest that organisational inaction is driven more by uncertainty and capability gaps than by resistance or denial of risk.

Across the preceding analysis, organisational preparedness emerges as a set of practical governance and architectural actions. These include maintaining a cryptographic inventory, designing systems for cryptographic agility, deploying hybrid classical–post-quantum solutions during migration, assessing vendor readiness, and documenting transition plans. Together, these measures reduce long-term exposure while remaining compatible with current operational constraints.

This thesis contributes to organisational cybersecurity research by framing PQC as a strategic preparedness issue rather than a purely technical problem. It highlights the importance of aligning technological risk assessment with regulatory expectations, investment signals, and organisational capability development. Future research could expand empirical analysis across additional sectors and jurisdictions, but the core conclusion remains clear. Quantum-safe cybersecurity is no longer optional planning for a distant future. It is a present-day responsibility for organisations that manage sensitive and long-lived data.

9. References

Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature* **614**, 676–681 (2023). https://doi.org/10.1038/s41586-022-05434-1

AppViewX. (2024). Key takeaways from NIST guidance on transitioning to post-quantum cryptography. https://www.appviewx.com/blogs/key-takeaways-from-the-latest-nist-guidance-on-transitioning-to-post-quantum-cryptography

Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574, 505–510. https://doi.org/10.1038/s41586-019-1666-5

Bauer, B., Bravyi, S., Motta, M., & Chan, G. K.-L. (2020). Quantum algorithms for quantum chemistry and quantum materials science. Chemical Reviews, 120(22), 12685–12717. https://doi.org/10.1021/acs.chemrev.9b00829

Björck, F., Henkel, M, Stirna, J. and Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography (NISTIR 8105).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Council of the European Union, & European Parliament. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Cybersecurity and Infrastructure Security Agency. (2023). Post-quantum cryptography initiative: Preparing for the quantum computing transition. U.S. Department of Homeland Security. https://www.cisa.gov/quantum

Council of the European Union, & European Parliament. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Council of the European Union, & European Parliament. (2022). Directive (EU) 2022/2555 (NIS 2 Directive). Official Journal of the European Union. http://data.europa.eu/eli/dir/2022/2555/oj

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Encryption Consulting. (2025). Harvest now, decrypt later: Managing quantum risk in cryptographic systems. https://www.encryptionconsulting.com/education-center/harvest-now-decrypt-later/

Engel, G. S., Calhoun, T. R., Read, E. L., Ahn, T.-K., Mančal, T., Cheng, Y.-C., Blankenship, R. E., & Fleming, G. R. (2007). Evidence for wavelike energy transfer through quantum coherence in photosynthetic systems. *Nature, 446*(7137), 782–786. https://doi.org/10.1038/nature05678

ENISA. (2024). Navigating cybersecurity investments in the time of NIS2. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

Entrust. (2023). What is Post-Quantum Cryptography and Why is it Important? https://www.entrust.com/resources/learn/post-quantum-cryptography

European Commission. (2024). Commission Recommendation (EU) 2024/1101 on a coordinated implementation roadmap for the transition to post-quantum cryptography. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reco/2024/1101/oj/eng

European Union. (2025). Regulation (EU) 2025/327 establishing the European Health Data Space. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2025/327/oj

Flamini, F., Spagnolo, N., & Sciarrino, F. (2018). Photonic quantum information processing: A review. Reports on Progress in Physics, 82(1), 016001. https://doi.10.1088/1361-6633/aad5b2

Fu, JB., Li, B., Zhang, XF. *et al.* (2021). Experimental review on Majorana zero-modes in hybrid nanowires. *Sci. China Phys. Mech. Astron.* 64, 107001 https://doi.org/10.1007/s11433-021-1737-4

Gambetta, J. M., et al. (2015). Building logical qubits in a superconducting quantum computing system. Nature Physics, 18(2), 118–125. https://doi.org/10.48550/arXiv.1510.04375

Gyongyosi, L., & Imre, S. (2019). A survey on quantum computing technology. Computer Science Review, 31, 51–71. https://doi.org/10.1016/j.cosrev.2018.11.002

DuBose R. & Madhvapathy Rao M. HashiCorp. (2026). Prioritizing data for post-quantum cryptography. https://www.hashicorp.com/en/blog/prioritizing-data-for-post-quantum-cryptography-pqc

IBM. (2025). What is symmetric encryption? IBM Think. https://www.ibm.com/think/topics/symmetric-encryption

Ifinedo, P. (2013). Information systems security policy compliance: An. *Psychological Review*, *84*(2), 191-215.

