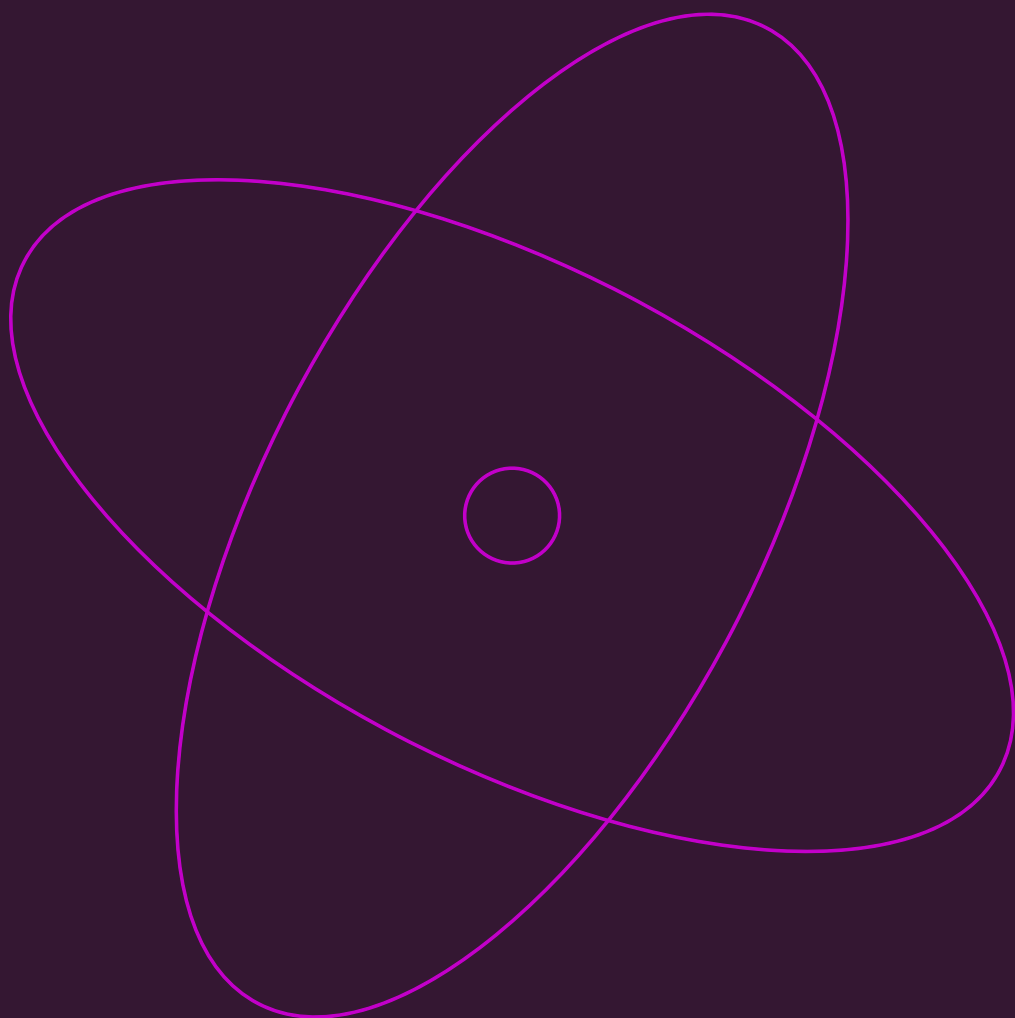




WHITE PAPER

PREPARING FOR THE QUANTUM ERA

A Practical Guide to Post-Quantum Cryptography

About

This document is Volume 1 of a three-volume guide on preparing for the quantum era and transitioning to post-quantum cryptography (PQC). The three volumes¹ are designed for different audiences, moving from awareness and decision-making to governance, financial planning, and technical implementation.

VOLUME 01

Preparing for the Quantum Era

Updated Strategic Guidance

This volume introduces the quantum threat, raises awareness, and provides updates on timelines, policy developments, and the urgency of post-quantum migration. Its target audience is decision-makers.

VOLUME 02

Managing the PQC Transition

Governance, Planning and Investment

This volume explains what is needed to initiate a PQC transition within an organisation, including governance, planning, responsibilities, funding considerations, and coordination across stakeholders. Its target audience is security, risk and compliance (GRC) teams, project managers and technical coordinators.

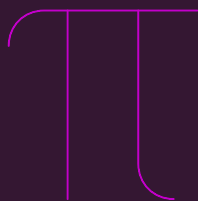
VOLUME 03

Implementing the PQC Migration

Technical and Migration Guidance

This volume provides technical guidance on post-quantum cryptography and PQC migrations, including algorithm choices, implementation considerations, interoperability, testing, and operational deployment. Its target audience is engineers, developers, IT architecture and operations teams.

¹ The documents can be found here: <https://cybersecuritycoalition.be/resource/white-paper-preparing-for-the-quantum-era>



1. Executive Summary	4
1.1 Strategic Urgency	4
1.2 The Quantum Threat	4
1.3 Post-Quantum Cryptography Explained	5
1.4 Steps Towards Quantum Readiness	5
1.5 Timeline for PQC Migration	5
1.6 Strategic Recommendations	6
1.7 Call to Action for Decision-Makers	6
2. Understanding the Quantum Threat	7
2.1 A new Computing Paradigm – With Consequences	7
2.2 The Quantum Threat: Acting Before It's Too Late	8
2.3 The Uncertain but Shrinking Timeline	9
2.4 Broader Risk Perspective	10
3. Understanding Post-Quantum Cryptography	11
3.1 Currently Deployed Cryptography	11
3.2 The Vulnerability of Current Cryptography	12
3.3 Research on Post-Quantum Algorithms	13
3.4 Post-Quantum Public-Key Standards	13
3.5 Performance	14
3.6 Cryptography in Hybrid Mode	14
4. Taking the First Steps Towards Post-Quantum Readiness	15
4.1 Phase 1: Awareness and Assessment	16
4.2 Phase 2: Planning and Strategy	18
4.3 Phase 3: Implementation and Beyond	19
Conclusion	21
Team	25

01

Executive Summary

1.1 Strategic Urgency

When the previous Preparing for the Quantum Era white paper was published in October 2025, its core message was awareness: quantum computing will eventually undermine the cryptographic foundations of today's digital world; "harvest now, decrypt later" makes some sensitive data vulnerable already; and migrating to post-quantum cryptography (PQC) will take many years.

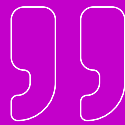
The past year has changed the tone of the debate around quantum risk. As discussed in Section 2.3, the timeline remains uncertain, but the risk horizon is shrinking: industry roadmaps, public-policy signals, and expert assessments increasingly point to the need for earlier action.

At the same time, post-quantum readiness has evolved from a long-term research topic into a practical cybersecurity priority, increasingly reflected in cybersecurity strategies, regulatory expectations, and resilience planning.

Early action is no longer driven primarily by the need to protect long-lived confidential data against future decryption. Starting the transition now provides organisations with the time and flexibility to address a broader set of cryptographic dependencies, including authentication and digital signatures, rather than being forced into a narrowly focused or rushed migration later.

For C-level executives, CIOs, CISOs, and IT decision-makers, the imperative is clear: preparation cannot wait.

Leadership in the quantum era means anticipating change before it becomes disruption.



1.2 The Quantum Threat

Quantum computers will ultimately be able to break public-key algorithms such as RSA and ECC. This puts secure communications, encrypted data and digital signatures at risk. Although large-scale machines are not yet available, governments and security agencies are already urging a shift to post-quantum cryptography (PQC).

