swiss financial
innovation desk

Action Plan to a Quantum-Safe Financial Future

A Pathway 2035 Deep-Dive

March 2025

Table of Contents

Executive Summary

Switzerland follows a principle-based and technology-neutral approach to financial regulation. While no specific legal mandate requires financial institutions to be quantum-safe, regulators such as FINMA expect proactive risk management. The Swiss Financial Innovation Desk (FIND) has taken an initiative to assess the urgency and implications of quantum-related risks for the financial sector. This includes expert consultations, publications and a fact-finding mission in March 2025.

Key Findings

a. **Quantum Threat Acceleration**

The risk of quantum computing attacks is real and increasing, with potential breakthroughs predicted as early as 2028. Asymmetric encryption methods like RSA and ECC are particularly vulnerable, while global efforts (e.g., NIST standards, EU initiatives) are accelerating the transition to post-quantum cryptography (PQC). The "Harvest Now, Decrypt Later" strategy poses an immediate risk.

b. **Regulatory Landscape**
Switzerland currently lacks a dedicated quantum-safe framework. FINMA requires financial institutions to manage technological risks independently, but there is no coordinated national action plan.

c. **Urgent Need for Action**
FIND emphasizes that Switzerland's financial sector must act swiftly to safeguard its reputation as a trusted global financial hub. Collaboration with industry associations (SBA, SIA, FC-CSC) and government entities (NCSC) is critical.

Implement a Seven-Step Action Plan.

- Establish quantum risk governance
- Assess affected business and technology components
- Minimize new legacy systems through quantum-safe procurement
- Address immediate "Harvest Now, Decrypt Later" risks
- Implement a migration plan to quantum-safe cryptography
- Align with industry standards and regulatory guidance
- Continuously review and adapt quantum strategies

By implementing this Action Plan, Switzerland's financial ecosystem can not only mitigate quantum risks but also position itself as a global leader in quantum-safe financial services.

1 Introduction

Switzerland is known for its principle-based and technology neutral policy making, there is no explicit law requiring financial service providers to be quantum-safe. The supervisory authority FINMA expects its licensees (such as banks or insurers) to identify and manage operational risks on a continuous basis and to proactively react to technological risks and implement appropriate measures to address them. So, what does that mean for a bank or an insurance company? What has to be done?

As an innovation concierge, the **Swiss Financial Innovation Desk (FIND)** fosters financial innovation and supports the ecosystem in finding helpful answers through community building, analyzing and outlining options to overcome blockers. It has offered non-binding guidance on whether and how the ecosystem should become quantum-safe by conducting research, interviewing subject matter experts, publishing the collaborative report Pathway 2035 for Financial Innovation – Your Navigator and organizing a fact-finding mission on 4 March 2025, with 22 financial ecosystem representatives to expand its findings.

The following overview outlines FIND's validation efforts with an Action Plan made on a voluntary, best-effort basis. Given the rapid pace of technological advancements, the Action Plan is time sensitive. While FIND acknowledges the potential for quantum technology for the financial sector, this report focuses primarily on addressing quantum-related risks, rather than exploring its opportunities.

2 FIND's Key Insights

The **risk of a quantum computing attack is not a hypothesis, but real**. Emerging research and industry reports indicate that the timeline for quantum computing threats is accelerating, with predictions shifting from the 2030s to as early as 2028, heightening concerns about potential risks to cryptographic systems occurring sooner than anticipated.[1] As already mentioned in our Pathway 2035 for Financial Innovation – Your Navigator, it is not a question of if but when[2]. In light of expanded expertise scope, our earlier report (see Thesis 5.2 in the Quantum-Safe chapter) requires clarification: **asymmetric cryptography is more significantly impacted than symmetric cryptography**. Particularly at risk are asymmetric encryption methods such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which are widely used for secure communication today.

---

1 See https://www.infosecurity-magazine.com/news/europol-warns-financial-sector/

2 See https://find-swiss.cdn.prismic.io/find-swiss/Z5jdBZbqstJ99779_Pathway-2035-for-Financial-Innovation-Your-Navigator.v1.0.2.pdf

Moreover, to clarify Chapter 5.3 of the mentioned report, it is important to note that key authorities and standardization bodies in Switzerland and abroad emphasize significant differences in their recommendations regarding the broader adoption of **PQC** (Post-Quantum Cryptography) as a concept versus **QKD** (Quantum Key Distribution) as a specific approach. While PQC algorithms are generally recommended for all areas where public-key cryptography is currently used, QKD, as a specific technology, is not widely endorsed at this stage and is often limited to niche applications. We advise conducting a thorough analysis of the scope and functionality of cryptographic technologies before deciding on their broader implementation.[3]

However, the threat already exists today: attackers can intercept encrypted data now and decrypt it in the future using quantum computers – a pattern known as "**Harvest Now, Decrypt Later**".

