BIS Papers
No 158

# Quantum-readiness for the financial system: a roadmap

by Raphael Auer, Donna Dodson, Angela Dupont, Maryam Haghighi, Nicolas Margaine, Danica Marsden, Sarah McCarthy and Andras Valko

Monetary and Economic Department

July 2025

JEL classification: C19, C63, C8, M15, G1, G17.

Keywords: central banking, quantum computing, quantum-safe cryptography, quantum-readiness, cryptographic agility, financial stability, financial system, cyber security.

The views expressed are those of the authors and not necessarily the views of the BIS.

This publication is available on the BIS website (www.bis.org).

ISSN 1682-7651 (online)
ISBN 978-92-9259-869-3 (online)

# Quantum-readiness for the financial system: a roadmap

Raphael Auer, Donna Dodson, Angela Dupont, Maryam Haghighi,
Nicolas Margaine, Danica Marsden, Sarah McCarthy and Andras Valko[1]

## Abstract

Quantum computers may in the future break today's widely used encryption. This paper provides a framework to support the financial system in the transition to quantum-safe cryptographic infrastructures. It emphasises the need to start the transition today – with broad awareness and cryptographic inventory as critical foundations. While post-quantum cryptography offers a viable near-term solution, implementation challenges – including performance trade-offs and system integration – require coordinated planning. We caution against regarding this change as simple algorithm replacement. Ensuring the continued security and resilience of the global financial system may involve cryptographic agility, defence in depth, hybrid models and phased migration. Quantum key distribution may hold long-term potential, but several national security agencies note that it still faces infrastructure challenges that limit its immediate applicability.

Keywords: central banking, quantum computing, quantum-safe cryptography, quantum-readiness, cryptographic agility, financial stability, financial system, cyber security.

JEL classification: C19, C63, C8, M15, G1, G17.

[1] Raphael Auer and Andras Valko are with the Bank for International Settlements (BIS), Maryam Haghighi and Danica Marsden are with the Bank of Canada, Sarah McCarthy is with the University of Waterloo and Donna Doodson is a former employee of the National Institute of Standards and Technology. Angela Dupont is with the BIS and the Bank of France. Nicolas Margaine works at Bank of France. The views expressed are those of the authors and not necessarily those of the BIS, the Bank of Canada or the Bank of France. We thank Marc Farag, Jermy Prenio, Brian Ritchot, Pietro Tiberi and William Zhang for valuable comments on earlier drafts.

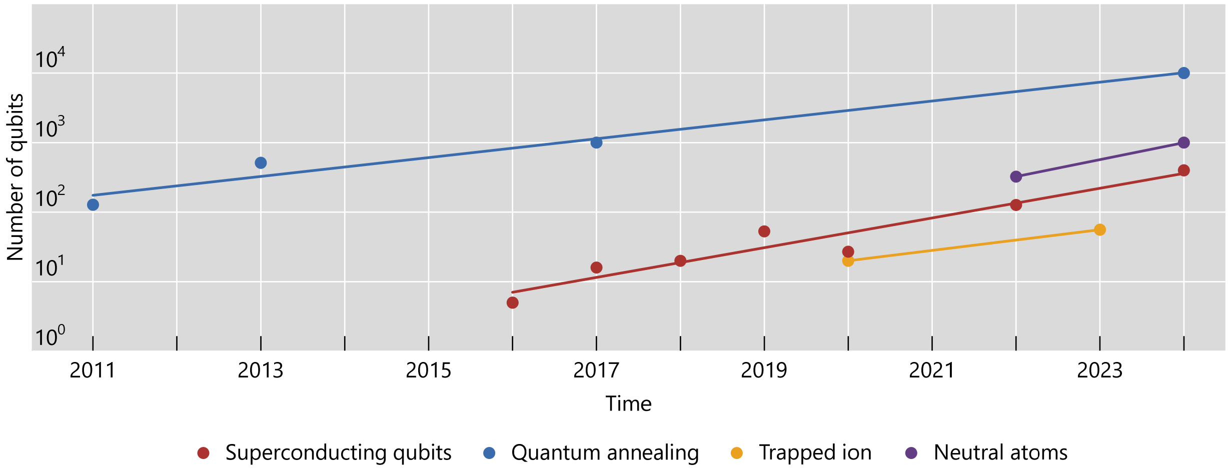
# 1. Introduction

The rapid advancement of quantum computing presents both opportunities and risks for the financial sector (Auer et al (2024)). Quantum computers may offer opportunities for innovation as they can solve certain classes of problems better than classical computers. At the same time, they pose a significant threat to the global financial system due to their expected ability to break some of the encryption methods that are widely used in today's financial systems.

While small-scale quantum computers exist today, the timeline for the appearance of a cryptographically relevant quantum computer (CRQC), ie a computer capable of compromising current public key cryptography, remains uncertain. However, if current trends continue, a CRQC may be realised as soon as in the next decade (Graph 1). Each year, the Global Risk Institute releases the *Quantum threat timeline report*, which synthesises the insights of leading experts on the current state of quantum computing and the threat it poses for cyber security. The 2024 report indicates that 27% of experts expect the emergence of a CRQC to take place within 10 years and 50% expect it within the next 15 years.[2]

Evolution of quantum computing capabilities over time

Graph 1



Source: authors' elaboration based on companies' communications.

We note that the dangers posed by quantum computers are more imminent than their development horizon. Risks to data confidentiality, integrity and authentication extend to data harvested today, intended to be decrypted later – a scenario termed "harvest now, decrypt later" (HNDL) (Auer et al (2024)). Given this uncertainty and the complexity involved in migrating cryptographic infrastructures, organisations must urgently initiate preparations today. Cyber incidents within the financial system can threaten global stability, making cybersecurity a critical concern for central banks and financial institutions (CPMI-IOSCO (2016); Doerr et al (2022)).

In view of these developments, this paper outlines a strategic and pragmatic approach for public and private sector financial actors alike to transition towards

[2] Global Risk Institute (2024) provides a range with a pessimistic interpretation and an optimistic interpretation, indicating that between 19 and 34% of experts expect the emergence of a CRQC within 10 years.

quantum-safe cryptographic environments. Specifically, we emphasise raising internal awareness, implementing robust governance structures and maintaining comprehensive cryptographic inventories. Rather than simply replacing existing algorithms, our recommended actions include employing defence in depth strategies, prioritising resilience, adopting cryptographic agility,[3] using hybrid cryptographic schemes and implementing phased migration plans. Notably, initiatives such as the BIS Innovation Hub's Project Leap – the first phase of which was conducted jointly with the Bank of France and Deutsche Bundesbank – demonstrate the feasibility and urgency of quantum-safe preparations through practical experimentation with post-quantum cryptographic solutions (BIS (2023)).[4]

The remainder of this paper proceeds as follows. Section 2 explores the technical foundations of cryptography and the implications of quantum computing for financial systems and potential quantum-safe solutions. Section 3 provides a structured quantum-readiness roadmap, both on a systemic level and for individual participants in the financial system. Section 4 concludes.

## 2. A cyber threat to the financial system

### 2.1 Cryptography within financial digital infrastructure

Cryptography is used extensively across the financial system to provide assurances including confidentiality, integrity, authentication, access control and non-repudiation. Confidentiality means that messages or data are transformed into an unreadable encrypted format so that unauthorised parties are unable to view them. Data integrity ensures that data cannot be modified or altered without detection. Cryptographic authentication serves to verify the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system. Digital signatures, used for authenticating the identity of the signatory, can demonstrate to a third party that a signature was generated by the claimed signatory, thereby providing non-repudiation for electronic documents and contracts.

Cryptographic algorithms are the fundamental building blocks providing these cryptographic assurances. An algorithm can be considered as a set of mathematical instructions, which generates cryptographic keys, ciphertexts and signatures. A key is a parameter that – together with the sensitive data – determines the outcome of the encryption or signing algorithm. Without knowing the exact value of the key, it is difficult to know the outcome or answer of the algorithm, and it is that difficulty upon which the security of cryptography rests.

There are two principal types of key-based cryptographic algorithms: symmetric key and asymmetric key (also referred to as public key). They are compared in Table 1. These two classes of algorithm serve different assurance functions and cannot be used interchangeably. Asymmetric cryptography is primarily utilised to set up a secure communication channel or to support the certification of a user's identity, while symmetric cryptography is a more efficient method of encrypting large volumes of data within an established communication channel. Many digital communication use

[3] See Bucciol and Tiberi (2023).

[4] This work was based, in part, on earlier work, see Bank of France (2022).

cases require a combination of symmetric and asymmetric cryptography (Hellman (1978); Hellman et al (1980)).[5]

## Symmetric vs asymmetric cryptography

Table 1

| Symmetric key algorithms | Asymmetric key algorithms |
|---|---|
| Uses a single shared key for both encryption and decryption | Public key is used for encryption, while private key is used for decryption. Digital signatures perform encryption with private key and decryption with public key |
| Provides confidentiality for bulk data | Usually employed to establish a symmetric key or for authentication |
| Faster compared with asymmetric key cryptography | Enables secure communication without the need for prior key exchange |
| Requires secure key distribution to all communicating parties | Provides authentication and digital signatures in addition to confidentiality |
| Well suited for scenarios in which efficiency and performance are critical | Slower compared with symmetric key cryptography due to complex mathematical operations |
| Example algorithm widely used in the financial community is AES | Examples of algorithms used today in the financial systems include Rivest-Shamir-Adleman (RSA), elliptic curve cryptography (ECC) and Diffie-Hellman key exchange |

Sources: author’s elaboration.