Migration is complex: updating systems across diverse infrastructures can take many years. The urgency is heightened by the "harvest now, decrypt later" model, where adversaries collect encrypted data today to decrypt once quantum capabilities mature. Sectors with long data-retention requirements — government, healthcare, finance, critical infrastructure — are especially exposed to this risk. Starting the migration early is essential to ensure data protection and operational continuity in the quantum era. Chapter 2 will provide a clearer view of these risks and their urgency.

Leadership in the quantum era means anticipating change before it becomes disruption.

1.3 Post-Quantum Cryptography Explained

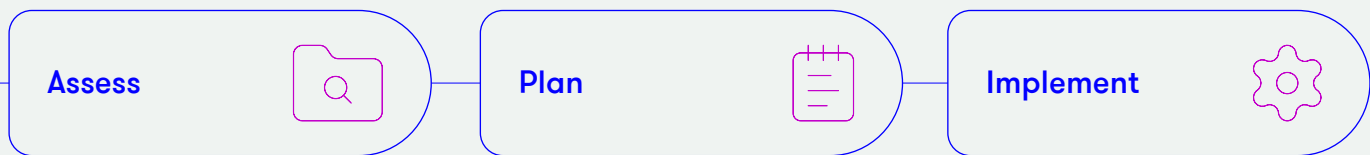
Post-quantum cryptography (PQC) is a new class of algorithms based on mathematical problems that remain unsolvable even for quantum computers. Global standards bodies such as NIST are already defining PQC standards. Current cryptographic protocols will be phased out over the coming years. Chapter 3 examines this topic in greater depth.

1.4 Steps Towards Quantum Readiness

To protect data from quantum threats, organisations must begin transitioning to post-quantum cryptography.

- **Assess:** Identify quantum risks and evaluate exposure.
- **Plan:** Build a migration roadmap aligned with compliance needs.
- **Implement:** Deploy PQC solutions and ensure resilience.

Chapter 4 outlines the actions organisations should take now.



1.5 Timeline for PQC Migration

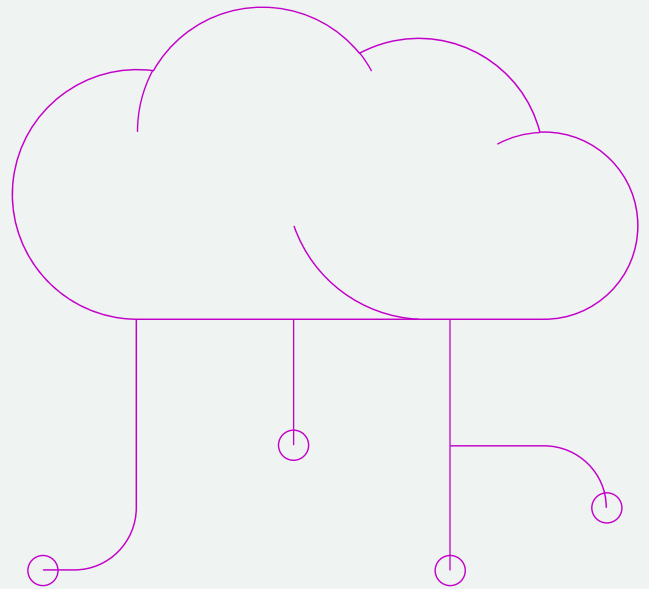
While the exact moment when quantum computers will break modern cryptographic algorithms remains uncertain, this uncertainty is irrelevant to strategic planning. Governments and regulators are not waiting for breakthroughs; they are setting migration timelines based on risk and infrastructure readiness.

For decision-makers, the implication is clear: waiting is no longer an option. Action is required now, regardless of when quantum computers arrive.

The European Union's Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (PQC) sets three milestones:



- **By 2026**
National strategies and awareness campaigns established by Member States.
- **By 2030**
Critical infrastructure and high-risk use cases protected with PQC.
- **By 2035**
Broad adoption across all sectors and lower-risk use systems completed.



1.6 Strategic Recommendations

The most consequential near-term actions for security leadership are not technical. They are organisational.

- **Fund:** Secure funding and scope for a quantum readiness programme.
- **Organise:** Make sure that ownership roles across security, architecture, compliance, and infrastructure are explicitly assigned rather than assumed.
- **Inventory:** Catalogue cryptographic assets and assess data sensitivity and retention.
- **Plan:** Develop a migration strategy aligned with EU roadmap milestones, prioritising high-risk and long-lived systems.
- **Engage:** Work with vendors to ensure PQC readiness and update contracts with transparency clauses.
- **Implement:** Deploy hybrid cryptographic solutions to ensure continuity and enable future upgrades.
- **Invest:** Build crypto-agility to adapt quickly to evolving standards and threats.
- **Report:** Ensure that PQC appears in risk reporting to boards and steering committees.
- **Monitor:** Track quantum developments, assess cybersecurity implications, and join industry collaborations to stay informed.

1.7 Call to Action for Decision-Makers

Quantum readiness is no longer a distant concern — it is a strategic imperative. If you are a C-level executive, CIO, CISO, or IT leader, your role is pivotal in preparing your organisation for the post-quantum era.

Acting now not only safeguards data and operations but also positions your organisation as a leader in digital resilience. This is the moment to build trust, ensure compliance, and future-proof infrastructure against emerging threats.

The time to act is now.

Understanding the Quantum Threat

2.1 A new Computing Paradigm – With Consequences

Quantum computing, once a science-fiction concept, is now advancing rapidly. With billions in investment from governments and technology giants, the arrival of usable quantum machines is no longer a question of if but when.

Its power comes from two principles of quantum mechanics: superposition and entanglement. Superposition allows a qubit to exist in multiple states at once, while entanglement links qubits so that the state of one instantly influences another. Together, they enable quantum computers to solve problems that would take classical machines centuries.

The possibilities are transformative: breakthroughs in materials science, logistics, and drug development; faster training of AI models; and optimisation problems beyond the reach of today's technology.

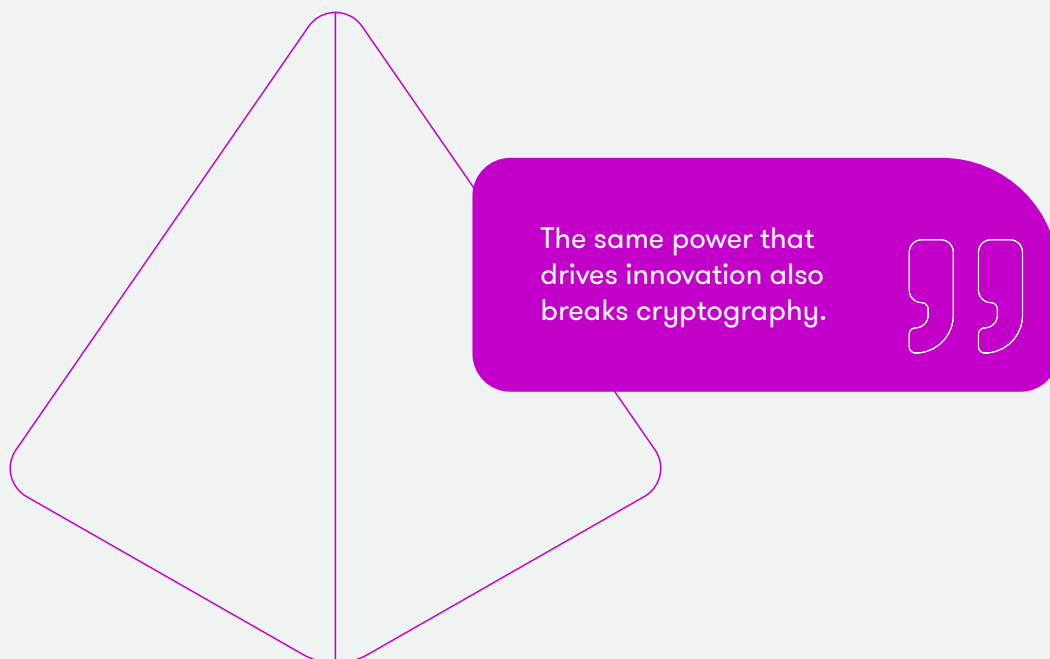
But this power carries risk. The same mathematical problems that secure digital systems today — such as factoring large numbers — become solvable with

a cryptographically relevant quantum computer [CRQC]. Widespread cryptographic algorithms could be broken, undermining the security of global digital infrastructure.