Information Commissioner's Office. (2023). Encryption and data security under the UK GDPR. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/

K. Kechedzhi, S.V. Isakov, S. Mandrà, B. Villalonga, X. Mi, S. Boixo, V. Smelyanskiy. (2024). Effective quantum volume, fidelity and computational cost of noisy quantum processing experiments, Future Generation Computer Systems. https://doi.org/10.1016/j.future.2023.12.002

Lambert, N., Chen, Y.-N., Cheng, Y.-C., Li, C.-M., Chen, G.-Y., & Nori, F. (2013). Quantum biology. *Nature Physics, 9*(1), 10–18. https://doi.org/10.1038/nphys2474

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

Microsoft Azure Quantum. (2025). Interferometric single-shot parity measurement in InAs–Al hybrid devices. Nature, 617, 46–51. https://doi.org/10.48550/arXiv.2401.09549

M. Mosca, (2018) "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, 2018, DOI: 10.1109/MSP.2018.3761723

Mosca, M., & Piani, M. (2021). 2021 Quantum Threat Timeline Report. https://info.quintessencelabs.com/hubfs/Quantum-Threat-Timeline-Report-2021-full-report-final%20(1).pdf

Moody, D., Perlner R., Regenscheid A., Robinson A., Cooper D. (2024) National Institute of Standards and Technology. (2024). NIST IR 8547: Strategy for cryptographic transition. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8547.ipd

National Institute of Standards and Technology. (2024). FIPS 203–205: Post-quantum cryptography standards. U.S. Department of Commerce. https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

National Institute of Standards and Technology. (2025). NIST selects HQC as fifth algorithm for post-quantum encryption. U.S. Department of Commerce. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Das Sarma, S. (2008). Non-Abelian anyons and topological quantum computation. *Reviews of Modern Physics, 80*(3), 1083–1159. https://doi.org/10.1103/RevModPhys.80.1083

OECD (2025) Mapping the global quantum ecosystem. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/mapping-the-global-quantum-ecosystem_47891dd2/20251217-0001.pdf?utm_source=chatgpt.com

Organisation for Economic Co-operation and Development. (2025). *An overview of national strategies and policies for quantum technologies.* OECD Publishing. https://www.oecd.org/en/publications/an-overview-of-national-strategies-and-policies-for-quantum-technologies_5e55e7ab-en/full-report/component-5.html

Paglieri L, Bonomi Savignon A, Scalabrini F, Costumato L (2025), "Navigating the quantum frontier: examining government strategy to the next technological revolution". *Transforming Government: People, Process and Policy*, Vol. 19 No. 4 pp. 700–724. https://doi.org/10.1108/TG-04-2025-0089

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the HAIS-Q. Computers & Security, 42, 165–176.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2023 BUDGET (2023). https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf?utm_source=chatgpt.com

Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press. DOI:10.1016/j.jmig.2007.07.001

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Sohn, I., Bang, J. & Heo, J. Dynamic Concatenation of Quantum Error Correction in Integrated Quantum Computing Architecture. *Sci Rep* **9**, 3302 (2019). https://doi.org/10.1038/s41598-019-39439-0

TEHDAS2 Joint Action. (2025). New TEHDAS2 Guideline Supports Researchers in Secure Use of Health data. https://tehdas.eu/results/new-tehdas2-guideline-supports-researchers-in-secure-use-of-health-data/

Terhal, B. M. (2013). Quantum error correction for quantum memories. Reviews of Modern Physics, 87(2), 307–346. https://doi.org/10.1103/RevModPhys.87.30

VTT Technical Research Centre of Finland. (2025). VTT and IQM launch the first 50-qubit superconducting quantum computer developed in the Europe. Press release. https://www.vttresearch.com/en/news-and-ideas/vtt-and-iqm-launch-first-50-qubit-quantum-computer-developed-europe

Annexes

Annex A print-out from PyCharm and Annex B is the python code for research analysis.