Whereas algorithms provide the foundation for the deployment of cryptography, there are other factors such as key management, implementation practices and security protocols that are crucial for maintaining the security and integrity of the implementation. Key management governs the generation, distribution, use, storage, rotation and eventual destruction of keys. If these actions are not executed properly, even the strongest cryptographic algorithm is not effective in practice. There are multiple approaches to the management of cryptographic keys. One prevalent approach, public key infrastructure (PKI), is used in the context of asymmetric cryptography. PKIs enable secure communication by allowing public keys to be distributed openly, whilst private keys remain confidential. Establishing trust within this key management process is critical, for example by validating that a public key is associated with a particular user identity via a certificate. A PKI is also responsible for issuing, revoking and managing these certificates. A critical component of the PKI is the ”root of trust” which has ultimate authority for allocating trusted nodes.

Trust in the financial system is fundamentally tied to the trust provided by cryptography. Users of information technology (IT) must have confidence in the security of the financial system’s IT infrastructures and networks. Employing robust cryptographic methods ensures the protection of financial information, payment transactions and the smooth operation of the broader economy. Only a system in which data and communications are securely safeguarded with robust cryptographic solutions against unauthorised access, alteration and misuse, can maintain public trust.

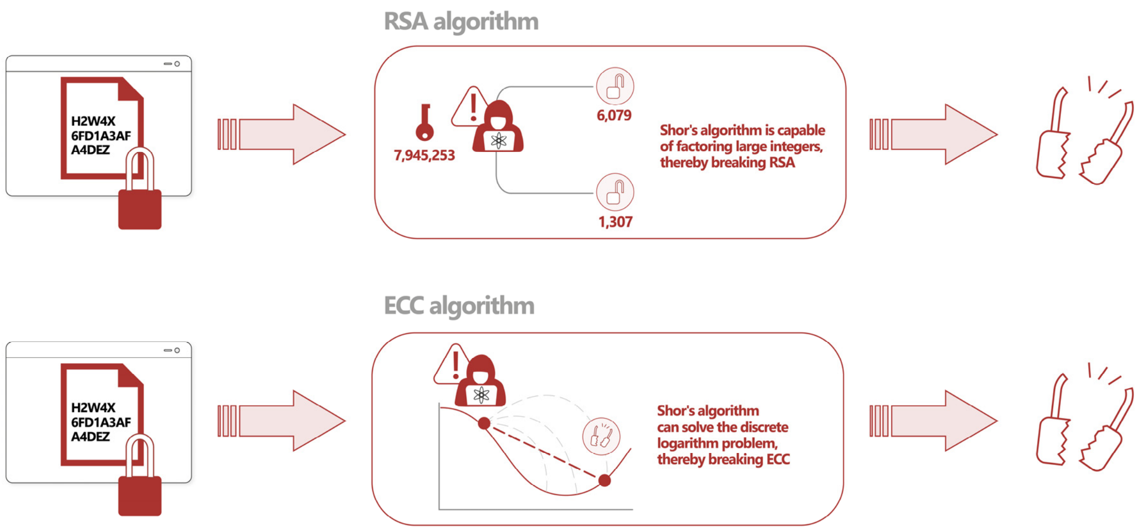
[5] For example, European Payments Council (2025) recommends symmetric key cryptography for bulk data encryption, and asymmetric key cryptography for encrypting symmetric keys and to perform signatures.

## 2.2 Cyber threats and quantum computers

Cryptanalysis refers to the discovery of a mathematical flaw in the security underpinnings of a cryptographic algorithm. This may consist of discovering the secret key or the ability to forge a valid signature. This exposes the user to cryptographic attacks such as data breaches in which an adversary obtains unauthorised access, into a computer network; accesses confidential information; and gains the ability to forge signatures or otherwise tamper with authenticated documents. Beyond cryptanalysis, the particular implementation or misuse of an algorithm can introduce attack surfaces. This can be prevented by following proper key management practices and secure software development practices, as well as the use of automated testing and zero-trust models. Undertaking code reviews and audits, as well as educating the existing workforce and hiring experienced developers also serve to prevent this occurring.

Quantum computing poses a threat to today's cryptography because of its enhanced ability to perform cryptanalysis. Shor's algorithm (Shor (1994), when run on a quantum computer, can factor large numbers and therefore break today's public key cryptographic algorithms, namely Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC),[6] in polynomial time (Graph 2) – ie within a time period that is useful to an adversary and allows them to access or tamper with confidential data or to forge an identity. At the time of Shor's discovery in 1994, a quantum computer did not yet exist and so the threat was not considered imminent. But accelerated development in the quantum computing space has shortened the timeline to reach

Cryptographic algorithms vulnerable to quantum computers Graph 2


RSA algorithm
H2W4X
6FD1A3AF
A4DEZ
7,945,253
6,079
1,307
Shor's algorithm is capable of factoring large integers, thereby breaking RSA
ECC algorithm
H2W4X
6FD1A3AF
A4DEZ
Shor's algorithm can solve the discrete logarithm problem, thereby breaking ECC

Source: authors' elaboration.

[6] RSA is based on the hard problem of factoring large prime numbers. CRQCs will be able to factor prime numbers exponentially faster than classical computers. ECC relies on the computational difficulty of solving discrete logs over elliptic curves. CRQC will be able to simultaneously explore potential solutions thereby reducing the difficulty of solving for the discrete logs.

the point at which Shor's algorithm can be put into practice. Further, since gaining access to a quantum computer would offer an actor the unprecedented possibility of obtaining classified information. It is questionable whether this step would be immediately announced publicly.

Grover's quantum search algorithm (Grover (1996)) has a similar impact to symmetric key cryptography, providing a quadratic speedup compared with classical key search. The risk from this can be mitigated for now by increasing key size – national governments currently recommend using Advanced Encryption Standard (AES) with a 256-bit key for sensitive and classified information (NIST (2024d)).

The primary threat of a CRQC to today's public-key cryptography is the ability to retrieve the private key of asymmetric key cryptography, and then either forge a signature or obtain the symmetric key to decrypt the data. The risk of malicious data decryption can be considered a present threat, as data could be collected today via HNDL attack, despite the impact of the attack not being experienced until a future date. HNDL attacks can result in data breaches and the future disclosure of highly confidential information. For instance, compliance with the EU's General Data Protection Regulation (GDPR) may be affected, as a quantum computer could undermine the security of the cryptographic methods currently used to protect personal data. In fact, the GDPR mandates that organisations should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the pseudonymisation or encryption of personal data. As the risk of quantum attacks is increasing, additional protection of key establishment schemes against such attacks will be required.

HNDL is not relevant to signature forging because an active attacker needs access to a CRQC in real time to run Shor's algorithm and obtain the private key. However, this does not mean that classical digital signatures can continue to be used until CRQC becomes available. Looking at the criticality of some long-term contracts such as mortgages, and the significant number of financial contracts signed digitally that will need to be updated with new signatures, there is good reason to start the migration in a timely manner. Specifically, for applications where digital signatures or data authentication is long-lived and today's signatures will still be operative at the time when a CRQC does exist, actions may be needed today to provide protection from future quantum forgeries. For an organisation, this may mean revoking signatures and resigning or counter signing a contract with a quantum-safe signature. Devices which are required to authenticate software updates may need to be equipped with post-quantum digital signatures upon manufacture today, so that they will be able to verify code signing with future quantum-proof signatures (NIST (2024d).

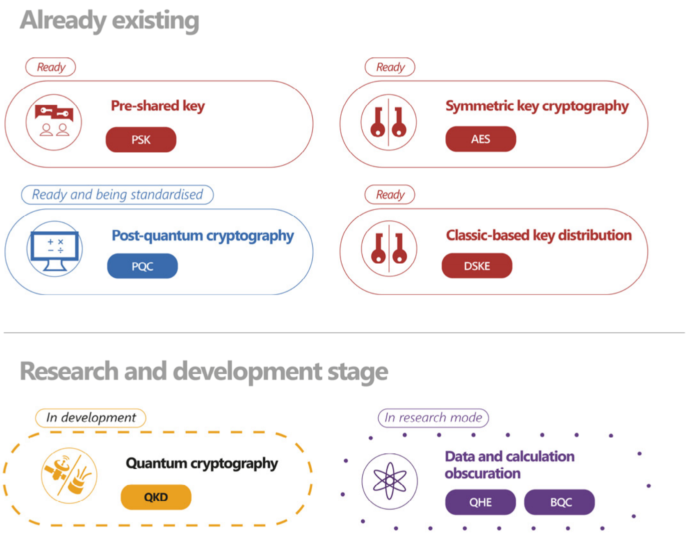
A security protocol invokes multiple cryptographic algorithms to construct a connection with desired security properties. The predominant cryptographic protocols employed to secure our data and transactions today include TLS, SSH, QUIC and IKEv2/IPsec, supported by X.509 certificates. If cryptographic algorithms are broken, this consequently renders these protocols insecure as well. TLS has established secured communication channels between a client and a server via a handshake protocol through untrusted networks. This handshake combines ECDH key exchange with a negotiated digital signature to establish trust and a shared master secret between the two parties, allowing them to send and receive data encrypted by AES. This widely used protocol for securing internet communications in its previous, but still widely used, version TLS 1.2, cannot be configured with post-quantum cryptographic algorithms. For the TLS framework to support quantum-safe cryptography, a system needs to migrate to its newest version, TLS 1.3. As a result, all legacy systems still relying on TLS 1.2 are vulnerable to the quantum threat and must consider upgrading to the more recent version that offers enough flexibility to incorporate quantum-safe cryptography. As these protocols are an integral component of legacy systems, the migration to quantum safety requires a complete overhaul, with care taken to manage the migration process.

While this paper adopts an information security perspective, the quantum threat also has implications for the operational resilience of financial systems. For example, digital signatures are used to sign applications, preventing IT systems from running without authorisation. Compromising signature algorithms may allow an attacker to gain access to a system, or to attach a forged signature to a piece of malicious code, thereby breaking the security of a system. The quantum threat amplifies the need for effective operational resilience mechanisms, for example business continuity policies that help to resume operations and restore data in the event of a security breach (Prenio and Restoy (2022)).