Cryptography underpins online banking, government services, secure communications, and critical infrastructure. Every time we log in, update software, or access a secure website, cryptography ensures confidentiality and integrity. If those algorithms fail, the consequences will be severe. Chapter 3 explores this in depth and introduces post-quantum cryptography [PQC].

Before that, it is important to understand the threat itself: why does it matter today? The following chapters examine these risks, the uncertain timeline for CRQCs, and the steps organisations can already take.

The same power that drives innovation also breaks cryptography.



2.2 The Quantum Threat: Acting Before It's Too Late

The quantum threat is not a distant science-fiction scenario. Even without a fully developed CRQC, the risk is real: the possibility of one emerging in the coming decades demands urgent action today.

Migration to quantum-safe cryptography is complex. It requires mapping interdependencies, testing algorithms, and coordinating across vendors, partners, and legacy systems. This is far more than a software update; some systems may take years, others a decade or more. Past experience proves the challenge — phasing out TLS 1.0, for example, took over ten years. The long migration time makes early preparation critical.

Another driver of urgency is the “harvest now, decrypt later” model. Adversaries may already be storing encrypted data, waiting until quantum machines can break it. When that day comes, archives containing government communications, corporate secrets, or health records could all be exposed. Any long-lived data is at risk.

Declassification laws highlight the danger. In 2022, the federal government set timelines of 20, 30, or 50 years depending on sensitivity. Yet intercepted cables could be decrypted decades earlier if a CRQC appears within 10–15 years — undermining sovereignty and public trust.

This risk is not theoretical. Nation-states are investing heavily in quantum research, seeking the first-mover advantage of breaking encryption at scale. Whoever builds the first CRQC could gain unprecedented access to communications, military intelligence, satellite channels, financial flows, and critical infrastructure — a global game-changer.

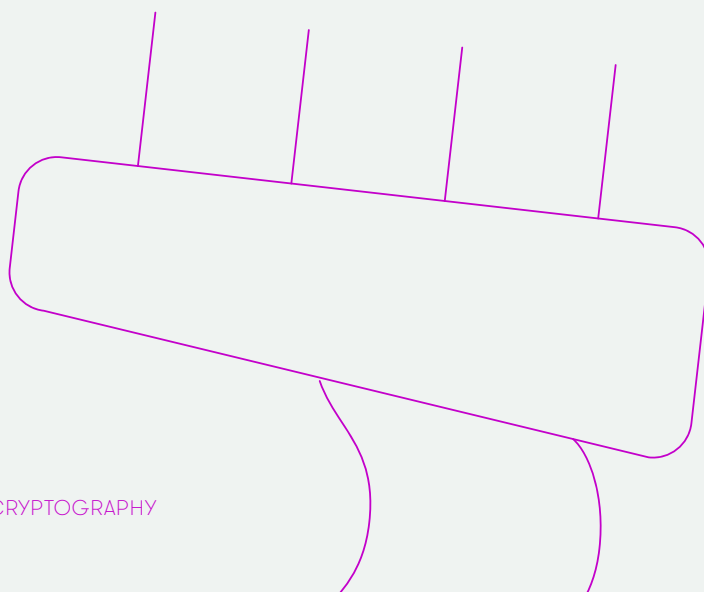
Equally concerning is the risk of forged digital signatures. These underpin services from software updates and secure logins to identity documents and financial transactions. Without post-quantum signatures, attackers could fake updates, insert malicious code, and block remediation. The same threat extends to digital identities, payment systems, and authentication frameworks.

It is useful to distinguish between two eras:

Before a CRQC exists, both long-lifetime data and long-lived digital signatures are vulnerable. Data encrypted today may be decrypted in the future, and signatures relied upon for years may no longer provide proof of authenticity and integrity.

After a CRQC is achieved, the risk becomes immediate. Harvested data can be decrypted, live communications broken, and digital signatures forged in real time. Existing authentication and authorisation infrastructure would collapse overnight.

These two realities — long-term data vulnerability and slow migration — make the quantum threat uniquely urgent. Even if a CRQC is still years away, the choices made today will determine whether systems and data remain secure in the decades ahead.



2.3 The Uncertain but Shrinking Timeline

Quantum computers capable of breaking modern algorithms do not yet exist, but their development is a widely acknowledged threat. Experts agree on one point: while the exact moment cannot be predicted, preparation must begin now. There is no public evidence of a CRQC, and one is unlikely to appear in the next few years. Yet the past year has changed the tone of the debate around quantum risk. Industry leaders have sent strong signals that the timeline for post-quantum migration is compressing.

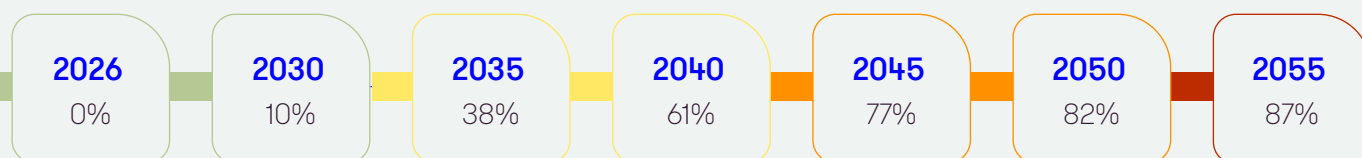
In early 2026, Google announced a target of 2029 for its complete PQC migration, explicitly linking this to progress in quantum hardware, error correction, and new resource estimates for breaking cryptography¹. Cloudflare quickly followed, accelerating its own goal to be fully post-quantum secure by 2029². Microsoft likewise has committed to transitioning its products and services to PQC by 2029³. This urgency is also reflected in public policy: U.S. Executive Order 14412, “Securing the Nation Against Advanced Cryptographic Attacks,”⁴ directs an accelerated transition of federal information systems to NIST-approved post-quantum cryptography.

The race towards quantum advantage is led by major technology companies such as IBM, Google,

Microsoft, and Amazon, alongside specialised start-ups including D-Wave, IonQ, Rigetti, and Quantinuum. These efforts are reinforced by national investments from powers such as the United States and China. While Belgium lacks a dedicated national quantum strategy, the European Commission has recently adopted its own⁵.

Many industry actors publish roadmaps outlining projected milestones, providing a useful lens for tracking progress. Monitoring these developments helps contextualise the risk horizon and underlines why preparation cannot wait. Several forward-looking assessments illustrate the urgency. A multi-year study by Germany’s Federal Office for Information Security (BSI), updated in 2025, concluded that a quantum computer able to break RSA-2048 could realistically arrive by 2040⁶.

With faster advances — such as in error correction or hardware scaling — the timeline could shrink to just 10 years. The Global Risk Institute’s Quantum Threat Timeline Report similarly estimated a 28% to 49% chance of such a computer emerging within the next decade⁷. These figures, based on expert judgement rather than engineering blueprints, reflect a growing consensus: the risk horizon is approaching.