Annex A

==========

RESULTS AND ANALYSIS

Post-Quantum Cryptography (PQC) Readiness Survey

==========

---

1. Awareness of PQC

Have you heard about quantum safe security (Post-Quantum Cryptography, PQC)?24

Number of valid responses: 29

Response distribution:

- Yes I have heard of it but unclear what it means for us: 16 (55.2%)

- Yes somewhat aware: 8 (27.6%)
- Yes well aware: 3 (10.3%)
- I am not aware: 2 (6.9%)

Interpretation:

The dominant category is 'Yes I have heard of it but unclear what it means for us' (55.2%), indicating a relatively concentrated pattern in this item.

---

2. Job role profile

What is your job role? (Select from the options or provide your own)

Number of valid responses: 29

Response distribution:

- Information Security Officer: 12 (41.4%)
- IT Specialist: 5 (17.2%)
- Manager / Supervisor: 5 (17.2%)
- Information Security Specialist: 3 (10.3%)
- Chief Information Security Officer (CISO) / Director of Information Security: 1 (3.4%)
- Senior Cybersecurity Specialist: 1 (3.4%)
- Chief Information Officer (CIO) Head of IT Management: 1 (3.4%)
- Code 8 (label not defined): 1 (3.4%)

Interpretation:

The dominant category is 'Information Security Officer' (41.4%), indicating a relatively concentrated pattern in this item.

---

3. Dependency on quantum-vulnerable encryption

How would you assess your current systems' dependency on encryption methods that could be broken by quantum computers?

Number of valid responses: 29

Descriptive statistics:

- Mean: 2.31
- Median: 2
- Standard deviation: 1.05
- Quartiles (Q1, Q2, Q3): (1.5, 2, 3.0)

Methodological note: The mean value is reported as a descriptive summary indicator. As the response scale is ordinal, the mean should be interpreted directionally rather than as a precise measurement.

Response distribution (ordered low → high):

- Highly dependent multiple critical systems: 7 (24.1%)
- Fairly dependent: 11 (37.9%)
- Minimal dependence: 7 (24.1%)
- I don't know: 3 (10.3%)

- Code 5 (label not defined): 1 (3.4%)

Interpretation:

The most common response is 'Fairly dependent' (37.9%). The mean of 2.31 suggests responses lean toward the lower end of the scale.

---

4. Importance of PQC readiness

How important do you consider developing PQC readiness compared to other cybersecurity or health and social care sector requirements?

Number of valid responses: 29

Descriptive statistics:

- Mean: 2.55
- Median: 3
- Standard deviation: 0.93
- Quartiles (Q1, Q2, Q3): (2.0, 3, 3.0)

Methodological note: The mean value is reported as a descriptive summary indicator. As the response scale is ordinal, the mean should be interpreted directionally rather than as a precise measurement.

Response distribution (ordered low → high):

- As very important, high priority: 4 (13.8%)
- Important, but not the most urgent: 10 (34.5%)

- As a medium requirement: 10 (34.5%)
- As a rather minor requirement: 5 (17.2%)

Interpretation:

The most common response is 'As a medium requirement' (34.5%). The mean of 2.55 suggests responses lean toward the higher end of the scale.

---

5. Organizational Barriers to PQC Adoption

What are the biggest obstacles you see for adopting PQC in your organization? (Select the most relevant)

All respondents selected at least one obstacle, yielding a total of 73 obstacle mentions.