## 2.3 Overview of quantum-safe solutions

Solutions and standards for quantum-safe security already exist. Exploring their advantages, limitations and maturity will help organisations to prepare appropriate protection for their critical data and systems. The emergence of the quantum threat has led to research into the field of quantum-resistant cryptography. The cryptographic community has been working on new methods to mitigate the quantum threat for over a decade. Today, different options are at different stages of maturity. Some are already implementable, while others are still at the research and development stage. Among these options, three main categories can be identified: symmetric cryptography, post-quantum cryptography and quantum cryptography (Graph 3). The terminology might imply that "post-quantum cryptography" comes

Known methods for securing data that are stationary or in transit Graph 3


Already existing
Ready
Pre-shared key
PSK
Ready
Symmetric key cryptography
AES
Ready and being standardised
Post-quantum cryptography
PQC
Ready
Classic-based key distribution
DSKE
Research and development stage
In development
Quantum cryptography
QKD
In research mode
Data and calculation obscuration
QHE
BQC

Source: authors' elaboration.

after "quantum cryptography", but this is not the case, as will be explained below.

Post-quantum cryptography (PQC) is a class of cryptographic algorithms that can be run on our classical computers today. Its security is based on mathematical problems that are difficult for both classical and quantum computers to solve. It includes familiar concepts such as key establishment mechanisms and digital signatures, much like those used today. From a standardisation perspective, post-quantum cryptography stands out as the cryptographic solution that is most ready for migrating to quantum-safe systems. Its readiness is underscored by extensive research, ongoing development and the rigorous standardisation process it has undergone. The National Institute of Standards and Technology (NIST) opened up a call for proposals in 2016, encouraging researchers worldwide to develop viable post-quantum algorithms.[7] This was followed by several rounds of filtering, based on confidence in security, efficiency, suitably and ease of implementation. Whilst NIST conducted this process, it relied heavily on community input from all over the world. The initial algorithms were standardised in August 2024,[8] with continued analysis of the remaining finalists and a call for further algorithm proposals. Guidelines for transitioning to the new standards were released in November 2024 (NIST (2024d)). Meanwhile, other standardisation bodies such as ETSI, ITU-T, Internet Engineering Task Force (IETF), ASC X9 and ISO are publishing guidance and recommendations based on the NIST process (ETSI (2015); IETF (2021)). As part of its responsibility for internet protocols, IETF is investigating the addition of PQC support to its existing standards.[9] This is evident in the formation of a Post-Quantum Use in Protocols Working Group in 2023 and a hackathon on the integration of PQC into X.509 certificates.[10]

Today, to the best of the cryptography community's knowledge, PQC is considered a reliable choice for ensuring future-proof security against quantum threats. However, implementing PQC poses several challenges, including increased computational requirements, potential integration issues with existing systems and the need for thorough evaluation of new algorithms to ensure they meet both security and performance standards. The much larger key sizes, higher bandwidth costs, computationally intensive sampling mechanisms and high precision requirements mean that they are not simply drop-in replacements for today's cryptography. This is particularly challenging for applications such as point of sale systems that have limited computational resources and where low latency is essential.

Quantum cryptography fundamentally differs from both classical and post-quantum cryptography, which both rely on hard mathematical problems to ensure the security of data transmission and storage. In contrast to these, quantum cryptography leverages the principles of quantum mechanics for security. Quantum cryptography offers information-theoretic security guarantees. This means that increased computational power does not improve the attacker's ability to thwart the system's security. The most well known application of quantum cryptography is quantum key distribution (QKD), which is in development mode. However, QKD brings different challenges (Graph 4), including the need for specialised hardware. The core of the technology requires specialised and dedicated communication lines (involving optical fibre and satellite links). Accordingly, it can be an expensive option that limits interoperability. Furthermore, while it can establish a secure key between

[7] See NIST (2016).

[8] See NIST (2024a,b,c).

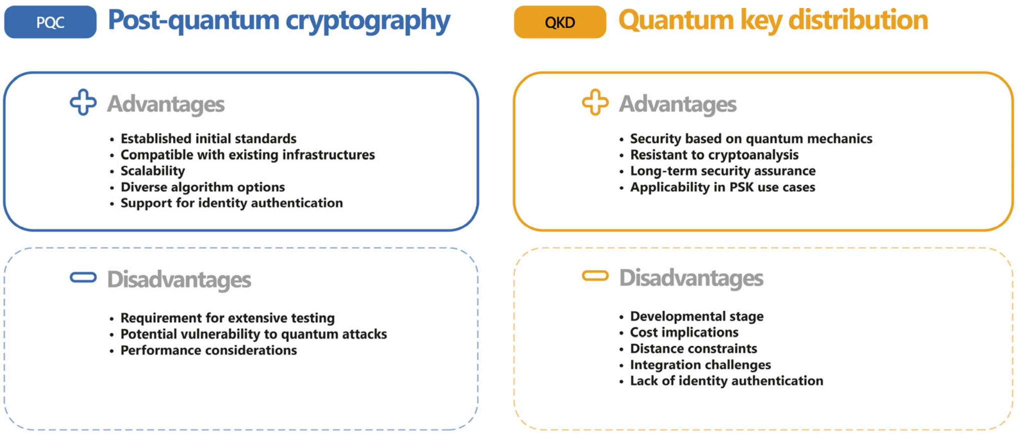
[9] See IETF (2025).

[10] See IETF (2024).

two or more parties, it does not have the ability to authenticate those parties. QKD experimentation has been conducted and certification efforts are ongoing, with a common criteria protection profile released by ETSI (ETSI (2024)).

A broader toolkit for quantum-safe solutions

Graph 4



PQC Post-quantum cryptography

Advantages

- Established initial standards
- Compatible with existing infrastructures
- Scalability
- Diverse algorithm options
- Support for identity authentication

Disadvantages

- Requirement for extensive testing
- Potential vulnerability to quantum attacks
- Performance considerations

QKD Quantum key distribution

Advantages

- Security based on quantum mechanics
- Resistant to cryptoanalysis
- Long-term security assurance
- Applicability in PSK use cases

Disadvantages

- Developmental stage
- Cost implications
- Distance constraints
- Integration challenges
- Lack of identity authentication

Source: authors' elaboration.

Among other quantum-cryptographic methods, quantum homomorphic encryption (QHE) and blind quantum computing (BQC) are noteworthy new technologies, though they are currently still in the research phase. As opposed to classical asymmetric cryptography, PQC and QKD, which support the establishment of keys between two communicating endpoints, QHE and BQC aim to preserve the confidentiality of data during computations. They cannot be used as replacements for existing asymmetric cryptography. QHE is an innovative approach that allows computations to be performed on encrypted data without needing to decrypt them first. This means that sensitive information remains protected throughout the computing process. QHE holds promise for secure data processing in various applications, from cloud computing to financial transactions. However, it is still in the experimental stage, with researchers working to overcome challenges related to efficiency, scalability and practical implementation. BQC is another promising quantum-safe method under investigation. BQC enables a client to delegate quantum computations to a quantum server while keeping the data and the computation itself hidden from the server. This ensures that even if the server is compromised, the privacy and integrity of the client's data are maintained. BQC has significant potential for secure cloud-based quantum computing services. Nevertheless, it is currently in the research phase, with ongoing studies focused on improving its feasibility, security and performance. Both QHE and BQC represent exciting advancements in the quest for quantum-safe solutions. Although they are not yet ready for widespread deployment, continued research and development in these areas are essential to prepare for a future in which such quantum algorithms can be implemented to secure systems.

Several protocols used today, such as TLS[11] and MACsec,[12] already support pre-shared keys (PSK). This refers to a shared key being transmitted out of band, such as upon device manufacture or via a manual in-place update. PSK gives strong security guarantees and with an appropriate key length quantum-security (NSA (2022)). A challenge relating to PSK is their distribution and this creates scalability challenges. Indeed, QKD could be adapted to become such a scalable key distribution solution. Centralised symmetric key management systems are also used to support PSKs. These key management systems ensure that keys are only accessible to those who have appropriate permissions. As shown in Graph 5, each solution presents benefits and challenges. Exploring each solution and understanding which one or which combination of solutions is most suitable for different use cases will enhance security frameworks, integrating more agile and resilient infrastructures.

## 2.4 Cryptography best practices

Quantum cryptography is still in an experimental phase and pre-shared keys have practical challenges. At the present time, the quantum-safe solution that is immediately available and implementable for organisations at a production level is PQC. Many organisations will find that a migration to PQC is their best option to protect sensitive data from quantum computers within the timeframe available for a transition. Nevertheless, this does not exclude the need to investigate other options over the mid and long run.

Transitioning to PQC is much more than a matter of replacing today’s public key algorithms with the new post-quantum ones. Historical precedents such as the migration from SHA-1 to SHA-2 showcase how lengthy the process of cryptographic transition is.[13] Starting the migration process early is essential to safeguard against future quantum threats. New cryptographic methods need to be deployed to integrate more flexibility and rapid response in a time in which cyber attacks are increasingly sophisticated and complex.

The concept of defence in depth is a contemporary approach to cyber resilience, involving a layered security defence incorporating diverse attack countermeasures. That way, if one layer is breached or needs to be patched, the remaining layers are in place to mitigate any lapses in security. Each layer is designed to block distinct types of attack. The benefit of this approach is that an adversary must breach all defences to successfully compromise a data system. The cost to the organisation is having multiple assets to manage and keep track of and this requires additional effort to maintain and secure the system. In the quantum era, one may utilise a combination of pre-shared keys and post-quantum cryptography, perhaps alongside two-factor

[11] RFC 8773: TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key / RFC 9257 - Guidance for External Pre-Shared Key (PSK) Usage in TLS / RFC 6071 - IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap / RFC 6617 - Secure Pre-Shared Key (PSK) Authentication for the Internet Key Exchange Protocol (IKE).