Quantum Risk Timeline

¹ <https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline>

² <https://blog.cloudflare.com/post-quantum-roadmap>

³ <https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts>

⁴ <https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks>

⁵ <https://digital-strategy.ec.europa.eu/en/policies/quantum>

⁶ https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer_node.html

⁷ <https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b>

Adding to the uncertainty is the pace of innovation. Progress in quantum algorithms, error mitigation, and hardware is not linear, and breakthroughs could drastically shorten the timeline.

While Mosca's Theorem¹ has traditionally been used to illustrate the urgency of quantum-safe migration, organisations should now avoid using it as the primary basis for determining migration timelines. In practice, transition schedules are increasingly being driven by regulatory requirements, industry mandates, customer expectations, vendor roadmaps, and supply-chain dependencies. As a result, organisations should align their planning with

emerging compliance obligations and ecosystem readiness rather than relying solely on forecasts of when a cryptographically relevant quantum computer (CRQC) may emerge.

We do not know the exact year the post-CRQC era will begin, but we do know its impact. Just as you would not wait for an earthquake to reinforce a vulnerable bridge, you should not wait for the first CRQC to secure cryptographic infrastructure. Whether driven by technological breakthroughs or by regulatory and industry imperatives, the direction of travel is clear: the threat is real, the consequences severe, and the time to act is now.

2.4 Broader Risk Perspective

The shift to PQC is often seen as a technical encryption update, but in reality it is part of a much broader cyber risk and resilience challenge. This means treating PQC migration as part of enterprise risk management — integrating it with existing vulnerability management, threat monitoring, supply chain security, and operational resilience efforts.

As organisations gradually adopt PQC, they must also contend with a hybrid cryptographic environment where new and old algorithms co-exist. This transitional state expands the attack surface through potential implementation bugs, coexistence risks, and integration weaknesses between classical and quantum-safe systems.

By merging PQC initiatives into a broader enterprise resilience strategy, organisations move beyond a checkbox compliance mindset. This holistic approach ensures they are mitigating both present and future quantum-related threats, strengthening detection and response functions, maintaining visibility across hybrid cryptographic environments, and boosting overall readiness for the converging challenges of quantum computing, AI, and other emerging cyber threats.

¹ <https://ieeexplore.ieee.org/document/8490169>

The direction of travel is clear: the threat is real, the consequences severe, and the time to act is now.



Understanding Post-Quantum Cryptography

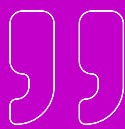
3.1 Currently Deployed Cryptography

Understanding the quantum threat requires first looking at how cryptography is used today and why some algorithms are more vulnerable than others.

There are two main categories: **confidentiality** and **authentication**. In symmetric cryptography, the same key is shared by sender and receiver. Block and stream ciphers provide confidentiality, while hash functions and Message Authentication Code (MAC) algorithms ensure authentication. Most real-world systems use both, achieved through authenticated encryption with a single key.

Symmetric cryptography faces two challenges. First, before communication can occur, both parties must agree on a shared secret — a complex task for large-scale systems and impractical in open networks like the internet.

Post-quantum cryptography is not optional — it's the next foundation of trust.



The solution is **public-key cryptography**. A sender can encrypt a key with the recipient's public key, which is then decrypted with the private key. Alternatively, public-key agreement allows two users to establish a shared secret by exchanging public keys — reducing the challenge to verifying the authenticity of those keys.

This authentication problem is addressed through **digital signatures**. A Certification Authority (CA) signs a user's name and public key with its private key, enabling anyone with the CA's public key to verify authenticity. This shifts trust to the CA's key, a manageable problem. Digital signatures also serve broader purposes, akin to handwritten signatures: they can authorise transactions or validate code updates.

As of 2025, around 90 billion devices and applications use cryptography for confidentiality and authentication. Roughly 60 billion rely on public-key cryptography (often combined with symmetric methods), while 30 billion use only symmetric-key cryptography.

The following applications rely on public-key cryptography:

- **Network communications:** TLS and SSH (transport layer security), IPsec (network layer security), Bluetooth (data link security), messaging apps such as WhatsApp, iMessage, Messenger, Signal, and email security protocols like S/MIME and PGP.
- **Data at rest:** in databases or cloud environments, public-key cryptography manages the symmetric keys that encrypt bulk data.
- **Authentication:** digital signatures are used for code authenticity, secure boot and secure update. Digital signatures are essential for updates. They also underpin user authentication and authorisation standards such as FIDO2, OpenID Connect, and OAuth, as well as e-passports and electronic identity cards. Public Key Infrastructures (PKIs) distribute authenticated copies of public keys.
- **Financial transactions:** digital signatures protect credit card payments via the EMV standard and are fundamental to cryptocurrencies such as Bitcoin and Ethereum.
- **Trusted Execution Environments:** platforms like Intel SGX/TDX and Arm TrustZone use digital signatures for remote attestation.

The public-key algorithms used in these protocols rely on two number-theory problems considered hard for classical computers:

- **Factoring large integers:** the basis of RSA for encryption and digital signatures.
- **Computing discrete logarithms:** in multiplicative groups modulo a large prime or elliptic curve groups, underpinning DSA, ECDSA, EdDSA, and the Diffie-Hellman key exchange protocol.

Public-key cryptography is always combined with symmetric-key cryptography, which is two to three orders of magnitude more efficient. This combination is traditionally called “**cryptography in hybrid mode**”¹.

The most widely used symmetric algorithms are block ciphers such as AES and 3-DES, and stream ciphers such as ChaCha20 and SNOW-3G. These are paired with MAC algorithms to provide authenticated encryption (e.g. AES-GCM, ChaCha20-Poly1305). Digital signature schemes are combined with hash

functions such as SHA-2 and SHA-3. In the post-quantum world, “hybrid algorithm” has a different meaning (see later).

Some applications rely exclusively on symmetric-key cryptography:

- **Networking at the data link level:** 2G/3G/4G/5G (mobile communications), WPA, WPA2, WPA3 (Wi-Fi).
- **Data at rest:** protection on local devices (e.g. hard disk encryption).
- **Payments:** debit card transactions and some contactless or mobile payment schemes.
- **Password protection schemes.**

In addition to mainstream applications, more advanced cryptographic techniques are gaining traction. These include zero-knowledge proofs (for pseudonyms or privacy-friendly proofs of attributes), oblivious pseudo-random functions (to detect leaked passwords without revealing which), and methods for computing on encrypted data such as multi-party computation and fully homomorphic encryption.



3.2 The Vulnerability of Current Cryptography

With this understanding of how cryptography is applied, the next question is resilience: which techniques are threatened by quantum computing, and why?

The quantum threat does not affect all algorithms equally. In 1994, mathematician Peter Shor introduced a quantum algorithm that can efficiently factor large numbers and compute discrete logarithms. A CRQC running Shor’s algorithm could break all widely used public-key algorithms, as their security depends on the hardness of these problems.

Symmetric cryptography is affected differently. Grover’s algorithm (1996) could, in theory, speed up brute-force attacks. However, standards such as

AES-256 and SHA-3 (with appropriate parameters) can counter this at moderate cost. In practice, experts believe Grover’s algorithm will not be feasible to implement for decades, meaning the timeline for upgrading symmetric systems is far less urgent than for public-key cryptography.

The reassuring point is that cryptography itself will not disappear — it must simply evolve. Post-quantum cryptography (PQC) represents a new generation of algorithms believed to withstand both classical and quantum attacks. Designed to run on classical systems, they can be integrated into existing hardware and software. These algorithms rely on hard mathematical problems that are currently resistant to quantum attacks.

¹ In the post-quantum world, “hybrid algorithm” has a different meaning (see later).



3.3 Research on Post-Quantum Algorithms

Since the invention of public-key cryptography in 1975, researchers have explored alternatives beyond number theory — both to diversify and to seek more efficient schemes. These early efforts were not initially motivated by concerns about quantum computing.