In the United States, **Quantum Computing Cybersecurity Preparedness Act** was signed into law in December 2022. It remains in effect to date, despite change of administration leadership. This law requires federal agencies to conduct an inventory and prioritization of vulnerable IT systems and develop a plan to migrate to post-quantum cryptography. The National Institute of Standards and Technology (NIST) has been further tasked with developing standards for post-quantum cryptography (PQC). Over the last two years, NIST has published four official standards[4], one other is expected to become officially recognized in due course subject to all formalities being completed:

a **ML-KEM**[5] (aka FIPS 203 aka **CRYSTALS-Kyber)**, intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily as well as its speed of operation.
b **ML-DSA**[6] (aka FIPS 204 aka **CRYSTALS-Dilithium)**, intended as the primary standard for protecting digital signatures.

[3] See https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/technologiebetrachtungen/Technologiebetrachtung-QCPQC-DE.pdf.download.pdf/Technologiebetrachtung-QCPQC-DE.pdf; https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20244398; https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf; https://cyber.gouv.fr/actualites/la-distribution-quantique-de-cle-son-utilisation-et-ses-limites; https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[4] See https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[5] Short for Module-Lattice-Based Key-Encapsulation Mechanism.

[6] Short for Module-Lattice-Based Digital Signature Algorithm.

c **SLH-DSA**[7] (aka FIPS 205 aka **SPHINCS+**), also designed for digital signatures. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

d **Hamming Quasi-Cyclic (HQC)** is a code-based encryption algorithm selected by NIST on 11 March 2025 as PQC standard for key encapsulation mechanisms (KEM). It complements existing standardized algorithms, particularly ML-KEM (Kyber).

e **Falcon** (expected to become FIPS 206) is a post-quantum signature method that has been selected by NIST but has not yet been officially published as part of the first series of NIST standards.

The **EU Commission** has also vamped up: its Recommendation (EU) 2024/1101 of 11 April 2024[8] deals with the implementation of post-quantum cryptography. It suggests an action plan for the coordinated implementation of the transition to post-quantum cryptography in the EU within two years. It encourages its member states to develop a comprehensive strategy for the transition to post-quantum cryptography to ensure the security of digital infrastructure and services for public administrations and critical infrastructure. The commission emphasizes the need for coordinated implementation to ensure cross-border interoperability and mitigate quantum computing risks.

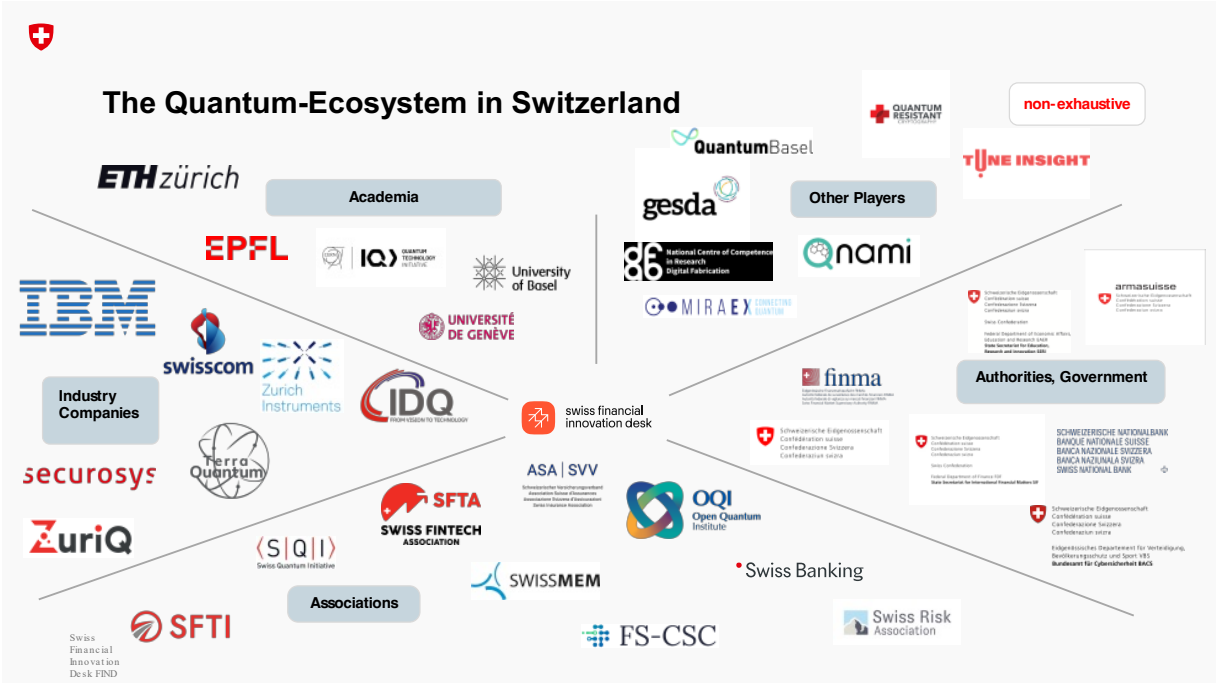
Regarding **Switzerland**, as previously noted, there is no explicit legislation mandating a quantum-safe action plan. In the financial sector specifically, FINMA relies on individual licensed financial institutions to proactively and appropriately manage technological risks. More broadly, the Federal Council has thus far responded to three interpellations on the subject, each with a slightly different focus and scope (see Annex for details on each interpellation).