[12] 802.1AE-2018: MAC Security (MACsec, Revision of 802.1AE-2006).

[13] SHA-1, a widely used hash function, has been in use since 1995, but in the early 2000s it was found to have vulnerabilities. In 2017, a practical collision attack was successfully executed, proving that SHA-1 was no longer secure. A more secure version of the algorithm, SHA-2, has been available since 2002. NIST retired the SHA-1 algorithm in 2022, setting the final phase-out date as 31 December 2030 (NIST (2022)).

authentication for access control, to reduce the chances of a successful data breach. For each use case, organisations can tailor their solution in coordination with vendors after evaluating security requirements and the acceptable level of overheads and costs.

An associated principle is cryptographic agility, which refers to the ability to reconfigure or modify cryptographic defences in response to cyber threats or attacks. It is a measure of an organisation's ability to adapt cryptographic solutions or algorithms (including their parameters and keys) quickly and efficiently in response to developments in cryptanalysis, emerging threats, technological advances and/or new vulnerabilities. Further, it is a design principle for implementing, updating, replacing, running and adapting cryptography and related business processes and policies with no significant architectural changes, minimal disruption to business operations and short transition times (FS-ISAC (2024)). Upgrading the security infrastructure to protect against quantum threats offers an opportunity to incorporate agility to accommodate future cryptographic developments, which could take the form of increased key sizes or switching to alternative algorithms. This aligns with the principle of defence in depth, which ensures that there is always a back-up layer of security, and is a suitable solution for central banks, which need to avoid any downtime for their systems. Furthermore, it provides long-term cost effectiveness as it allows for seamless adaptation to evolving standards. However, the disadvantages of this risk-averse approach are a larger hardware and software footprint, a more advanced cryptographic infrastructure for employees to be trained on and to maintain, and further complexity around interoperability and algorithm negotiation.

Both concepts support the use of hybrid techniques. Hybridisation refers to retaining traditional cryptography in tandem with new quantum-safe techniques (Graph 5).[14] A modular approach to cryptographic infrastructure accommodates hybridisation techniques such as nesting multiple algorithms. The resulting security is as strong as the strongest algorithm, hence if unforeseen (classical or quantum) attacks on quantum-safe alternatives emerge, the security will still be as strong as it was previously.

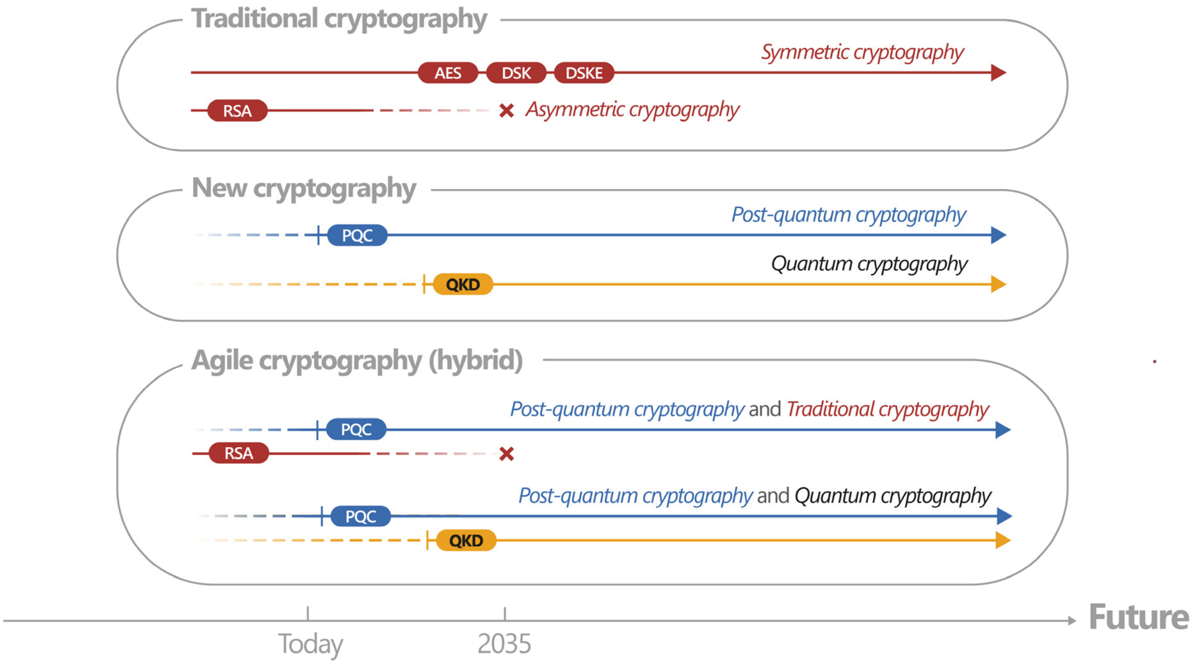
The opinions and advice on hybrid methods vary across jurisdictions. NIST specifies the instantiation of a hybrid scheme, namely combining a cryptographic algorithm standardised by NIST, the so-called post-quantum cryptographic algorithms with traditional cryptography (NIST (2024d)). The new Federal Information Processing Standards "support security protocols and applications that choose to implement hybrid approaches" (NIST (2024d)), but NIST has stated that this is not a necessary step as it is confident in the intensive evaluation process of the newly standardised algorithms. The National Security Agency (NSA) "has confidence in CNSA 2.0[15] algorithms and will not require national security system developers to use hybrid certified products for security purposes" (NSA (2024)). According to this view, hybridisation introduces some risk of implementation error and may prolong the transition process. The IETF highlights the fact that many post-quantum algorithms

[14] The term "hybridisation" is also used to refer to combining multiple quantum-safe cryptographic methods, including a combination of post-quantum cryptography and quantum cryptography.

[15] The Commercial National Security Algorithm suite 2.0 is a set of cryptographic algorithms selected by the NSA to protect national security systems against both classical and quantum threats. It updates the earlier CNSA 1.0 suite by incorporating quantum-resistant algorithms.

are relatively new and have not been subject to the same depth of study as RSA and ECC, and thus the security community may wish to favour hybrid cryptographic implementation as an appropriate step prior to an eventual transition to new quantum-safe cryptography (IETF (2021)). The National Cyber Security Centre of the United Kingdom recommends following the NIST standards for PQC and preparing to use it alongside traditional cryptography during the transition period (NCSC (2020)). The German Federal Office for Information Security (BSI) and the French Cybersecurity Agency (ANSSI) state that if possible PQC should be used only in a hybrid mode alongside conventional cryptography (BSI (2020); ANSSI (2023)).

Quantum-safe and agile cryptography roadmap Graph 5


Traditional cryptography
Symmetric cryptography
AES
DSK
DSKE
RSA
Asymmetric cryptography
New cryptography
Post-quantum cryptography
PQC
Quantum cryptography
QKD
Agile cryptography (hybrid)
Post-quantum cryptography and Traditional cryptography
PQC
RSA
Post-quantum cryptography and Quantum cryptography
PQC
QKD
Future
Today
2035

Source: authors' elaboration.

Graph 5 shows a roadmap of the various approaches and options to cryptography going forward. Out of the traditional cryptographic methods (top box), symmetric-key techniques will continue to be used, with an increased key length. On the other hand, the existing asymmetric cryptography techniques, most specifically RSA, will need to be discontinued.

The two main alternatives to the discontinued asymmetric cryptographic techniques are QKD and PQC, as shown in the middle box. Both have their advantages and disadvantages, and both tracks should be pursued, but since QKD is still in the experimental phase, the approach available in the near term is PQC. Many national cyber security agencies have published a position on the use of QKD, arguing that this technology still faces infrastructure challenges that limit its immediate applicability. For example, the United Kingdom's National Cyber Security Centre has stated that "quantum safe cryptography using standards-compliant products is the recommended mitigation for the quantum threat, once such products become available." ((NCSC) (2020)). Meanwhile, the NSA "views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution" than

QKD and does not support the use of QKD in National Security Systems (NSA (undated)). The Canadian Centre for Cyber Security recommends "migrating to standardised PQC as the best option for organizations to achieve quantum safety" (CCCS (2025)). The conclusions of joint work undertaken by the national cyber security agencies of France, Germany, the Netherlands and Sweden are similar (see eg ANSSI et al (2024)).

The third box shows how hybrid techniques can be applied going forward. In the immediate future, a combination of classic cryptography with PQC is relevant, as well as a hybrid combination of different PQC algorithms. Going forward, as QKD becomes more mature, a hybrid combination of PQC with QKD might become a viable option.

All options need to be considered, depending on the use case, with a short-, mid- and long-term view. Independently of the type of cryptographic schemes deployed, organisations need to anticipate the replacement of RSA as early as possible. NIST has already stated that RSA will be deprecated after 2030 and disallowed after 2035 (NIST (2024d)).

## 2.5 Implications of PQC migration

The migration to PQC is not a "flip the switch" moment – it will take place over an extended period of time. Unlike some cryptographic upgrades of the past, the new algorithms are not a drop-in replacement. Rather, they introduce significant architectural and operational challenges. Hence, it is crucial to determine the areas of organisational infrastructure to prioritise and assess the size and scope of each part.

Many PQC algorithms, particularly lattice-based schemes, require substantially more memory and computational resources than their classical counterparts, which can strain embedded and resource-constrained systems. The newly standardised PQC algorithms are significantly different in terms of speed, processing power and memory required, both compared with each other and with today's cryptography. For instance, the public key size of RSA encryption used to give 112 bits of security is 256 bytes. In comparison, a PQC algorithm such as ML-KEM public key providing 192-bit security has a size of 1,184 bytes, with the respective private key having a size of 2,400 bytes. For signatures, a 128-bit security ECC key is 32 bytes in size, giving a signature size of 64 bytes. In contrast, the same security level for ML-DSA generates 1,312-byte public keys and 2,420-byte signatures. More favourably, FN-DSA, at 192-bit security, has a public key size of 897 bytes and a signature size of 666 bytes, but utilises floating point arithmetic, which is challenging to implement securely and requires specialised hardware to achieve desirable speeds. These capabilities may not be uniformly available across existing infrastructure.