By the early 1990s, three main approaches had emerged:

- **Code-based cryptography:** e.g. the McEliece algorithm, based on the difficulty of decoding large random error-correcting codes.
- **Multivariate cryptography:** relying on the hardness of solving quadratic or multivariate polynomial equations over finite fields.
- **Hash-based signatures:** depending on the security properties of cryptographic hash functions.

So far, no quantum algorithm is known that can efficiently solve these problems.

The publication of Shor’s algorithm (1994, public-key crypto) renewed interest in these alternatives, grouped under the term post-quantum cryptography (PQC) or quantum-safe cryptography. The field grew steadily, and the first PQC conference was held in Leuven in 2006.

In the early years of public-key cryptography, knapsack schemes attracted attention for their efficiency compared to number-theory-based schemes. However, they proved insecure. Research has since revived this line under the name of lattice-based cryptography. For encryption, it relies on the hardness of solving large linear equations with noise added (the Learning With Errors — LWE problem). For digital signatures, it uses the hardness of the Short Integer Solutions — SIS problem. To improve efficiency, additional structure is introduced into lattices; these are known as modular lattices.

Other promising approaches include isogeny-based cryptography. Although the first scheme of this type (SIKE) was broken, there is optimism about its potential over the next decade.

Belgian researchers have played a major role in PQC development. They proposed innovative lattice-based algorithms (see Section 3.4) built on rounding rather

than noise (e.g. SABER). They also uncovered major flaws in high-profile schemes, including multivariate algorithms (RAINBOW, SNOVA) and isogeny-based schemes (SIKE). By exposing these weaknesses before standardisation, they strengthened the security of emerging PQC standards.

3.4 Post-Quantum Public-Key Standards

Early research eventually led to formal standardisation, most prominently by the US National Institute of Standards and Technology (NIST). In 2016, NIST launched an open call for post-quantum standards. After a multi-year competition with over 80 submissions, five schemes were selected. By October 2025, three had been published. Three are lattice-based, one is hash-based, and one is code-based.

Public-key encryption/key establishment:

- **ML-KEM**
Module-Lattice-Based Key-Encapsulation Mechanism (FIPS 203, Aug 2024)
formerly CRYSTALS-Kyber
- **HQC-KEM**
Hamming Quasi-Cyclic Key Encapsulation Mechanism, a code-based scheme (FIPS 207, expected 2027)

Digital signature schemes:

- **ML-DSA**
Module-Lattice-Based Digital Signature Algorithm (FIPS 204, Aug 2024)
formerly CRYSTALS-Dilithium
- **SLH-DSA**
State-Less Hash-based Digital Signature Algorithm (FIPS 205, Aug 2024)
formerly SPHINCS+
- **FN-DSA**
FFT over NTRU-Lattice-based Digital Signature Algorithm (FIPS 206, expected 2026)
formerly Falcon

In addition, the IETF has published two stateful hash-based signature schemes: XMSS (RFC 8391) and LMS (RFC 8554). They are more efficient than SLH-DSA but require the signer to maintain state — loss of state breaks security — making them unsuitable for replicated environments.

NIST is still evaluating an alternative signature scheme with better performance. Some EU member states favour Frodo-KEM over ML-KEM: its larger, less structured public keys may offer added security at the cost of efficiency. Germany's BSI supports Classic McEliece, with very large public keys but compact ciphertexts.

China, Japan, Malaysia, and Korea are also considering national PQC standards, potentially diverging from NIST's selections. Even if ML-KEM and ML-DSA are expected to dominate, the global landscape will likely remain complex.

Finally, it is important to note that no efficient battle-tested PQC constructions neither enterprise-ready implementations yet exist for anonymous credentials, oblivious PRFs, or certain zero-knowledge proofs — these remain active research topics.

3.5 Performance

With new standards emerging, many organisations ask: how do these algorithms compare in practice? Are they slower, bulkier, or harder to implement than existing techniques?

Several companies have released libraries implementing the new standards. For research and testing, the Linux Foundation's Open Quantum Safe project¹ is useful — though not production-ready.

In terms of speed (key generation, encryption, decryption, signing, verification), ML-KEM and ML-DSA perform close to current standards, with differences largely offset by newer hardware. Legacy devices may see slowdowns, and no PQC scheme matches the extremely fast verification of RSA signatures with exponent $e = 3$. SLH-DSA (SPHINCS+) has efficiency issues, though limiting the number of signatures could improve performance.

¹ <https://openquantumsafe.org>

The main challenge is size: public keys, ciphertexts, and signatures can be three to ten times larger (or more). In some contexts — embedded devices, small packet sizes, large certificate chains — substituting PQC schemes directly may break applications. This issue is compounded when combining classical and post-quantum schemes (see next section).

For communications security, standards are advancing quickly, but PKI remains a bottleneck. Some experts propose new architectures for distributing authenticated public keys rather than adapting the current PKI.

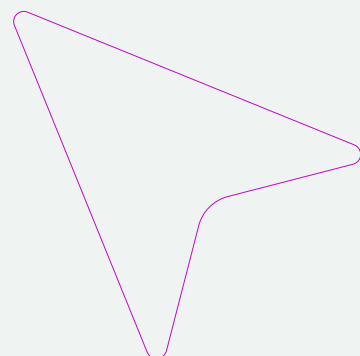
Finally, securing implementations against physical attacks (side-channel, fault, or combined) remains difficult. In environments like embedded devices, building secure and efficient implementations will require further research.

3.6 Cryptography in Hybrid Mode

Although confidence in post-quantum schemes is growing, experts agree it is too early to replace all classical algorithms outright. The preferred migration path is therefore hybrid cryptography, which combines classical and post-quantum protection. Both sender and receiver must support both algorithms.

- **Encryption and key establishment:** a key is encrypted first with a classical algorithm, then with a post-quantum algorithm; or a shared key is derived via both Diffie-Hellman and a post-quantum scheme, then combined.
- **Digital signatures:** both a classical and a post-quantum signature are generated, and the verifier must check both.

The drawback of hybrid schemes is higher cost and complexity, and, hence, attack surface. The benefit is greater crypto-agility: once a hybrid approach is deployed, replacing the classical algorithm with a new post-quantum one becomes easier.



Taking the First Steps Towards Post-Quantum Readiness

The looming threat of quantum computing has direct implications for today's digital infrastructure. While the exact timeline remains uncertain, the risk to widely used public-key algorithms is real, and proactive preparation is both prudent and expected.

Organisations do not need to start from scratch. National agencies, industry consortia, and international bodies have published detailed guidance. Notably, the Dutch PQC Migration Handbook¹ and the EU Coordinated Implementation Roadmap² provide in-depth resources. The EU roadmap sets phased targets: national strategies by 2026, protection of critical infrastructure and other high-risk use cases by 2030, and broad adoption across sectors by 2035. Organisations should align their plans with these milestones.

Quantum readiness begins with awareness — and succeeds with action



This chapter translates these ambitions into practical steps for Belgian organisations. While each case is unique, most will follow a similar three-phase journey towards quantum-safe readiness.

These phases may overlap in practice, but their sequential logic provides a valuable structure to help prioritise actions and allocate resources. Taking the first step today — even just gaining awareness of the issue and assessing exposure — can save significant effort and cost in the years ahead.

¹ <https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook>

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

Phase 1

Awareness and Assessment

Phase 2

Planning and Strategy

Phase 3

Implementation and Beyond

4.1 Phase 1: Awareness and Assessment

4.1.1 Build an understanding on quantum computing

The first step towards post-quantum readiness is developing a clear understanding of quantum computing and its impact on cybersecurity. This is not just a technical issue; it requires strategic awareness across IT, security, leadership, and audit teams.