Ranked obstacles (long-tail grouped):

- Technological uncertainty solutions still in progress: 15 (20.5%)
- Lack of resources time or money: 15 (20.5%)
- Lack of skills or training: 14 (19.2%)
- Lack of guidelines and standards: 13 (17.8%)
- Lack of management or decision making support: 8 (11.0%)
- Other context-specific obstacles (aggregated): 8 (11.0%)

Interpretation:

The leading barriers are concentrated around 'Technological uncertainty solutions still in progress', 'Lack of resources time or money', 'Lack of skills or training'. This suggests that capability, resourcing, and uncertainty factors dominate over niche technical constraints.

```
================================================================================
========

FIGURE GENERATION

================================================================================
========

Saved: Figure_1_Dependency.png

Saved: Figure_2_Importance.png

Saved: Figure_3_Awareness.png

Saved: Figure_4_Obstacles.png

Saved: Figure_5_Role_by_Awareness.png


SUCCESS: Console analysis printed and all 5 figures generated.


Process finished with exit code 0
```

Annex B

```
# ========================================================
# PQC SURVEY ANALYSIS (CONSOLE OUTPUT) + 5 FIGURES
# CONSOLIDATED CLEAN VERSION (NO DUPLICATE CODE PATHS)
#
# Outputs:
#   Figure_1_Dependency.png
#   Figure_2_Importance.png
```

```
#   Figure_3_Awareness.png
#   Figure_4_Obstacles.png
#   Figure_5_Role_by_Awareness.png  (HEATMAP MATRIX)
#
# Key methodological features:
# - Row-wise coalescing to avoid inflated N from duplicated columns
# - Dependency scale correction (swap codes 1 <-> 2 for that question)
# - Long-tail obstacle grouping (<5% mentions aggregated)
# - Safe label handling (no crashes if lookup is incomplete)
# ============================================================

import zipfile
import xml.etree.ElementTree as ET
import re
import math
import itertools
from collections import Counter, defaultdict

import matplotlib.pyplot as plt
import numpy as np
import textwrap



# ============================================================
# 1) Helper functions
# ============================================================

def safe_label(labels: dict, code: int) -> str:
    """Return label for code; if missing, show an explicit fallback."""
    return labels.get(code, f"Code {code} (label not defined)")

def norm(col: str) -> str:
    """Normalize column name by removing trailing digits (for duplicated columns)."""
    return re.sub(r"\d+$", "", col)
```

```
def parse_int(v):
    try:
        return int(float(str(v).strip()))
    except:
        return None

def mean(nums):
    return sum(nums) / len(nums) if nums else None

def pstdev(nums):
    if len(nums) <= 1:
        return 0.0
    mu = mean(nums)
    return math.sqrt(sum((x - mu) ** 2 for x in nums) / len(nums))

def median(nums_sorted):
    n = len(nums_sorted)
    if n == 0:
        return None
    mid = n // 2
    return nums_sorted[mid] if n % 2 else (nums_sorted[mid - 1] + nums_sorted[mid]) / 2

def quartiles(nums):
    if not nums:
        return None, None, None
    s = sorted(nums)
    q2 = median(s)
    n = len(s)
    mid = n // 2
    lower = s[:mid]
    upper = s[mid+1:] if n % 2 else s[mid:]
    q1 = median(lower) if lower else None
    q3 = median(upper) if upper else None
```

```
    return q1, q2, q3


def is_dependency_question(qtext: str) -> bool:
    t = qtext.lower()
    return ("dependency" in t and "encryption" in t and "quantum" in t)


def is_likert_question(qtext: str) -> bool:
    t = qtext.lower()
    # Keep your established classification
    return ("dependency on encryption" in t) or t.startswith("how important")


def coalesce_codes_by_row(row_count: int, cols: list[str], columns: dict) -> list[int]:
    """
    Row-wise coalescing:
    For each respondent, take the first non-empty code among duplicated columns.
    Prevents inflated N caused by duplicate exported columns.