Other issues to consider are the complex sampling processes which lie at the heart of several lattice-based schemes. A lot of the security guarantees are rooted in these time-consuming sampling processes, which can be traded off for storage by employing lookup tables – introducing alternative challenges – and they can introduce security weaknesses if not deployed correctly. This is just one example of how the implementation of PQC can be complex for unfamiliar developers.

The PQC algorithms have not yet stood the test of time and are subject to changes and reconfigurations. Migration must therefore account for protocol-level adaptations, new key encoding formats, and the need for hybrid or transitional mechanisms to maintain compatibility and confidence during rollout. Together, these factors underscore the need for detailed planning and risk assessment across the full stack – from hardware and libraries to protocols and applications. Accordingly, when choosing which algorithms to migrate to, one should consider the requirements and priorities for each use case.

# 3. Quantum-readiness: a roadmap for the financial system

In what follows, we outline a roadmap to support the transition to quantum-safe cryptographic infrastructures. The interconnected nature of the financial system mandates coordinated and proactive action by institutions within a jurisdiction and globally. Therefore, we start with recommendations for a systemic quantum-readiness roadmap, followed by guidelines relevant for each institution in their quantum-readiness journeys.

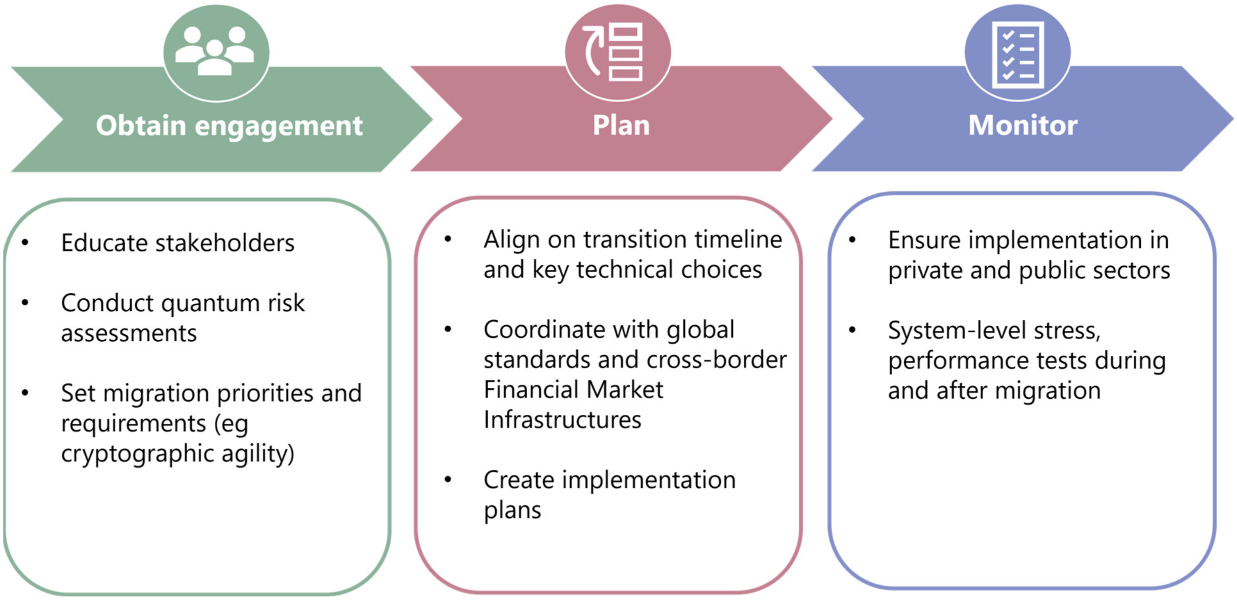
## 3.1 A systemic roadmap

Private sector financial institutions, central banks, regulatory organisations, various branches of government and cross-border payment systems are intrinsically integrated and connected. These links may involve frequent exchanges of information including sensitive and private data that need to be carefully guarded in order to protect the public interest. As a result, it is crucial to prepare for and manage the risks of tomorrow while continuously enhancing current processes and technologies.

Financial services are deployed extensively on a global and cross-border basis. They are exceedingly digital and web-based, and thus heavily rely on encrypted digital transactions. The interconnectedness of the domestic and global financial system adds to the complexity of quantum-readiness and mandates a coordinated and proactive action plan by central banks, supervisory authorities and financial institutions around the world. Conversely, in the absence of coordination, actors that are not adequately protected against the quantum threat could become weak links, impacting the security of the entire financial system.

Graph 6 illustrates some key steps on the road to ensuring the quantum-readiness of the financial system from the point of view of central banks and supervisors. Since the transition requires broad collaboration across different participants in the financial system, the first phase consists of obtaining engagement across the relevant stakeholders. This includes educating stakeholders and the general public. A crucial next step involves assessing the risks represented by quantum computers on a systemic level. The risk analysis needs to take into account the sensitivity of various data assets, as well as the longevity of the protection required. Following the risk assessment and building on its output, participants in the financial system will need to set migration priorities and requirements. This should include aspects of cryptographic agility in order to prepare systems for a continuously evolving cyber threat landscape.

A systemic roadmap to quantum-readiness in the financial system Graph 6



**Obtain engagement**

- Educate stakeholders
- Conduct quantum risk assessments
- Set migration priorities and requirements (eg cryptographic agility)

**Plan**

- Align on transition timeline and key technical choices
- Coordinate with global standards and cross-border Financial Market Infrastructures
- Create implementation plans

**Monitor**

- Ensure implementation in private and public sectors
- System-level stress, performance tests during and after migration

Source: authors' elaboration.

The engagement phase will be followed by the planning phase in which participants in the financial system translate the jointly agreed priorities and requirements into a system-level migration timeline and a set of common technical choices. Individual organisations can take their migration steps separately but major cornerstones of the transition need to be agreed across multiple actors due to the interconnectedness of the financial system. For example, a cut-off date for phasing out legacy cryptographic protocols needs to be approved by all organisations that use those protocols, or adequate backward compatibility mechanisms need to be incorporated. Key technical choices requiring alignment include, for example, cryptographic algorithms, key size and hybridisation. Financial actors also need to agree about the level of cryptographic agility that will be supported by the domestic financial system. Cryptographic agility, that is the ability to modify cryptographic defences in response to evolving cyber threats, is an important aspect of future-proof security systems. In a trade-off between flexibility and efficiency, stakeholders will need to agree the right balance for the financial system. Moreover, domestic plans need to be aligned with transition plans in other jurisdictions and in cross-border systems, such as multi-currency payment and settlement infrastructures.

Following the planning phase, participants in the financial system will execute transition plans, while central banks and supervisors will play a key role in monitoring progress. Regular follow-up and continuous alignment will help to ensure that the plans are executed in a timely manner, both in the private and public sectors, and the financial system reaches the required level of protection against quantum computing attacks. As a final step in the transition process, system-level stress, performance and penetration tests will need to be performed to verify the suitability of cyber protection achieved. In addition, QC resistance will need to be integrated into the cyber risk management framework of all participants, to support the continuous monitoring of quantum readiness going forward.

## 3.2 Quantum-readiness for financial system participants

The framework for this transition involves three critical actions: awareness, planning and execution. These actions should be considered through the interconnected lenses of people, policies, processes and technology with a particular emphasis on how data protection interacts with each element. A well coordinated approach ensures that all facets of the organisation are aligned to address the multifaceted risks and challenges posed by quantum computing rather than viewing it as a simple technical upgrade. In light of the emerging quantum threat, IT systems will need to adapt and integrate cryptographic agility.

### 3.2.1 Raising internal awareness and assessing readiness

As financial institutions embark on their quantum-readiness journey, they must first define what quantum-readiness means for the organisation and initiate a strategic conversation about the migration. This involves assessing the risks posed by emerging quantum capabilities and building organisational consensus around the need for cryptographic transformation.

At the centre of this process is the appointment of an executive leader responsible for driving the quantum-readiness programme. This individual must work closely with senior management across departments to align readiness efforts with institutional priorities and risk management frameworks. Their strategic mandate will include overseeing education efforts to raise awareness among staff and fostering a shared understanding of quantum-related challenges and opportunities.

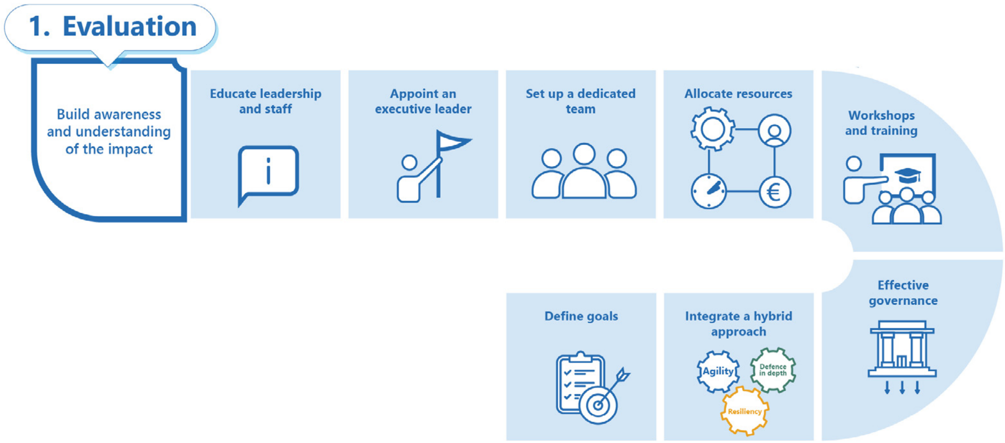
Forming a dedicated, cross-functional team is essential in this initial phase. This team should include representatives from technology, legal, human resources, finance, operations and security departments. Together, they will shape the roadmap towards readiness, identify key risks and set early priorities. Establishing a preliminary budget to support research, training and external consultation is another vital early task. Staff upskilling through workshops and targeted training will ensure that all relevant stakeholders possess the knowledge needed to engage with the topic meaningfully.

