

FINMA & QUANTUM COMPUTING – FLASH

The New FINMA Supervisory Notice 05/2026 on Quantum Computing and Its Implications for Swiss Financial Institutions

2026 · QUANTUM COMPUTING AND POST-QUANTUM CRYPTOGRAPHY FLASH · APPROX. 12 MIN. READ · DR. IUR.
DIRK SPACEK

1. Background

On 9 July 2026, the Swiss Financial Market Supervisory Authority FINMA published Supervisory Notice 05/2026 on the topic of quantum computing. It summarises the results of a survey conducted between November 2025 and January 2026 among 60 Swiss financial institutions – licensed banks, insurance undertakings, managers of collective assets and financial market infrastructures – and derives supervisory expectations from the findings. The focus is not on the future productive use of quantum computers themselves, but on their foreseeable ability to break the cryptography that is widely used in the financial sector today. A complete migration to quantum-safe methods will therefore become necessary, and given heterogeneous, historically grown IT landscapes (legacy IT), such a migration can take several years. This is where a time-related risk factor lies: whoever waits to react until powerful quantum computers are available is unlikely to complete the necessary transformation in time.

2. What Is Quantum Computing – and Why Does It Concern Financial Institutions?

Quantum computing refers to a form of information processing based on quantum mechanics. While classical computers calculate in binary, using bits (0 or 1), quantum computers work with so-called qubits, which exist in a state of **superposition** of both states at once, i.e. a qubit can simultaneously be a little bit «0» and a little bit «1», like a coin still spinning in the air before it lands. Qubits can also be **entangled with one another**, meaning that the outcome of one qubit is instantly linked to the state of another, no matter how far apart they are. As a result, many qubits together can process far more information than the same number of separate bits. In a financial services context, this makes it possible to solve certain calculations – in particular combinatorial optimisation problems, simulations and number-theoretic problems – more efficiently than with classical computer programs.

For the financial sector, this gives rise to two very different dimensions. On the **opportunity side**, considerable economic benefit is expected, in particular in *risk management* (faster and more precise simulation of complex dependencies between assets, and Value-at-Risk and stress-test calculations), in *portfolio optimisation* (better allocation assessments across different asset classes), in *derivatives valuation* as well as in *fraud detection* and trading. Large international banks and the domestic Swiss banking sector (among others, according to the expert report of the

Swiss Bankers Association) are therefore already investing in quantum-computing pilot projects today, even though broad productive use is mostly expected only in the 2030s.

On the **risk side**, cryptography is the focus: widely used asymmetric encryption methods with two keys, such as RSA, ECDSA, EdDSA or (EC) Diffie-Hellman, rely on mathematical computational problems that are easy to solve in one direction but hard to solve in the other. The public key, for instance, contains a huge number (the result of a multiplication). Anyone wishing to decrypt it without knowing the private key – i.e. the original multiplication factors – would have to work backwards and factor this huge number into its two original factors. That is practically impossible unless one has far greater computing power. This is where quantum computers can become dangerous: thanks to superposition and entanglement (see above), a quantum computer can solve exactly this kind of reverse calculation far faster than a normal computer. This could compromise encryption, digital signatures and authentication – the foundation of online banking, payment systems, TLS/HTTPS connections, electronic signatures and also of crypto-assets. This is, in essence, a well-known pattern: technical advances/innovations always bring new risks with them. Particularly acute is the risk of so-called «*harvest now, decrypt later*» attacks through quantum computing: data encrypted today can already be intercepted and stored so that it can be decrypted at a later point in time using future quantum computing power – a risk that is already real today, even though a sufficiently powerful quantum computer does not yet exist in ideal form.

3. Key Points of FINMA Supervisory Notice 05/2026

Legally, the notice is not based on a new legal foundation but on the existing, technology-neutral and principles-based requirements for governance and risk management relating to operational risks and resilience. These principles are already set out, by analogy, in FINMA Circular 2023/1 – Operational Risks and Resilience – Banks, in FINMA Circular 2018/3 – Outsourcing – Banks and Insurers, and in FINMA Supervisory Notice 08/2024 – Governance and Risk Management in the Use of Artificial Intelligence.

In its new supervisory notice, FINMA states that governance and risk management requirements must also cover the risks arising from quantum computing. It sets out recommendations for consideration in internal risk management. However, the recommendations are limited primarily to the migration to quantum-safe algorithms (post-quantum cryptography, «**PQC**», see further detail below). FINMA does not comment on the topic of Quantum Key Distribution – i.e. the specific use of quantum computing to exchange a secret key between two parties – or on questions relating to the productive use of quantum computer applications.