    """
    merged = []
    for r in range(row_count):
        chosen = None
        for col in cols:
            code = parse_int(columns[col][r])
            if code is not None:
                chosen = code
                break
        if chosen is not None:
            merged.append(chosen)
    return merged


def filter_substantive_codes(freq: Counter, labels: dict) -> Counter:
    """
    Keep only codes defined in the lookup labels.
    This prevents undefined/placeholder codes from appearing in figures.
    """
```

```
    return Counter({k: v for k, v in freq.items() if k in labels})

def wrap_text(s: str, width: int = 40) -> str:
    return "\n".join(textwrap.wrap(s, width))


# ============================================================
# 2) Minimal XLSX reader (standard libraries)
# ============================================================

def read_shared_strings(z):
    if "xl/sharedStrings.xml" not in z.namelist():
        return []
    root = ET.fromstring(z.read("xl/sharedStrings.xml"))
    ns = "{http://schemas.openxmlformats.org/spreadsheetml/2006/main}"
    out = []
    for si in root.findall(f"{ns}si"):
        out.append("".join(t.text or "" for t in si.findall(f".//{ns}t")))
    return out

def get_sheet_target(z, sheet_name):
    wb = ET.fromstring(z.read("xl/workbook.xml"))
    ns = "{http://schemas.openxmlformats.org/spreadsheetml/2006/main}"
    rel_ns = "{http://schemas.openxmlformats.org/officeDocument/2006/relationships}"

    rId = None
    for s in wb.findall(f"{ns}sheets/{ns}sheet"):
        if s.get("name") == sheet_name:
            rId = s.get(f"{rel_ns}id")
            break
    if not rId:
        return None

    rels = ET.fromstring(z.read("xl/_rels/workbook.xml.rels"))
```

```
    pkg = "{http://schemas.openxmlformats.org/package/2006/relationships}"
    for r in rels.findall(f"{pkg}Relationship"):
        if r.get("Id") == rId:
            return "xl/" + r.get("Target")
    return None

def read_sheet(z, shared, sheet_name):
    target = get_sheet_target(z, sheet_name)
    if not target:
        raise ValueError(f"Sheet '{sheet_name}' not found.")
    root = ET.fromstring(z.read(target))
    ns = "{http://schemas.openxmlformats.org/spreadsheetml/2006/main}"

    rows = []
    for r in root.findall(f".//{ns}row"):
        row = []
        for c in r.findall(f"{ns}c"):
            v = c.find(f"{ns}v")
            if v is None:
                row.append("")
            elif c.get("t") == "s":
                row.append(shared[int(v.text)])
            else:
                row.append(v.text)
        rows.append(row)
    return rows


# ============================================================
# 3) Parse lookup_table
# ============================================================

def parse_lookup(lookup_rows):
    """
```

```
    Parses lookup_table into:
      lookup[nid] = {"text": question_text, "labels": {code:int -> label:str}}
    """
    lookup = {}
    current = None
    for r in lookup_rows:
        if len(r) < 2:
            continue
        text = (r[0] or "").strip()
        code = (r[1] or "").strip()

        if text and code and not code.isdigit():
            nid = re.sub(r"\d+$", "", code)
            lookup[nid] = {"text": text, "labels": {}}
            current = nid
            continue

        if current and text and code.isdigit():
            lookup[current]["labels"][int(code)] = text

    return lookup


# ============================================================
# 4) Plotting helpers
# ============================================================

GRADIENT = ["#003f5c", "#2f4b7c", "#665191", "#a5cfe2", "#d7f3ff"]

def plot_ordered_bar(freq: Counter, labels: dict, title: str, filename: str):
    codes = sorted(freq.keys())
    names = [safe_label(labels, c) for c in codes]
    counts = [freq[c] for c in codes]
```

```
    colors = GRADIENT[:len(codes)] if len(codes) <= len(GRADIENT) else [GRADIENT[-1]] * len(codes)