As part of the preparatory steps, governance structures must be put in place to guide decision-making and coordination across the migration process. The governance framework will promote consistency across divisions and ensure that the institution’s broader security and resilience goals are upheld.

A key decision will involve whether to adopt a hybrid approach – combining classical and quantum-resistant methods – or move entirely to post-quantum cryptography. Institutions may, for example, implement cryptographic agility by supporting multiple algorithms, such as using ML-DSA or SLH-DSA alongside RSA. Defence in depth strategies should also be considered, integrating traditional public key infrastructures with symmetric key systems and exploring the potential of QKD to generate secure cryptographic material. Establishing clarity on the scope of quantum readiness allows institutions to evaluate technical feasibility, assess associated costs and risks, and determine the best strategic approach. These initial steps lay the foundation for the practical work ahead, setting a clear vision and building the internal capacity necessary to support the migration.

Quantum-readiness roadmap

Step 1 – Awareness Graph 7



Source: authors' elaboration.

### 3.2.2 Planning the migration

Planning the migration to quantum-safe cryptography requires a comprehensive understanding of how and where cryptography is used within the institution. Institutions must start by identifying and prioritising sensitive information and systems that demand long-term protection. These may include classified communications, proprietary financial data and other critical systems that, if compromised, could have significant operational or reputational consequences.

A structured assessment of information sensitivity and the duration of protection required is vital in this phase. Institutions should classify data based on sensitivity – eg public, confidential or restricted – and estimate the timescales for which it must remain secure. For example, some financial records may require protection for several decades, while others may only need safeguarding for a few years. This exercise helps determine which systems need immediate attention and which can be addressed over time.

Many banking applications depend on cryptographic services provided by different layers of infrastructure. These include hardware, firmware, operating systems, applications and networks, each with its own migration considerations (Table 2). A phased migration strategy should be developed, mapping each system component to its appropriate timeline. For instance, while cloud services may automatically update protocols like TLS, legacy applications may require custom redevelopment. This nuanced approach prevents unnecessary disruption and helps maintain operational continuity.

Layers of IT systems impacted by quantum-safe migration

Table 2

| Layer | Systems and processes | Impact |
|---|---|---|
| **Hardware** | **Cryptographic hardware** | Devices such as hardware security modules, trusted platform modules or smart cards need to support quantum-safe algorithms |
| | **Network services** | Routers, switches and firewalls need firmware updates to support quantum-safe protocols |
| **Firmware** | **Embedded systems** | Firmware in internet of things devices, smart cards, and other embedded systems that use public-key cryptography for authentication will need to adopt quantum-safe algorithms |
| **Operating system** | **Kernel modules** | Cryptographic libraries and modules within the OS kernel must be updated to include quantum-safe algorithms |
| | **System devices** | Services that rely on encryption, such as file systems, secure boot processes, and network services, need to be updated |
| **Application** | **Software applications** | Applications that use cryptography for data protection, authentication, and communication must be updated to use quantum-safe algorithms |
| | **Web browsers** | Browsers need to support quantum-safe TLS/SSL protocols for secure web communications |
| | **Emails** | Protocols like S/MIME and PGP that rely on public-key cryptography for email encryption will need to transition to quantum-safe algorithms |
| **Network** | **Protocols** | Network protocols such as TLS, VPNs, SSH as well as Internet Key Exchange and IPsec protocols used for secure communication over IP networks will need to transition to quantum-safe cryptographic algorithms |
| | **Certificates** | Digital certificates and public key infrastructures (PKIs) need to be updated to use quantum-safe cryptographic algorithms |
| **Data** | **Databases** | Databases that store encrypted data must ensure that the encryption algorithms used are quantum-safe |
| | **Backup systems** | Backup and systems need to ensure that stored data remain secure against quantum attacks |
| **Security** | **Identity and access management (IAM)** | IAM systems must support quantum-safe authentication and authorisation mechanisms |
| | **Authentication and key management** | Single sign-on (SSO) solutions that rely on public-key cryptography will need to transition to quantum-safe methods |
| | **Security information and event management (SIEM)** | SIEM system needs to be updated to monitor and respond to quantum-safe cryptographic events |
| **Development** | **Development tools** | Compliers, code libraries and development frameworks must support quantum-safe cryptographic algorithms |
| | **Code review and testing** | Processes for code review and security testing need to incorporate checks for quantum-safe cryptographic practices |
| **Governance and compliance** | **Policies** | Organisational policies must be updated to mandate the use of quantum-safe cryptographic methods |
| | **Audits and assessments** | Regular audits and assessments need to ensure compliance with quantum-safe practices |

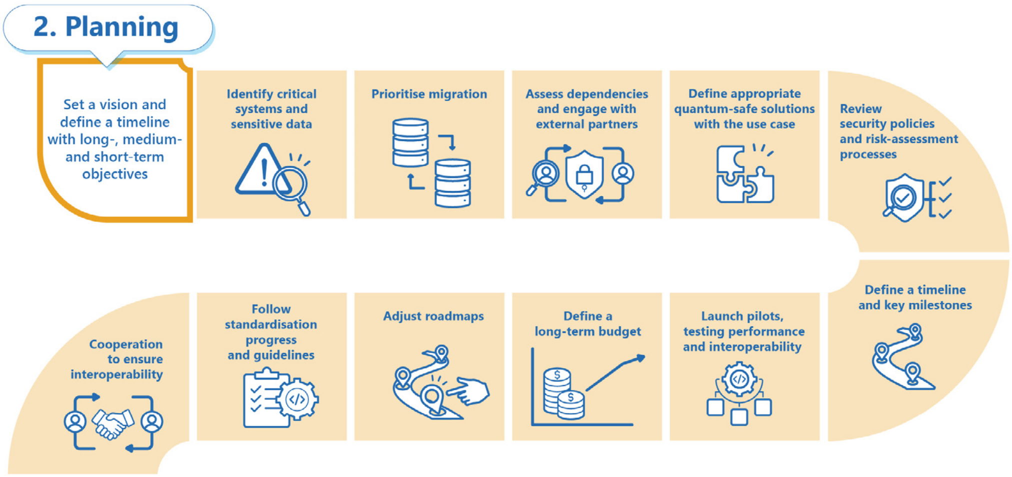
This list is not intended to be exhaustive, rather it provides significant examples.

Source: authors' elaboration.

Quantum-readiness roadmap

Step 2 – Planning

Graph 8


2. Planning
Set a vision and define a timeline with long-, medium- and short-term objectives
Identify critical systems and sensitive data
Prioritise migration
Assess dependencies and engage with external partners
Define appropriate quantum-safe solutions with the use case
Review security policies and risk-assessment processes
Define a timeline and key milestones
Launch pilots, testing performance and interoperability
Define a long-term budget
Adjust roadmaps
Follow standardisation progress and guidelines
Cooperation to ensure interoperability

Source: authors' elaboration.

Developing a cryptographic inventory is a crucial step in mapping the institution's cryptographic landscape. Automated discovery tools can identify how and where cryptography is used throughout the infrastructure, including on-premises and in cloud systems. These tools should generate detailed reports on the algorithms in use – whether symmetric, asymmetric or digital signatures – and flag outdated or vulnerable implementations. Manual reviews may still be necessary, particularly for legacy systems or security modules not easily scanned by automated tools.

Once the inventory is complete, institutions must determine the changes that need to be made internally, which updates will be handled by third-party vendors and which upgrades will be automatic. Coordination with vendors is critical, ensuring their roadmaps align with the institution's timeline and compliance expectations. This includes holding vendors accountable through service-level agreements and incorporating quantum-safe requirements into procurement processes. Existing risk management frameworks should be adapted to incorporate quantum resilience without the need for entirely new systems. Financial institutions can rely on their current practices for identifying critical systems and processes, as outlined by the Basel Committee and other supervisory bodies. These frameworks should be updated to reflect quantum-specific risks and extended to cover business continuity planning, third-party dependencies, and updated incident response procedures.

Institutions must also revise their internal security policies to reflect quantum-safe requirements. This includes protocols related to key management, data access controls, and cryptographic governance. New compliance requirements may need to be introduced for both internal users and external partners, ensuring consistent adherence to updated standards. Timelines and milestones must be clearly defined, accounting for interdependencies across systems and business functions. Activities such as cryptographic discovery, vendor integration, and data protection assessments should be scheduled to align with broader transformation initiatives. Pilot projects should be launched early in the planning phase to test migration approaches and identify potential issues. These pilots should involve systems with varying levels of complexity to provide insight into performance, compatibility, and resource requirements.

Budget planning should extend beyond the initial assessment phase. Institutions must account for costs related to staffing, tooling, system upgrades, testing, training, and ongoing monitoring. A long-term funding strategy will be essential to support the transition and sustain security throughout the post-migration period. Interoperability must be a central concern throughout the planning phase. Systems must remain functional during and after the transition, both internally and in communication with external entities such as other banks, financial market infrastructures, and public services. Institutions should prioritise the adoption of widely accepted standards and quantum-safe algorithms that support backward compatibility, facilitating a smooth migration process across the financial ecosystem.

### 3.2.3 Executing implementation

Executing the migration to quantum-safe systems is an iterative process that evolves alongside continued planning. Implementation should begin with systems identified as high priority or those with well tested quantum-resistant solutions. Automating parts of the transition can accelerate progress, particularly in systems that handle critical data or perform essential operations. Testing and validation are central to the execution phase. New cryptographic implementations must be thoroughly tested to ensure they function correctly within existing infrastructure, maintain performance levels, and do not compromise system integrity. These tests must confirm that systems are cryptographically agile – capable of switching between algorithms as standards develop – and that they remain compatible with partners that are not yet quantum-ready.