Organisations can build awareness through workshops, webinars, or by sharing resources such as this white paper. By engaging with this document, your organisation is already taking a meaningful step. As noted earlier, many publications can also support this journey.

Internal teams do not need deep expertise, but a basic grasp will enable them to collaborate effectively with external specialists and make informed decisions based on their organisation's context.

4.1.2 Assess data sensitivity, lifespan and migration effort

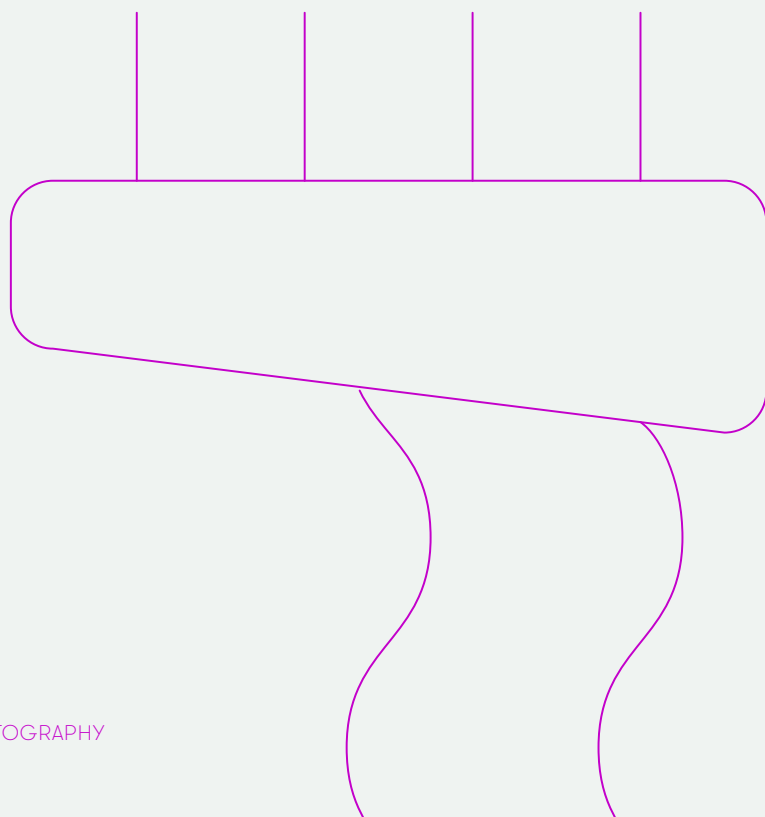
To understand which cryptographic mechanisms must be migrated, organisations first need clarity on their data: what it is, how it is used, and how sensitive it is. This does not require a full inventory but should cover key aspects such as:

- Type of data (at rest, in transit, in use).
- Assets handling the data.
- Value in terms of confidentiality, integrity, and availability.
- Classification (sensitivity).
- Retention period.
- Current protection mechanisms.
- Ease or difficulty of updating or replacing them.

This overview allows organisations to prioritise data sets for migration. Highly sensitive, long-lived data (e.g. state secrets, critical infrastructure) should come first. As explained in Chapter 2, data not at immediate risk may become vulnerable before systems can be upgraded. Data at rest protected by symmetric cryptography often poses less risk than data in transit, which usually relies on public-key cryptography.

Authentication mechanisms (e.g. digital signatures) also need early assessment, especially when they are difficult to replace or expected to remain in use when a CRQC appears.

Practical prioritisation guidelines will be addressed in Volume 2.



Levels		Confidentiality	Transition effort and impact	Asset lifetime
Low		Not significant	< 8 years	< 10 years
Medium		< 10 years	> 8 years low impact	> 10 years low impact
High		>= 10 years	> 8 years high impact	> 10 years high impact

Quantum Risk Levels¹

Migration timelines by risk level:¹

- **Low:** Migration can be scheduled in a later phase.
- **Medium:** Start planning by end of 2026, complete pilots by end of 2030, and achieve full migration by end of 2035.
- **High:** Start planning by end of 2026, with full migration completed by end of 2030.

Note: At this stage, the focus is only on assessing and prioritising data assets by sensitivity and required lifespan. The cryptographic mechanisms protecting the data will be addressed in the next step.

4.1.3 Identify and inventory cryptographic assets

Once critical data has been identified for migration, the next step is to assess how it is currently protected. This requires visibility into all systems and applications that rely on cryptography.

The assessment should provide insight into:

- Which cryptographic algorithms are used.
- Which libraries, hardware, and protocols are in place.
- Which dependencies exist on suppliers for cryptography.

A full inventory is valuable but should not delay migration. Since building it can be a major effort, organisations should use the earlier sensitivity and lifespan assessment to prioritise the systems that matter most. The inventory must be a living document, updated as systems evolve and risks

change. Because it reveals potential vulnerabilities, it must be secured and access limited to authorised parties. A governance model should define ownership, responsibilities, and processes for updates across teams and geographies.

Where possible, inventories should leverage automated tools such as network scans, code scanning, and database checks. These provide continuous input and help detect weak or outdated cryptography in near real time. This is relevant not only for quantum security but also for broader crypto-agility (see Section 4.3.4) and compliance.

Vendor dependencies are critical. Many cryptographic assets, both hardware and software, come from third parties. Organisations should evaluate vendor roadmaps and request cryptographic bills of materials (CBOMs) to identify where and how cryptography is used across products and services. Contracts and SLAs should be updated to require transparency on PQC support.

Beyond official suppliers, other sources must also be considered — internal collaboration tools, instant messaging, or shadow IT. These too should be inventoried, as customers may increasingly expect proof of PQC readiness.

Finally, legacy systems that cannot transition to PQC should be flagged early. If upgrading is not feasible, organisations must plan for their phase-out. Because replacements can take years, early identification is essential for timely mitigation.

¹ The European Union’s Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (PQC).

4.1.4 Identify vulnerabilities

By combining the data sensitivity assessment with the cryptographic inventory, organisations can prioritise which migrations to tackle first. As explained in Chapter 3, only certain algorithms are vulnerable to quantum attacks, with public-key cryptography the primary concern.

The inventory may also reveal algorithms and protocols already considered weak in the classical context, such as SHA-1 or TLS 1.1. Replacing these with secure modern alternatives strengthens today's security and provides a training ground for broader PQC migration. These early wins build experience, processes, and awareness ahead of the more complex transition.



4.2 Phase 2: Planning and Strategy

After building awareness and identifying cryptographic assets in Phase 1, the next step is to define a clear strategy and plan the transition to PQC. This involves setting direction, allocating resources, and creating a roadmap. It should be approached as a major software and hardware migration project, where tasks such as planning, inventory, and dependency mapping are common to any large-scale transition.

4.2.1 Developing a post-quantum strategy

The strategic plan should align with the organisation's business objectives and risk appetite. Key elements include:

- **Set clear objectives** — Define why migration is pursued: compliance, future-proofing, maintenance, or risk reduction.
- **Define the scope** — Identify which assets, data, and systems are covered, based on Phase 1 mapping.
- **Establish timelines** — Set target dates and intermediate milestones.
- **Define KPIs** — Determine how progress and success will be measured. Ensure KPIs are actionable and aligned with the roadmap.

➤ **Assign methodology and resources** — Select an execution approach. Based on scope and timeline, assess whether current tools and expertise suffice or if external support is needed.

➤ **Review** — Schedule regular reviews to adjust for evolving risks, external dependencies, and lessons learned.

These elements should guide, not constrain, the plan. For example, a broad scope with short timelines may require stronger resource investment.