    plt.figure(figsize=(6, 4))
    plt.bar(names, counts, color=colors, edgecolor="black")
    plt.ylabel("Number of responses")
    plt.title(title, pad=12)
    plt.xticks(rotation=30, ha="right")
    plt.tight_layout(rect=[0, 0, 1, 0.95])
    plt.savefig(filename, dpi=300)
    plt.close()

def plot_ranked_horizontal_bar(items: list[tuple[str, int]], title: str, filename: str):
    names = [n for n, _ in items]
    counts = [c for _, c in items]

    plt.figure(figsize=(7, 5))
    plt.barh(names, counts, color="#2f4b7c")
    plt.xlabel("Number of mentions")
    plt.title(title, pad=12)
    plt.tight_layout()
    plt.savefig(filename, dpi=300)
    plt.close()

def plot_role_awareness_heatmap(roles: list[str], awareness: list[str], matrix: np.ndarray, filename:
str):
    plt.figure(figsize=(10, 6))
    im = plt.imshow(matrix, cmap="Blues", aspect="auto")

    plt.xticks(range(len(awareness)), awareness, rotation=30, ha="right")
    plt.yticks(range(len(roles)), [wrap_text(r, 40) for r in roles])

    plt.title("Awareness of PQC by Job Role", pad=12)
    plt.xlabel("Awareness level")
    plt.ylabel("Job role")
```

```
    # Annotate only non-zero cells
    for i in range(matrix.shape[0]):
        for j in range(matrix.shape[1]):
            if matrix[i, j] > 0:
                plt.text(j, i, int(matrix[i, j]), ha="center", va="center", fontsize=10)

    plt.colorbar(im, label="Number of responses")
    plt.tight_layout()
    plt.savefig(filename, dpi=300)
    plt.close()


# ============================================================
# 5) Load workbook and build column index
# ============================================================

EXCEL_PATH = "survey draft - final.xlsx"

with zipfile.ZipFile(EXCEL_PATH) as z:
    shared = read_shared_strings(z)
    survey_rows = read_sheet(z, shared, "survey")
    lookup_rows = read_sheet(z, shared, "lookup_table")

lookup = parse_lookup(lookup_rows)

header = survey_rows[0]
data_rows = survey_rows[1:]
max_len = len(header)
data_rows = [r + [""] * (max_len - len(r)) for r in data_rows]
row_count = len(data_rows)

columns = {h: [] for h in header}
for r in data_rows:
```

```
    for i, h in enumerate(header):
        columns[h].append(r[i])


# ============================================================
# 6) Group columns by normalized question id
# ============================================================

groups = defaultdict(list)
for h in header:
    nid = norm(h)
    if nid in lookup:
        groups[nid].append(h)

def find_qid_startswith(prefix: str):
    return next((k for k, v in lookup.items() if v["text"].startswith(prefix)), None)

role_q = find_qid_startswith("What is your job role")
aware_q = find_qid_startswith("Have you heard")
imp_q  = find_qid_startswith("How important")
obs_q  = find_qid_startswith("What are the biggest obstacles")
dep_q  = next((k for k, v in lookup.items() if "dependency on encryption" in v["text"].lower()), None)

if not all([role_q, aware_q, imp_q, obs_q, dep_q]):
    missing = [name for name, q in [
        ("role_q", role_q), ("aware_q", aware_q), ("imp_q", imp_q), ("obs_q", obs_q), ("dep_q", dep_q)
    ] if q is None]
    raise ValueError(f"Could not identify required question IDs: {missing}")


# ============================================================
# 7) Console output (MBA thesis style)
# ============================================================
```

```
print("\n" + "=" * 90)
print("RESULTS AND ANALYSIS")
print("Post-Quantum Cryptography (PQC) Readiness Survey")
print("=" * 90)

footnote_mean = (
    "Methodological note: The mean value is reported as a descriptive summary indicator. "
    "As the response scale is ordinal, the mean should be interpreted directionally rather "
    "than as a precise measurement."
)

def print_distribution(freq: Counter, labels: dict, total_n: int, order="code_asc"):
    items = sorted(freq.items(), key=lambda x: (-x[1], x[0])) if order == "count_desc" else