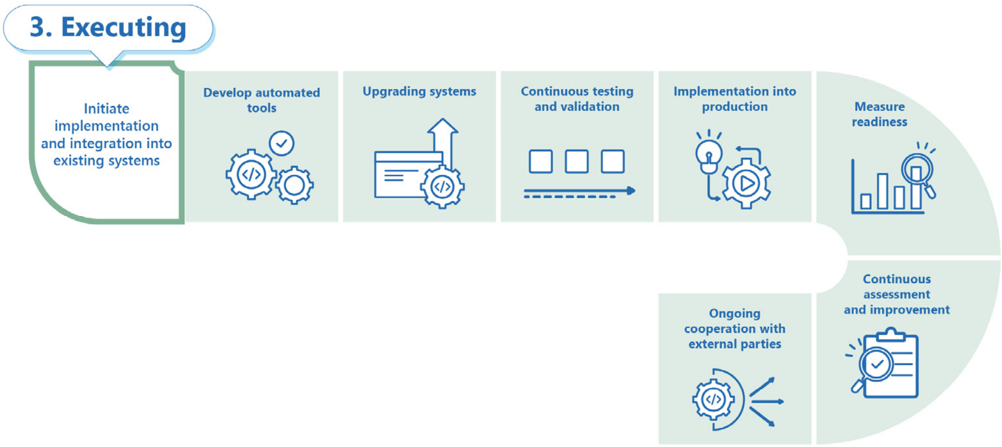
The deployment of quantum-safe solutions into live production environments marks a key milestone in the roadmap. Institutions must ensure that these implementations perform reliably under operational conditions and do not introduce unforeseen vulnerabilities. Regular testing and system health monitoring will help mitigate risks and ensure continued functionality. Establishing benchmarks and performance metrics allows institutions to track progress and assess readiness. These might include cryptographic performance, resilience to simulated quantum threats, interoperability, and compliance with defined standards. A structured framework for measurement helps institutions identify weaknesses, prioritise improvements, and document outcomes. Third-party systems and vendor integrations must also be evaluated against these metrics to ensure external compliance.

A continuous assessment cycle supports long-term success. As quantum technologies evolve, financial institutions must revisit their cryptographic strategies, update their risk assessments, and refine their implementations. This adaptive approach promotes institutional agility and helps maintain resilience in the face of emerging threats. Ongoing collaboration with vendors is essential during the implementation phase. Institutions must ensure that third-party systems meet updated cryptographic requirements and that shared roadmaps are maintained. Service-level agreements should reflect quantum readiness expectations, and the integration of new cryptographic capabilities must be seamless and secure. The execution phase will generate insights that feed back into the planning process, allowing for refinements and re-prioritisation. This feedback loop ensures that quantum-readiness remains an ongoing, dynamic effort, grounded in practical testing, clear governance, and a commitment to long-term cryptographic security. Through careful execution and iterative refinement, financial institutions can prepare for the quantum era without compromising operational integrity or trust.

Quantum-readiness roadmap

Step 3 – Executing

Graph 9


3. Executing
Initiate implementation and integration into existing systems
Develop automated tools
Upgrading systems
Continuous testing and validation
Implementation into production
Measure readiness
Continuous assessment and improvement
Ongoing cooperation with external parties

Source: authors' elaboration.

## 4 Safeguarding the financial system: the role of the public sector

From the point of view of a central bank or financial supervisor, the landscape of risks and threats extends far beyond the organisation's internal systems and cyber hygiene. Any threat that is harmful to their integrity can undermine citizens' trust and confidence in the financial system. On the other hand, the role of central banks relating to trust, oversight and policy, makes them well placed to work with other participants in the global financial system to inform and prepare the design of quantum readiness roadmaps.

Central banks play a pivotal role in the financial system, engaging with a diverse array of entities as part of their role in managing their jurisdiction's monetary policy, ensuring financial soundness and stability, and providing financial services. The role of central banks necessitates regular and frequent connection and exchanges of data with other institutions, including government organisations, financial institutions, financial market infrastructures and a variety of third-party entities. Given this fundamental role, it is vital for central banks to ensure a timely migration to quantum-safe environments to effectively manage and mitigate risk to the public. This includes migrating the central bank's own digital infrastructure, as well as promoting and supporting migration throughout the entire financial system.

Governments are investing to advance quantum-safe cryptographic techniques. This includes funding academic and private research, as well as collaborative projects aimed at developing new cryptographic systems. As mentioned in Section 2, the NIST has been leading efforts to standardise post-quantum cryptographic algorithms through a global competition that encourages the cryptographic community to propose and evaluate new quantum-resistant encryption methods. Governments are engaging in collaborative efforts with other nations to share knowledge, research findings and best practices for developing quantum-safe IT systems. For example, in April 2024, the United Kingdom and Denmark signed a memorandum of understanding on co-operation within the area of quantum science and technology (UK Government (2024)).  The quantum threat is a global issue that requires international cooperation.

Other national initiatives have been announced, such as the quantum-readiness roadmap published by the US National Security Agency, the Cybersecurity and Infrastructure Security Agency and NIST (NSA (2023)). This high-level document underscores the importance of preparedness, particularly for organisations supporting critical infrastructures. It delineates the necessity of an organisation initiating preparations by developing such a roadmap for themselves. In April 2024, the European Commission published recommendations for a coordinated implementation roadmap for the transition to post-quantum cryptography, recognising the need for immediate coordinated actions among member states to plan a transition to new quantum-safe cryptographic algorithms without interrupting the security of critical infrastructures (EU (2024)). Similarly, Canada published its National Quantum Strategy in 2022, which has a range of objectives including increased security in a quantum-enabled world (Government of Canada (2022)). Furthermore, the Canadian Forum for Digital Infrastructure Resilience has developed a quantum-readiness document with the primary aim of providing a comprehensive set of recommended practices and guidelines (CFDIR (2024)). The document offers actionable advice to stakeholders within the financial sector, enabling them to plan and prepare for the transition of their digital systems to quantum-safe cryptographic technologies and solutions. It seeks to shorten the learning curve associated with this migration by providing illustrative examples. A key feature of the publication is its proposed list of questions for security solution providers which serves as a tool for stakeholders to assess vendor preparedness for the quantum transition. This proactive approach underscores the importance of strategic planning and informed decision-making in achieving a quantum-safe future.

Within the central banking community, several initiatives have been conducted. The BIS Innovation Hub, jointly with the Bank of France and the Deutsche Bundesbank, launched Project Leap in 2023. This initiative has two key objectives: raising awareness among the central banking community and experimenting with quantum-safe cryptography (BIS (2023)). The first phase has demonstrated that building a quantum-safe communication channel between France and Germany is achievable, by setting up a Virtual Private Network (VPN) with post-quantum cryptography in a hybrid mode. As part of the experiment, payment messages were successfully sent across this VPN between the two central banks. This pragmatic approach focuses on implementing cryptographic algorithms that are already approved by the NIST standardisation process. The Federal Reserve has also demonstrated its awareness of the threat (Board of Governors of the Federal Reserve (2023)). In November 2024, the Bank of France and the Monetary Authority of Singapore (MAS) conducted a joint experiment that explored sending emails encrypted with post-quantum cryptography (Bank of France and MAS (2024)).

Other initiatives explore QKD, such as the trial of QKD networks by the People's Bank of China (IMF (2021)). A conceptual study by the Bank of Italy highlights the need to reinforce the security of payment systems that rely heavily on vulnerable cryptography (Bucciol and Tiberi (2023)). As such, the authors envisaged replacing cryptographic protocols that are potentially threatened by quantum computers with new cryptographic systems based on quantum cryptography to protect sensitive information in transit between data centres as well as data at rest. Commercial banks such as HSBC and JPMorgan Chase have also partnered with technology leaders to trial novel quantum-safe solutions in their systems (HSBC (2023); JPMorgan Chase (2024)).

While it is encouraging to see the above-mentioned organisations and central banks beginning to take important steps towards quantum-preparedness, much work is still needed. This includes a range of technical assessments, policy recommendations and regulatory analyses to ensure that the critical operations, including those conducted within the financial system, are best situated to manage and mitigate current and future risks with respect to quantum. It is imperative to assess the extent to which existing regulatory frameworks are adequate for regulating a coordinated response to the quantum threat. Regulators and policymakers need to map current regulations to the context of quantum technology and identify gaps in both regulatory frameworks. For instance, the European Union's Digital Operational Resilience Act (DORA) takes potential future threats into consideration by stating, in Article 13, that financial institutions need to monitor technological developments on a continuous basis, including with a view to understanding the possible impact of new technologies on IT security requirements and digital operational resilience.[16] This includes updating risk management processes to effectively combat current or new forms of cyber threats. Moreover, DORA establishes the need for inventory certificates by January 2025, which is among the first steps required in a successful quantum-readiness roadmap.

From a supervisory perspective, authorities will need to revise standards for stress testing and penetration testing in a quantum context. A collaborative approach led by the Financial Conduct Authority and the Word Economic Forum underscores the importance of coordinated efforts involving regulators, central banks, industry players and academia to address quantum security challenges (FCA and WEF, 2024)). The paper, published in January 2024, provides a comprehensive framework and roadmap to navigate the complexities of transitioning to quantum-secure systems, ensuring the financial sector's resilience and integrity in the face of emerging quantum technologies. It recommends proactive measures to mitigate the severe risks posed and a timeline for transitioning to new security models.

In February 2024, MAS released an advisory for financial institutions outlining necessary measures to address quantum risks. These include taking an inventory, working closely with vendors and advocating for both PQC and QKD as possible protections. In addition, MAS partnered with the Bank of France in November 2024 to demonstrate NIST-standardised PQC algorithms within Microsoft Outlook,

[16] Regulation (EU) 2022/2554 of the European Parliament.

highlighting the need for further research into PQC compatibility within common protocols (MAS (2024)).