4.2.2 Defining governance: roles and responsibilities

Clear governance is essential for a successful PQC migration. Leadership and executive sponsorship must be in place, with accountability defined at the top level to drive the transition. Operational responsibilities should be clearly assigned so teams know what is expected of them at each stage of the roadmap.

Governance also requires coordination structures for consistent monitoring of progress and a clear process for escalating decisions. External engagement is equally important: someone must be tasked with liaising with suppliers, regulators, standards bodies, and industry groups.

Documenting these roles and responsibilities early helps reduce ambiguity, avoid overlap, and maintain momentum throughout this complex, multi-year effort.

4.2.3 Evaluating post-quantum cryptographic solutions

Like classical cryptography, PQC offers algorithms with different security levels and performance characteristics. Organisations should set baseline requirements in a cryptography policy to guide algorithm selection. Not every algorithm suits every use case: factors such as computing power, memory, transaction speed, communication or storage overhead, and system integration all matter.

For each priority identified in Phase 1, organisations should select the most suitable algorithm consistent with their policy. Current standards are outlined in Section 3.4, but as standardisation is ongoing, staying up to date is essential.

4.2.4 Creating a transition roadmap

A detailed roadmap is essential to turn strategy into action. It should define realistic timelines, milestones, and KPIs, aligned with the prioritisation from Phase 1 and the planning insights from Phase 2. Migration effort must also be considered: if a high- or medium-risk system takes longer to migrate, it may need to be addressed earlier.

The roadmap should reflect organisational objectives and require close coordination with suppliers to assess their readiness and ensure joint planning. As a first step, a proof of concept on a simple use case — ideally in a test or development environment — can reveal knowledge or resource gaps and build confidence.

Public resources, such as the Dutch PQC Migration Handbook¹, offer practical guidance for designing roadmaps and anticipating implementation challenges.



4.3 Phase 3: Implementation and Beyond

After preparing the groundwork in Phase 1 and evaluating approaches in Phase 2, organisations move to implementation. This phase is about executing the PQC migration plan and embedding resilience into systems and processes for the long term. As before, a risk-based, iterative approach is essential.

4.3.1 Deploying post-quantum solutions

The final stage is the execution of the Phase 2 plan. By now, organisations should have a clear view of their most critical assets and which PQC alternatives they will migrate to. In some cases, high-priority assets may be migrated first, with the broader plan executed in parallel.

Key considerations during migration include:

- **Operational technology and long-lived hardware** — Updating such systems may be difficult if they are incompatible with new algorithms. Replacement or phase-out may be required. Algorithm choice for these devices must prioritise robustness, as upgrades are harder than for software. Cryptographic checks should become part of ongoing maintenance.
- **Hybrid solutions** — Standardised, tested hybrid approaches (see Chapter 3) should be used whenever feasible.

¹ <https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook>



4.3.2 Continuous monitoring and adapting

Transitioning to PQC is not the end—security requires continuous attention. After deployment, organisations must monitor the cryptographic landscape, reassess deployments, and adapt to new vulnerabilities, implementation issues, or updated standards. This is especially important as algorithms and best practices will continue to evolve after initial adoption.

Resilience depends on embedding cryptographic monitoring into regular security operations. This means tracking standards (e.g. NIST, ETSI), following cryptanalysis developments, and engaging in industry or vendor update channels. For organisations without urgent migration pressures, this phase also offers a chance to observe early adopters and adjust plans based on lessons learned and interoperability challenges.

4.3.3 Collaborating with industry peers

Implementation and resilience are strengthened through collaboration. Organisations often share suppliers, rely on similar technology stacks, or operate in interconnected sectors. Joint efforts can raise awareness with vendors, influence roadmaps, and support interoperable solutions.

Beyond supplier engagement, sharing experiences and coordinating with industry bodies, sector-specific groups, communities, or Belgian and European authorities can accelerate ecosystem-wide readiness. Collaboration improves cost-efficiency, reduces duplication, and strengthens preparedness.

In Belgium, initiatives such as the **Crypto Focus Group** of the Cyber Security Coalition and the **Quantum Circle** provide valuable platforms for knowledge exchange, alignment, and coordinated action.

4.3.4 Building toward crypto-agility

Post-quantum migration gives organisations rare visibility into how cryptography is used across their systems. But this should not be treated as a one-time fix. As vulnerabilities emerge and standards evolve, further migrations will be needed. The goal must be crypto-agility — the ability to adapt cryptographic mechanisms quickly and safely over time.

Crypto-agility means that replacing an algorithm should be as seamless as possible, ideally through configuration rather than redevelopment. While full agility across complex environments may not always be feasible, adopting crypto-agile practices where possible reduces future costs, minimises risk, and enables faster responses to new threats.

Organisations should integrate crypto-agility into PQC migration efforts now — through system design, procurement, change management, and cryptographic policy. This includes ensuring that products can receive secure firmware or software updates signed with quantum-safe algorithms. This principle underpins the upcoming Cyber Resilience Act (CRA), which mandates crypto-agility for new products from December 2027. Commission Implementing Regulation (EU) 2024/2690, effective October 2024, already requires IT providers to demonstrate crypto-agility where appropriate. Other frameworks such as DORA and NIS2 also stress up-to-date cryptographic practices, making crypto-agility a growing regulatory expectation. Future versions of the CyberFundamentals Framework will reflect this as well.

Crypto-agility is not limited to technology. It requires organisational alignment — policies, processes, and roles that enable timely, secure updates. Investing in crypto-agility is therefore a no-regret move, strengthening resilience and making future migrations — quantum-related or not — faster, safer, and more sustainable.

Finally, crypto-agility extends beyond PQC. Synergies between PQC programmes and other initiatives such as NIS2, DORA, and the CRA should be identified. Leveraging overlaps improves efficiency, aligns compliance, and reduces duplication, particularly for large organisations.

Conclusion

Quantum computing is no longer a distant possibility — it is becoming a reality.

This white paper was written to help business leaders understand the profound implications of this shift and to guide them in preparing their organisations for the post-quantum era.

The threat is clear: quantum computers will eventually break the cryptographic systems that protect today's most critical systems and sensitive data. The time to act is not when quantum computers arrive, but now—while there is still time to prepare.

Migration to post-quantum cryptography is not a simple software update. It requires a strategic, organisation-wide effort: inventorying cryptographic assets, engaging vendors, updating contracts, and investing in crypto-agile systems. It also requires leadership — executives who understand the stakes and are willing to drive change.

But this is more than a defensive move. Organisations that lead on quantum readiness will not only protect their data and operations — they will build trust with customers, partners, and regulators. They will show resilience, foresight, and a commitment to security that sets them apart.

Preparing for the quantum era is not only about mitigating risk — it is also about seizing opportunity. A secure organisation is a confident one, ready to innovate and grow in a digital world that is changing faster than ever. The future belongs to those who act today.

**Quantum resilience
is a leadership
challenge, not just
a technical one.**



What You Need to Know

- Migration to PQC is complex: it requires strategic planning, vendor coordination, and leadership.
- Early action builds trust: with customers, regulators, and partners.
- Quantum readiness is a competitive advantage: it enables innovation and resilience.
- The time to act is now: waiting increases exposure and cost.