sorted(freq.items())
    for code, count in items:
        pct = (count / total_n) * 100 if total_n else 0
        print(f"  • {safe_label(labels, code)}: {count} ({pct:.1f}%)")

def print_likert_summary(freq: Counter, labels: dict):
    expanded = sorted(itertools.chain.from_iterable([[c] * n for c, n in freq.items()]))
    n = len(expanded)
    mu = mean(expanded)
    sd = pstdev(expanded)
    q1, med, q3 = quartiles(expanded)

    print("Descriptive statistics:")
    print(f"  • Mean: {mu:.2f}")
    print(f"  • Median: {med}")
    print(f"  • Standard deviation: {sd:.2f}")
    if q1 is not None and q3 is not None:
        print(f"  • Quartiles (Q1, Q2, Q3): ({q1}, {med}, {q3})")
    print(footnote_mean)

    print("\nResponse distribution (ordered low → high):")
```

```
    print_distribution(freq, labels, n, order="code_asc")

    top_code = max(freq, key=freq.get)
    top_pct = 100 * freq[top_code] / n
    codes_sorted = sorted(freq.keys())
    midpoint = (codes_sorted[0] + codes_sorted[-1]) / 2
    orientation = "higher" if mu > midpoint else "lower"

    print("\nInterpretation:")
    print(
        f"The most common response is '{safe_label(labels, top_code)}' ({top_pct:.1f}%). "
        f"The mean of {mu:.2f} suggests responses lean toward the {orientation} end of the scale."
    )

def print_categorical_summary(freq: Counter, labels: dict):
    n = sum(freq.values())
    print("Response distribution:")
    print_distribution(freq, labels, n, order="count_desc")

    top_code = max(freq, key=freq.get)
    top_pct = 100 * freq[top_code] / n
    print("\nInterpretation:")
    print(
        f"The dominant category is '{safe_label(labels, top_code)}' ({top_pct:.1f}%), "
        "indicating a relatively concentrated pattern in this item."
    )

ordered_questions = [
    ("Awareness of PQC", aware_q),
    ("Job role profile", role_q),
    ("Dependency on quantum-vulnerable encryption", dep_q),
    ("Importance of PQC readiness", imp_q),
]
```

```
section = 1
for section_title, qid in ordered_questions:
    qtext = lookup[qid]["text"]
    labels = lookup[qid]["labels"]
    cols = groups[qid]

    merged = coalesce_codes_by_row(row_count, cols, columns)

    # Dependency correction: swap 1 <-> 2 for that question (data + labels)
    if is_dependency_question(qtext):
        merged = [2 if c == 1 else 1 if c == 2 else c for c in merged]
        if 1 in labels or 2 in labels:
            labels = dict(labels)
            labels[1], labels[2] = labels.get(2), labels.get(1)

    freq = Counter(merged)
    n = sum(freq.values())

    print("\n" + "-" * 90)
    print(f"{section}. {section_title}")
    print("-" * 90)
    print(qtext)
    print(f"Number of valid responses: {n}\n")

    if is_likert_question(qtext):
        print_likert_summary(freq, labels)
    else:
        print_categorical_summary(freq, labels)

    section += 1

# Obstacles (multi-select)
obs_text = lookup[obs_q]["text"]
obs_labels = lookup[obs_q]["labels"]
```

```
obs_cols = groups[obs_q]

agg = Counter()
for r in range(row_count):
    for col in obs_cols:
        code = parse_int(columns[col][r])
        if code is not None:
            agg[code] += 1

total_mentions = sum(agg.values())

print("\n" + "-" * 90)
print(f"{section}. Organizational Barriers to PQC Adoption")
print("-" * 90)
print(obs_text)
print(f"All respondents selected at least one obstacle, yielding a total of {total_mentions} obstacle
mentions.\n")

THRESHOLD = 0.05
main = {}
tail_count = 0

for code, count in agg.items():
    if total_mentions and (count / total_mentions) >= THRESHOLD:
        main[code] = count
    else:
        tail_count += count

print("Ranked obstacles (long-tail grouped):")
main_ranked = sorted(main.items(), key=lambda x: -x[1])
for code, count in main_ranked:
    pct = 100 * count / total_mentions if total_mentions else 0
    print(f"  • {safe_label(obs_labels, code)}: {count} ({pct:.1f}%)")
```

```
if tail_count:
    pct = 100 * tail_count / total_mentions if total_mentions else 0
    print(f"  • Other context-specific obstacles (aggregated): {tail_count} ({pct:.1f}%)")

print("\nInterpretation:")
if main_ranked:
    top3 = main_ranked[:3]
    top3_str = ", ".join(f"'{safe_label(obs_labels, c)}'" for c, _ in top3)
    print(
        f"The leading barriers are concentrated around {top3_str}. "
        "This suggests that capability, resourcing, and uncertainty factors dominate over niche technical constraints."
    )
else:
    print(
        "Obstacle mentions are dispersed across many categories with no single barrier reaching the reporting threshold, "
        "suggesting heterogeneity and organization-specific constraints."
    )

section += 1


# ============================================================
# 8) Generate Figures 1–5
# ============================================================

print("\n" + "=" * 90)
print("FIGURE GENERATION")
print("=" * 90)

# Figure 1: Dependency (apply swap + filter undefined codes out of chart)
dep_labels = dict(lookup[dep_q]["labels"])
dep_vals = coalesce_codes_by_row(row_count, groups[dep_q], columns)
```

```
dep_vals = [2 if v == 1 else 1 if v == 2 else v for v in dep_vals]
dep_labels[1], dep_labels[2] = dep_labels.get(2), dep_labels.get(1)
dep_freq = filter_substantive_codes(Counter(dep_vals), dep_labels)
plot_ordered_bar(dep_freq, dep_labels, "Dependency on Quantum-Vulnerable Encryption", "Figure_1_Dependency.png")
print("Saved: Figure_1_Dependency.png")

# Figure 2: Importance
imp_labels = lookup[imp_q]["labels"]
imp_vals = coalesce_codes_by_row(row_count, groups[imp_q], columns)
imp_freq = filter_substantive_codes(Counter(imp_vals), imp_labels)
plot_ordered_bar(imp_freq, imp_labels, "Perceived Importance of PQC Readiness", "Figure_2_Importance.png")
print("Saved: Figure_2_Importance.png")

# Figure 3: Awareness
aware_labels = lookup[aware_q]["labels"]
aware_vals = coalesce_codes_by_row(row_count, groups[aware_q], columns)
aware_freq = filter_substantive_codes(Counter(aware_vals), aware_labels)
plot_ordered_bar(aware_freq, aware_labels, "Awareness of Post-Quantum Cryptography (PQC)", "Figure_3_Awareness.png")
print("Saved: Figure_3_Awareness.png")

# Figure 4: Obstacles (main + tail)
items_for_plot = []
for code, count in sorted(main.items(), key=lambda x: x[1]):  # low->high for barh
    items_for_plot.append((safe_label(obs_labels, code), count))
if tail_count:
    items_for_plot.append(("Other context-specific obstacles", tail_count))

plot_ranked_horizontal_bar(items_for_plot, "Organizational Barriers to PQC Adoption", "Figure_4_Obstacles.png")
print("Saved: Figure_4_Obstacles.png")
```

```
# Figure 5: Role × Awareness (heatmap matrix, clean and readable)
role_labels = lookup[role_q]["labels"]
aware_labels = lookup[aware_q]["labels"]

# Keep substantive awareness (exclude "I don't know"/DK-style labels)
awareness_order = [c for c, lbl in aware_labels.items() if lbl and "know" not in lbl.lower()]
awareness_names = [aware_labels[c] for c in awareness_order]

role_vals = coalesce_codes_by_row(row_count, groups[role_q], columns)
aware_vals = coalesce_codes_by_row(row_count, groups[aware_q], columns)

roles_in_matrix = []
matrix_rows = []

for r_code in sorted(set(role_vals)):
    if r_code not in role_labels:
        continue
    row = []
    for a_code in awareness_order:
        cnt = sum(1 for r, a in zip(role_vals, aware_vals) if r == r_code and a == a_code)
        row.append(cnt)
    if sum(row) > 0:
        roles_in_matrix.append(role_labels[r_code])
        matrix_rows.append(row)

matrix = np.array(matrix_rows, dtype=int) if matrix_rows else np.zeros((0, len(awareness_order)),
dtype=int)

plot_role_awareness_heatmap(
    roles_in_matrix,
    awareness_names,
    matrix,
    "Figure_5_Role_by_Awareness.png"
)
```

```
print("Saved: Figure_5_Role_by_Awareness.png")

print("\nSUCCESS: Console analysis printed and all 5 figures generated.")
```