The survey underlying the notice shows that, while institutions are aware of the risks – around two thirds expect to be directly affected within seven years, and just as many consider it plausible that, for example, RSA-2048 encryption – a method based on a huge number formed by multiplying two secret prime numbers – could be broken within 24 hours within the next ten years. Concrete measures, however, have so far only been taken by a few: 72% of institutions have neither planned nor implemented any measures, and only 8% already have a concrete roadmap. From this, FINMA diagnoses an industry-wide need to catch up.

FINMA's Five Recommendation Blocks

- **Strategy and Roadmap:** FINMA suggests that work should be based on a strategy adopted by the ultimate management body (board of directors), including an implementation plan, milestones and target dates – with **a roadmap for the PQC migration by mid-2027 at the latest**. This strategy can be part of an existing cyber-risk mitigation strategy. PQC migration is understood to mean migrating existing cryptographic methods – i.e. wherever RSA or ECDSA are used today, for example in digital signatures or in the transmission of data over TLS/HTTPS connections – to new quantum-safe encryption methods that are not based on the kind of mathematical problems a quantum computer could solve efficiently using, for example, the Shor algorithm (prime factorisation). **PQC encryption schemes** are based on other problem-solving approaches, such as **lattice-based cryptography** (multi-dimensional point grids in hundreds of dimensions based on vector calculations; here, encryption relies on a “good” and a “bad” description that only match up together). The US authority NIST already officially standardised three such methods in 2024:
 - ML-KEM (FIPS 203) for key exchange and encryption;
 - ML-DSA (FIPS 204) for digital signatures;
 - SLH-DSA (FIPS 205) – also for signatures, in case lattice-based methods later prove vulnerable after all.
- **Risk Analysis and Inventory:** The basis is formed by a **risk analysis of all business processes** with regard to the encryption, signature and authentication technologies used (including outsourced and externally sourced services, as well as novel technologies such as distributed electronic registers). This results in a **continuously maintained cryptographic inventory**, showing which algorithms are vulnerable to quantum computers (e.g. RSA, ECDSA, EdDSA, DH, EC-DH) and need to be replaced.
- **Data Requiring Protection:** Data requiring long-term protection must be identified as a priority and protected against «*harvest now, decrypt later*» attacks. Given the lack of long-term experience with PQC algorithms, the use of hybrid solutions combining classical and PQC algorithms is recommended for the time being.
- **Crypto-Agility:** As future PQC methods may also need to be replaced, FINMA recommends crypto-agility – the ability to exchange and renew cryptographic algorithms without profound architectural changes – as a binding requirement for new ICT systems and applications.

External Service Providers: Responsibility for outsourced functions remains with the institution under FINMA Circular 2018/3 «Outsourcing». **Crypto-agility** should be required for new outsourcing relationships in the software and data domain and should be requested promptly for existing **contracts with IT providers**, ideally embedded in regular release cycles.

4. Assessment and Need for Action

Even though cryptographically relevant quantum computers do not yet exist today, FINMA emphasises that technological development is accelerating and that considerable uncertainty remains as to the timing of their emergence. Legally, **PQC migration** is therefore not an isolated IT project but an **institution-wide task**, affecting governance, compliance, risk management, information security, procurement and third-party management alike, and requiring corresponding documentation vis-à-vis the board of directors and the supervisory authority. FINMA also announces that it will actively continue to monitor the topic and increasingly incorporate it into its ongoing supervisory activities – a **review in the context of future supervisory meetings and examination reports** is therefore **to be expected**.

Key Takeaway for Practice: For practice, this gives rise to short-term priority steps for financial institutions: 1) initiating or documenting a strategic decision at management/board level on a PQC roadmap, 2) building a cryptographic inventory, 3) identifying data requiring long-term protection, and 4) contractually securing crypto-agility vis-à-vis service providers. Since the deadline for a PQC roadmap («by mid-2027 at the latest») is not far off, and the migration itself could take several years, an early start is advisable. A *combined involvement of IT/encryption experts, governance specialists and IT compliance legal specialists* is therefore recommended.

This short publication is for general information purposes only and does not replace legal advice in an individual case.

Dirk Spacek, Dr. iur., LL.M. is a lawyer and partner in Zurich. He advises companies on all contract and commercial law matters, with a particular focus on issues at the intersection of technology, intellectual property and data/cyber law.