Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 05/2026

Quantum computing

9 July 2026

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Contents

1 Introduction

At the end of 2025, the Swiss Financial Market Supervisory Authority FINMA conducted a survey of 60 Swiss financial institutions on the opportunities and risks of quantum computing (QC). The institutions are aware of the cyber risks posed by cryptographically relevant quantum computers. In most cases, however, there is a lack of a clear roadmap and sufficiently forward-looking planning for the migration to quantum-safe encryption.

In financial market law, the technology-neutral, principles-based regulatory requirements for effective governance and risk management also cover the risks arising from the emergence of powerful quantum computers. Consistent with international norms, FINMA expects supervised institutions to address these risks in a timely manner and to align their governance and risk management accordingly.

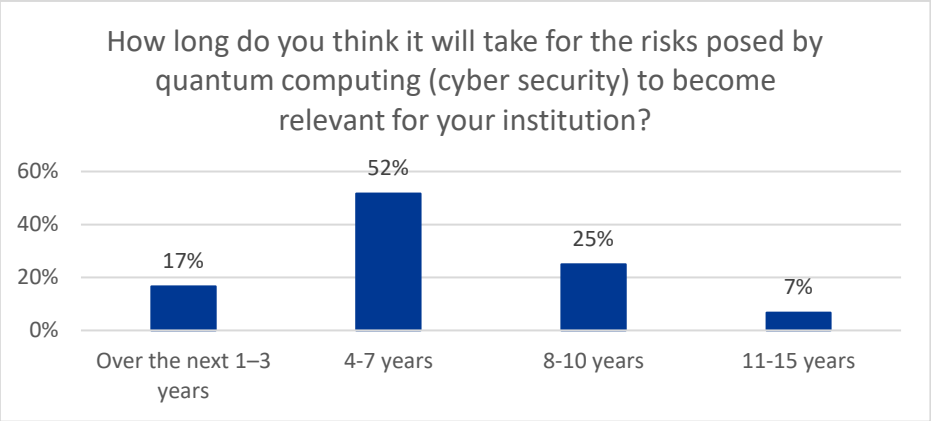
Based on its supervisory activities, FINMA concludes that further developing risk management would be advisable for many institutions in order to ensure ongoing compliance with the requirements relating to operational risks and resilience.

2 Survey results

Between November 2025 and January 2026, FINMA surveyed a total of 60 authorised banks, insurance companies, managers of collective assets and financial market infrastructures on the opportunities and risks of QC. The survey results show that Swiss financial institutions are generally aware of the cyber risks posed by quantum computers, particularly the potential vulnerability of encryption technologies, but that most are still in the early stages of the transition to quantum-safe encryption.

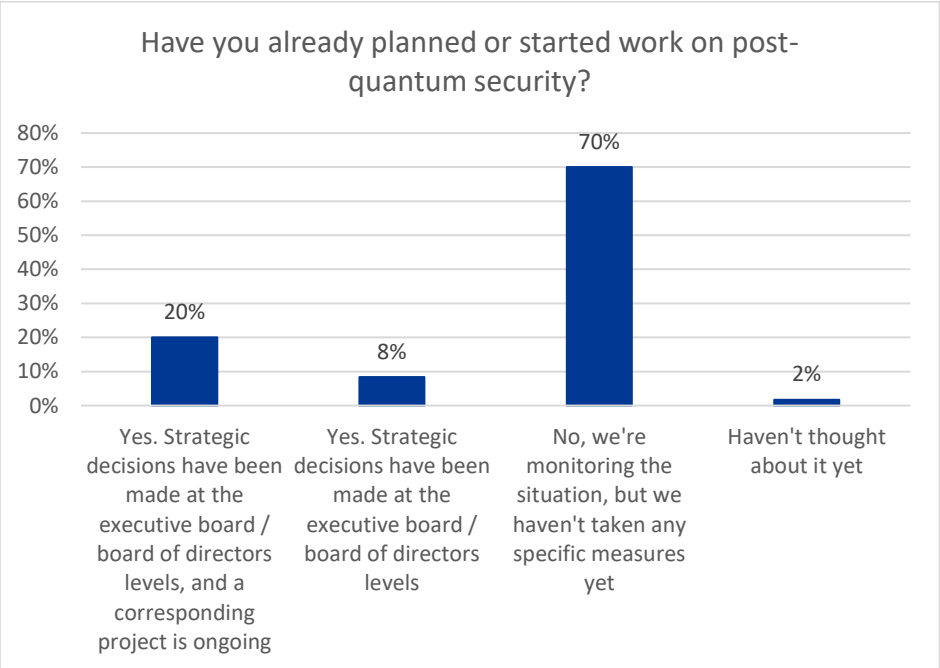
Institutions are aware of the cyber risks posed by QC