In September 2024, the G7 Cyber Expert Group (CEG), chaired by the US Department of the Treasury and Bank of England, published recommendations (G7 (2024)). CEG identifies the quantum computing era as one of both potential benefit and risk to the financial system. The group encourages jurisdictions to monitor developments in quantum computing and promote collaboration among relevant current encryption methods. Financial authorities will need to work closely with relevant parties from the public and private sectors to raise awareness of the importance of transitioning to quantum-safe cryptography. Prioritising areas of intervention and exploiting synergies among G7 jurisdictions and standard-setting bodies will be key for success. This statement by the G7 CEG highlights the need for proactive measures, international coordination and ongoing dialogue to address the opportunities and risks of quantum computing in the financial sector. The Bank of Italy additionally ran a G7 workshop in September 2024 with a view to developing a shared understanding of the most urgent issues, a potential roadmap to address the transition to quantum resilience and, to the greatest extent possible, an agreed policy agenda.

## 5. Conclusion

The ability of quantum computers to break today's cryptographic algorithms represents an imminent threat to the financial system. This requires urgent action. Due to the long-term sensitivity of financial data, vulnerable cryptography must be replaced by new, quantum-safe solutions well before quantum computers reach maturity.

This paper provides a framework to support public and private financial institutions – particularly central banks – in the transition to quantum-safe cryptographic infrastructures. It shows that quantum-safe algorithms are not simple drop-in replacements for existing algorithms and a systemic approach is necessary to perform the transition. A strategic, pragmatic roadmap – from raising awareness, through planning, to executing cryptographic migration – has been outlined.

While the transition to quantum-readiness requires significant effort, this paper argues that it is also an opportunity to build more resilient infrastructures and systems. It recommends embedding principles of security by design, cryptographic agility and defence in depth, to better address unforeseen threats. Enhanced security for financial transactions and data will help safeguard trust in the financial system.

Central banks, as pivotal entities in the global financial system, are well positioned to support and lead the way to increased resilience. With their long-term perspective, central banks can promote a proactive, systemic approach and help create the alignment necessary for coordinated action across the global financial system to ensure the continued security and integrity of financial data. The time to act is now.

# Glossary of terms

## B

**Blind quantum computing (BQC)**: a cryptographic protocol that allows a client to delegate quantum computations to a server while keeping the input, process and results completely private.

## C

**Cryptographic agility**: the ability to adapt and switch cryptographic algorithms seamlessly and efficiently. It ensures that organisations can remain ahead of cryptographic vulnerabilities and embrace emerging cryptographic standards, keeping data secure even in the face of quantum computing advancements or other breakthroughs in algorithmic attacks.

**Cryptographically relevant quantum computer (CRQC)**: a quantum computer powerful enough to break widely used cryptographic systems, such as those based on Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC).

**Cryptographic defence in depth**: the concept of applying cryptographic mechanisms from different origins at different layers in the cryptographic infrastructure. Through this diversity, if one mechanism is compromised, additional layers continue to protect the bank's information.

## G

**General Data Protection Regulation (GDPR)**: a comprehensive European data protection law relating to data privacy and protection for individuals.

## H

**Harvest now, decrypt later (HNDL)**: a cyber security threat model in which malicious actors collect encrypted data today with the intention of decrypting it in the future, once more advanced technologies become available.

## P

**Post-quantum cryptography (PQC)**: a branch of cryptography focused on developing cryptographic algorithms that are secure against attacks from both classical and quantum computers.

**Pre-shared keys (PSK)**: a secret that is shared in advance between parties to establish secure communication.

## Q

**Quantum homomorphic encryption (QHE)**: a cryptographic technique enabling quantum computations to be performed on encrypted data without decrypting them. The results of the computation remain encrypted and can only be decrypted by the data owner.

**Quantum key distribution (QKD)**: a secure communication method that uses quantum mechanics to generate and share secret keys, ensuring data confidentiality by detecting any eavesdropping attempts.

## R

**Resilience of a cryptographic infrastructure**: building resilience into the cryptographic infrastructure allows the organisation to quickly recover and adapt its use of cryptography in response to disruptions or attacks. This capability ensures continuity and security in the face of rapidly evolving threats.

# References

Auer, R, A Dupont, L Gambacorta, J S Park, K Takahashi and A Valko (2024): "Quantum computing and the financial system: opportunities and risks", *BIS Papers*, no 149, October.

Bank for International Settlements (BIS) (2023): *Project Leap: quantum-proofing the financial system*, BIS Innovation Hub Eurosystem Centre, June.

Bank of France (2022): *The Banque de France has successfully experimented with Cryptonext Security post-quantum security technologies*, press release, 14 September.

Bank of France and MAS (2024): *Banque de France and Monetary Authority of Singapore conduct groundbreaking Post-quantum Cryptography experiment to enhance communication security*, press release, 5 November.

BIS Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (CPMI-IOSCO) (2016): *Guidance on cyber resilience for financial market infrastructures*, June.

Board of Governors of the Federal Reserve (2023): *Cyber and financial system resilience report,* July.

Bucciol, E and P Tiberi (2023): "Quantum safe payment systems", *Bank of Italy Markets, Infrastructures, Payment Systems*, no 35, June.

Canadian Centre for Cyber Security (CCCS) (2025): "Preparing your organization for the quantum threat to cryptography", *Awareness Series*, February.

Canadian Forum for Digital Infrastructure Resilience (CFDIR) (2024: *Canadian national quantum-readiness: best practices and guidelines*, July.

Doerr, S, L Gambacorta, T Leach, B Legros and D Whyte (2022): "Cyber risk in central banking", *BIS Working Paper*, no 1039, September.

European Payments Council (2025): "Guidelines on cryptographic algorithms usage and key management", EPC342-8, March.

European Telecommunications Standards Institute (ETSI) (2015): "Quantum safe cryptography and security", *ETSI White Paper*, no 8, June.

——— (2024): Quantum key distribution (QKD), common criteria protection profile – pair of prepare and measure quantum key distribution modules, *Group Specification*, no 16, April.

European Union (EU) (2024): *Commission recommendation (EU) on a coordinated implementation roadmap for the transition to post-quantum cryptography*, 2024/1101, 11 April.

Federal Office for Information Security (BSI) (2020): *Migration to post quantum cryptography*, August.

Financial Conduct Authority and World Economic Forum (2024): *Quantum security for the financial sector: informing global regulatory approaches*, white paper, January.

French Cybersecurity Agency (ANSSI) (2023): *ANSSI views on the post-quantum cryptography transition*, December.

French Cybersecurity Agency (ANSSI), BSI, Netherlands National Communications Security Agency and Swedish National Communications Security Authority, Swedish Armed Forces (2024): *Position paper on quantum key distribution*, January.

FS-ISAC (2024): *Building Cryptographic Agility in the Financial Sector*, Financial Services Information Sharing and Analysis Center.

Global Risk Institute (2024): *Quantum threat timeline report*, December.

Government of Canada (2022): *Canada's National Quantum Strategy*, Innovation, Science and Economic Development Canada, Ottawa.Grover, L (1996): "A fast quantum mechanical algorithm for database search", proceedings of the twenty-eighth annual ACM symposium on theory of computing, Philadelphia, pp 212–19.

G7 Cyber Expert Group (2024): *Statement on planning for the opportunities and risks of quantum computing*, September.

Hellman, M (1978): "An overview of public key cryptography", *IEEE Communications Society Magazine*, vol 16, no 6, November.

Hellman, E, B Diffie and R Merkle (1980): "Cryptographic apparatus and method", Patent US4200770A, 29 April.

HSBC (2023): *HSBC becomes first bank to join the UK's pioneering commercial quantum secure metro network*, media release, July.

International Monetary Fund (IMF) (2021): "The global cyber threat", *Finance and Development*, March.

Internet Engineering Task Force (IETF) (2021): *Hybrid post-quantum key encapsulation methods (PQ KEM) for transport layer security 1.2 (TLS)*, February.

——— (2024): *PQC in X509 interoperability project,* November.

——— (2025): *Hybrid key exchange in TLS 1.3: active internet-draft,* March.

JPMorgan Chase (2024): *Firm establishes quantum-secured crypto-agile network*, media release, May.

Monetary Authority of Singapore (2024): *Advisory on addressing the cybersecurity risks associated with quantum*, MAS Circular No. MAS/TCRS/2024/01, February.

National Cyber Security Centre (NCSC) (2020): "Preparing for quantum-safe cryptography", *NCSC White Paper*, November.

National Institute for Standards and Technology (NIST) (2016): *Post-quantum cryptography: call for proposals*.

——— (2022): *NIST Retires SHA-1 Cryptographic Algorithm*, December.

——— (2024a): FIPS 203: module-lattice-based key-encapsulation mechanism standard, August.

——— (2024b): FIPS 204: module-lattice-based digital signature standard, August.

——— (2024c): FIPS 205: stateless hash-based digital signature standard*,* August.

——— (2024d): "Transition to post-quantum cryptography standards", NIST IR 8547, November.

National Security Agency (NSA) (2022): *Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex*, Version 2.1, May.

——— (2023): *Quantum-readiness: migration to post-quantum cryptography*, August.

——— (2024): *The commercial national security algorithm suite 2.0 and quantum computing FAQ*, December.

——— (undated): Quantum key distribution (QKD) and quantum cryptography (QC).

Prenio, J and F Restoy (2022): "Safeguarding operational resilience: the macroprudential perspective", *FSI Briefs*, no 17, August.

Shor, P. W. (1994): *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), Santa Fe, NM, 20–22 November, IEEE Computer Society Press.

UK Government (2024): *The Science and Innovation Network Denmark supports a strong UK-Denmark quantum relationship*, British Embassy Copenhagen, December.