Executive Roadmap: What to Do and When

Timeframe	Key Actions
Next 6 Months	— Initiate a cryptographic asset inventory — Identify high-risk systems — Engage CIO/CISO on quantum readiness — Begin vendor discussions
Next 12 Months	— Develop a post-quantum migration strategy — Update procurement and security policies — Launch pilot projects with PQC algorithms — Begin staff awareness and training
Next 5 Years	— Complete migration of critical systems — Establish crypto-agility as standard practice — Monitor quantum threat landscape

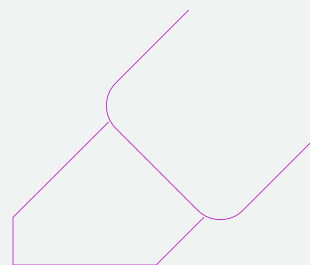
Key Questions for CIO/CISO

- What cryptographic assets are currently in use across our organisation?
- Which systems or data are most vulnerable to “harvest now, decrypt later” attacks?
- Are our vendors and partners preparing for post-quantum cryptography?
- How are we ensuring crypto-agility in future system designs?
- What internal capabilities or external support do we need to succeed?



ACRONYMS

3-DES	Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard with Galois/Counter Mode
AI	Artificial intelligence
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CBOM	Cryptographic Bill of Materials
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
CRQC	Cryptographically relevant quantum computer
CRYSTALS	Cryptographic Suite for Algebraic Lattices
DORA	Digital Operational Resilience Act
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
EMV	Europay, Mastercard, and Visa
EU	European Union
FFT	Fast Fourier Transform
FIDO2	Fast IDentity Online 2
FIPS	Federal Information Processing Standards
FN-DSA	Fast Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm
GDPR	General Data Protection Regulation
HQC-KEM	Hamming Quasi-Cyclic Key Encapsulation Mechanism
ICS	Industrial Control Systems
IETF	Internet Engineering Task Force
Intel SGX	Intel Software Guard Extensions
Intel TDX	Intel Trust Domain Extensions
IoT	Internet of Things
IPsec	Internet Protocol Security
IT	Information Technology



KEM	Key Encapsulation Method
KPI	Key Performance Indicator
LMS	Leighton-Micali Hash-Based Signatures
LWE	Learning With Errors
MAC	Message Authentication Code
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MPLS	Multiprotocol Label Switching
NIS2	Network and Information Systems Directive 2
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAuth	Open Authorization
OT	Operational Technology
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POS	Point of sale
PQC	Post-Quantum Cryptography
PRF	Pseudorandom function
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SD-WAN	Software-Defined Wide Area Network
SHA	Secure Hash Algorithm
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solutions
SLA	Service Level Agreement
SLH-DSA	State-Less Hash-based Digital Signature Algorithm
SNOVA	Simple Noncommutative-ring based UOV with key-randomness Alignment
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
WPA	WiFi Protected Access
XMSS	eXtended Merkle Signature Scheme

Team



This white paper is the result of a collaborative effort, bringing together expertise from the Belgian Cyber Security Coalition, the Quantum Circle, and the Centre for Cybersecurity Belgium (CCB). It has been produced to the best of the contributors' abilities.

Development Team

Sarah Ampe

Consultant Digital Risk
EY

Johan Kestens

Architect/Product Owner
Link2Trust

Bart Preneel

Full Professor
COSIC, KU Leuven

Maria Chiara Properzi

Analyst
CCB

Jan Sonck

Quantum Ecosystem Manager
Quantum Circle

Joachim Vererfven

Solutions Engineer
Proximus Group

Laura Vranken

IT Security Officer
Belfius

Jelle Wieme

Cybersecurity Engineer
CCB

Expert Reviewers

Bassili Ataya

Management Consultant in Cyber
Risk, Privacy and Cloud
Cavell Group

Rik Bobbaers

Tech CISO
ING Global

David Burghgraeve

Subject Matter Responsible IAM,
PAM & Crypto
Colruyt Group

Fabrice Clement

CISO
Proximus Group

Olaf Jonkers

CISO
itsme®

Christian Mathijs

Cathy Suykens
Cyber Security Coalition

Roel Peeters

Cryptography Expert
itsme®

Bojan Spasic

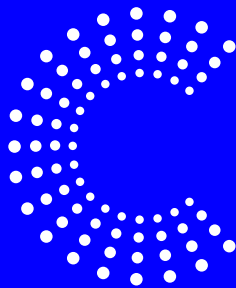
Senior Manager Technology
Research
Sony

Peter Spiegeleer

Enterprise Security Architect
Proximus Group

Kristof Verslype

Cryptographer
Smals



CYBER SECURITY **COALITION**

The mission of the Cyber Security Coalition is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem. We do so by bringing together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform aimed at fostering information exchange, operational peer-to-peer collaboration, making recommendations for more effective policies and guidelines, and finally carrying out joint awareness-raising campaigns aimed at citizens and organisations. More than 1,700 representatives of our 220+ member organizations participate in our activities and as such contribute to our mission.

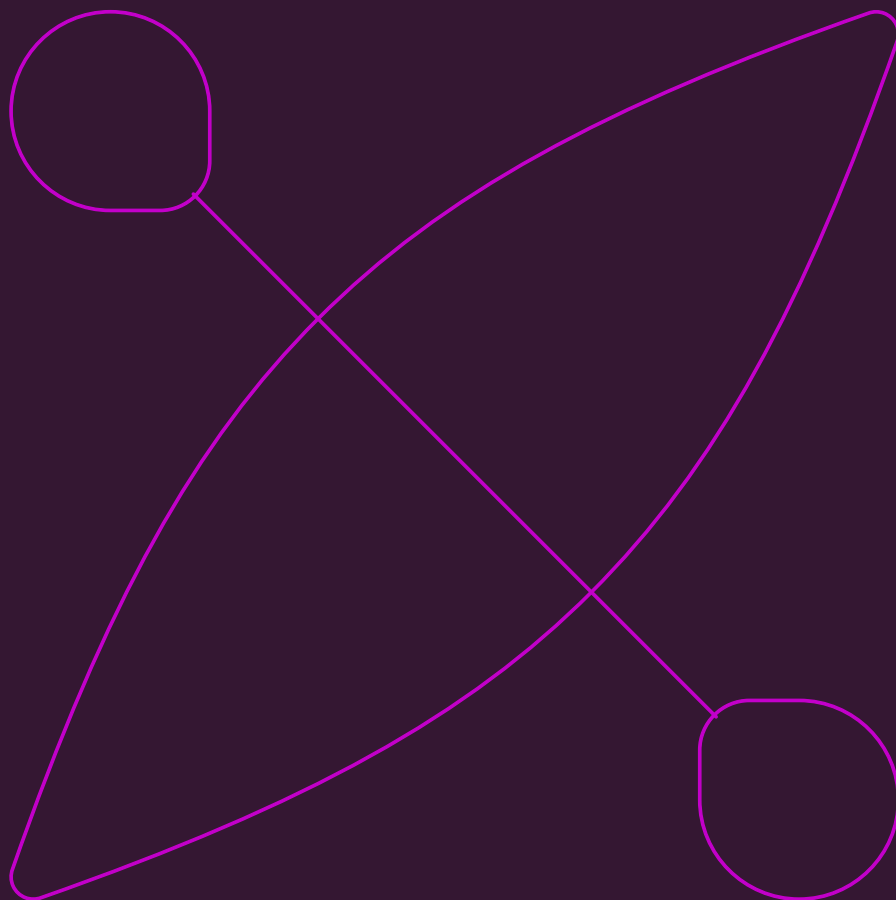
cybersecuritycoalition.be



quantum circle

The Quantum Circle is a community uniting quantum enthusiasts and experts to engage with the market on revolutionary technology, collaborate on distinguished industry use cases and applications, accelerate market adoption, shaping a visionary investment landscape with societal and economic impact.

quantumcircle.eu



Publication date

September 2026

Contact

Cyber Security Coalition

Henk Dujardin
CEO

+32 (0)475 84 00 42
henk.dujardin@cybersecuritycoalition.be

Quantum Circle

Jan Sonck
Quantum Ecosystem Manager

+32 (0)478 34 53 69
jan.sonck@quantumcircle.eu