Around two-thirds of the institutions surveyed by FINMA expect to be directly affected by the cyber risks posed by quantum computing within seven years. Similarly, around two-thirds expect that, within ten years at the latest, a quantum computer will be able to crack RSA 2048-bit encryption within 24 hours. Accordingly, the institutions surveyed see the greatest risk posed by quantum computers for data security. Further significant risks are seen in the incomplete migration to quantum-safe encryption, a lack of expertise, “harvest now, decrypt later” attacks, and interoperability with legacy systems.



Only a few organisations have a roadmap for quantum-safe encryption

Of the organisations surveyed, 72% stated that they had not yet planned or implemented any measures relating to quantum-safe encryption. 28% have taken a strategic decision in this regard, whilst 20% also have an ongoing project relating to it.



Only 8% of respondents have a specific roadmap for quantum-safe encryption. They usually foresee a timeline of four to five years until critical data and processes are expected to be quantum-safe. Around half of the institutions surveyed plan to draw up a roadmap over the next one to three years, whilst 43% have not yet made any decisions in this regard.

Crypto-agility, inventory and external partners are important

There is a consensus among respondents on the importance of two factors in the transition to post-quantum cryptography (PQC): On the one hand, crypto-agility – that is, the ability of IT systems to replace encryption algorithms quickly and flexibly – is widely regarded as important or very important (73%). On the other hand, compiling an inventory of the cryptographic methods used is also seen as providing high or very high added value (76%). The majority of institutions have not yet decided whether they wish to use third-party services for the PQC migration work. However, external partners and software suppliers play a central role in any case, as cyber risks are also a significant concern at these third parties and at the interfaces with them. Of those surveyed, 60% are therefore already in contact with software suppliers or plan to be.

Two-thirds expect QC to be used in their company in 8+ years' time

The institutions surveyed see the greatest business value of quantum computers in risk and portfolio analysis, as well as in transaction monitoring, algorithmic trading and the generation of better random numbers. However, many organisations consider the current level of maturity of most applications in their sector to still be at the research or early development stage. The third of respondents who have already given some thought to the use of quantum computers in their company see access to expertise and skilled staff, as well as the availability of reliable hardware, as the most important prerequisites. Almost two-thirds of those surveyed do not expect to start using QC applications themselves for another eight years or more.

Conclusions from the survey

Overall, the survey shows that whilst many supervised institutions recognise the future risks posed by QC, concrete measures to address these risks are only being taken in isolated cases. In this context, FINMA highlights the technical advances in research, the lengthy duration of migration projects, and the considerable uncertainties regarding the time remaining until the development of cryptographically relevant quantum computers.

3 Recommendations

The following recommendations are based on FINMA's supervisory activities. FINMA brings these to the attention of the supervised institutions concerned and recommends that they be taken into account in their internal risk management.

The recommendations are limited to the transition to quantum-safe algorithms[1] and do not address the use of quantum key distribution (QKD) or issues that may arise from quantum computing applications.

3.1 Strategy and roadmap

As a basis for the transition to quantum-safe encryption, FINMA recommends that the work be based on a strategy adopted by the board of directors, from which an implementation plan setting out milestones and priorities is derived. In particular, it is advisable to set target dates for the complete migration, as well as for the migration of critical business processes, to quantum-safe cryptography. FINMA recommends that a PQC roadmap be drawn up by mid-2027 at the latest.

The PQC strategy can form part of an existing strategy (e.g. on cyber risks).

3.2 Risk analysis and inventory

From FINMA's perspective, the first step in the transition to quantum-safe encryption is a risk analysis – on the one hand, with regard to the cryptographic methods used, and on the other, with regard to critical data that requires long-term protection.

FINMA therefore recommends analysing all business processes in detail to identify the encryption, signature and authentication technologies used. In FINMA's view, this analysis should take into account all information and communication technology systems (ICT systems), applications, infrastructure and new technologies such as distributed ledger technology (see Art. 973d para. 2 let. 2 Code of Obligations [SR 220]), regardless of whether these are operated in-house, outsourced or procured as a service.

From FINMA's perspective, such an analysis of business processes will result in a comprehensive inventory listing all the cryptographic methods used. This includes the encryption of data during transmission (e.g. VPN, TLS, HTTPS, etc.) as well as stored data; it also covers the use of digital signatures, key management and the authentication mechanisms employed. Furthermore, such an inventory makes it clear whether the algorithms used are quantum-vulnerable[2] and need to be replaced accordingly. For systems with such algorithms, FINMA considers it appropriate to draw up a migration plan commensurate with the associated risk. A cryptographic inventory that is continuously updated to reflect the current situation contributes to the effectiveness of these measures.

[1] ML-EM, NIST, FIPS 203, https://csrc.nist.gov/pubs/fips/203/final; ML-DAS, NIST, FIPS 204, https://csrc.nist.gov/pubs/fips/204/final; SLH-DAS, NIST, FIPS 205, https://csrc.nist.gov/pubs/fips/205/final.

[2] For example, RSA, ECDSA, EdDSA, DH, EC-DH.

3.3 Critical data

As part of the risk analysis, it is advisable to identify and analyse the protection requirements for critical data. In particular, consideration should be given to whether long-term security guarantees regarding confidentiality and integrity (or non-repudiation, e.g. in the case of electronic signatures) need to be ensured. FINMA recommends taking into account the risk of "harvest now, decrypt later" attacks – that is, where data that is encrypted today may be stolen with the intention of decrypting it at a later date using powerful quantum computers. Data that needs to remain protected in the long term should be given priority and protected accordingly using PQC algorithms.

As there is as yet no long-term experience with PQC algorithms, various organisations[3] recommend a hybrid solution over pure PQC algorithms in the short to medium term. This involves combining a traditional algorithm with a PQC algorithm, which further enhances security and guarantees security even if one of the two algorithms used turns out to be insecure. Hybrid encryption is frequently cited, in particular, as a means of protecting critical data against "harvest now, decrypt later" risks. However, this approach also leads to increased complexity, which entails implementation risks. The internal risk analysis may also indicate the need to use hybrid solutions during system migration.

3.4 Crypto-agility

It must be anticipated that even in the future, (PQC) algorithms currently regarded as secure will need to be replaced. For example, certain PQC algorithms might, unexpectedly, prove ineffective.

Crypto-agility describes the ability of an ICT system or application to flexibly swap out cryptographic algorithms. This goes beyond a migration to PQC algorithms and affects all the algorithms used. Crypto-agility is therefore recommended as a requirement for ICT systems and applications to be procured or developed. This ensures that ICT systems can be adapted to new encryption algorithms flexibly and without requiring major changes to the software architecture.

3.5 External service providers

In the case of both the outsourcing of functions and external communication interfaces, PQC migration generally entails dependencies on external service providers. These service providers must also switch to quantum-safe

[3] "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography. A joint statement from partners from 21 European states," 2025, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3.

cryptography in their systems in order to continue to guarantee the necessary level of security when powerful quantum computers become available. In order to plan and implement this change properly and cost-effectively, it usually makes sense to integrate it into regular release cycles. This requires longer-term planning in collaboration with the external service provider to address new requirements.

Responsibility for the outsourced function lies in all cases with the outsourcing institution (see FINMA Circular 2018/3 “Outsourcing” for further details). Future risks – such as those posed by powerful quantum computers – can also be anticipated today, and measures can be set out contractually with service providers.

It is recommended that crypto-agility[4] be made a prerequisite for all new outsourcing arrangements in the software and data sectors, and that, in the case of existing outsourcing arrangements, this be incorporated into the requirements at the earliest opportunity.

4 Outlook

Cryptographically relevant quantum computers do not yet exist. However, technological progress has gained momentum, and such computers can be expected to emerge in the coming years. Appropriate risk management is therefore required to address the cyber risks posed by quantum computers.

In view of the emerging risks posed by quantum computers, FINMA encourages early engagement with and mitigation of these risks – particularly given the complexity and time required for the migration to quantum-safe encryption technologies, the interdependencies between service providers and financial institutions, and the already very real risk of “harvest now, decrypt later” attacks.

FINMA will continue to actively monitor developments in the field of QC and will give greater prominence to this topic in its ongoing supervisory activities.

[4] The ability of IT systems to replace their cryptographic algorithms flexibly and without making major changes to the software architecture.