While the Federal Council recognizes the significance of quantum-safe cryptography, an action plan has yet to take full shape. Switzerland has not yet defined specific timelines, roles or requirements. The roles of key institutions, such as the National Cyber Security Centre (NCSC), as well as public procurement policies (Federal Office of Information Technology, Systems and Telecommunication, FOITT), regulatory standards (Federal Chancellery, FCh, eGov) and major federal initiatives - including Swiss Government Cloud (SGC), e-ID and EPD - have received only limited consideration in this context. Defining these roles and requirements, as well as identifying potential gaps, is essential for determining where public-private collaboration is needed and where private-sector initiatives should take the lead.

However, the Quantum-ecosystem in Switzerland is rich and diverse. The following list is not exhaustive:

[7] Short for Stateless Hash-Based Digital Signature Algorithm.

[8] See https://eur-lex.europa.eu/eli/reco/2024/1101/oj/eng



FIND identifies a substantial opportunity within the quantum threat by linking it to the Swiss financial sector's rich history of reliability, quality, trust and confidentiality. Through the timely and determined implementation of a national action plan and the execution of a quantum and quantum safe strategy, the Swiss ecosystem could position itself as a leader, using it as a unique selling proposition. In parallel, the opportunities of quantum computing need to be further assessed and developed, as future excellence and leadership will be closely tied to achieving so-called **quantum supremacy**.

3 Act Swiftly by Implementing a Seven-Step Action Plan

The following seven-step Action Plan intends to provide a helpful high-level outline of potential measures.[9] In no way is it meant to be exhaustive or replace other or more specific recommendations by e.g., industry associations, industry practice groups or internal action plans by the financial institutions' own subject matter experts. Moreover, it does not substitute for a national action plan.

	What
1	Put quantum safe on the agenda and appoint and empower internal roles to drive and oversee further activities
2	Create an overview of affected business and technology components, processes and policies and determine interdependencies
3	Limit creation of new legacy, by establishing general Quantum Safe requirements for procurement and internal software development processes
4	Identify elements exposed to "Harvest now, decrypt later" and initiate mitigation actions

[9] See https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3

5	Implement a comprehensive migration plan to Quantum Safe, in alignment with internal change portfolios and supplier technology action plans and considering requirements such as crypto-agility and the buildup of a crypto-inventory
6	Collaborate with industry organizations and align with standardization bodies and regulatory guidance
7	Regularly review this action plan and adjust as necessary, equally review developments in quantum computing and quantum-safe cryptography

Responsibilities and decision-making authority within financial institutions vary across corporate governance and organizational units, depending on factors such as the articles of association, organizational regulations and internal policies.

The **first line of defense** should establish a process for identifying, managing and mitigating risks from quantum attacks - using the seven-step Action Plan as a starting point for more advanced approaches. The **second line of defense** should ensure that policies, procedures and controls are developed and that the first line conducts self-assessments for adequacy. The **third line of defense** should assess quantum-related risks and incorporate them into a risk-based internal audit plan to evaluate the completeness and effectiveness of controls.

4 Annexes

4.1 Interpellation M. Dobler "Use of Quantum-Safe/Quantum-Resistant Cryptography by the Federal Government"

The following interpellation of M. Dobler of 18 December 2024[10], member of the Swiss National Council, was answered by the Federal Council on 19 February 2025[11]:

"A year ago, the Federal Council commented on the interpellation 23.3689 regarding quantum-safe systems, as well as on 24.4215 in November 2024. However, this had a general Swiss reference. In relation to the federal government, the following specific questions now arise:

1. *What is the federal government's strategy for implementing/transitioning to quantum-safe cryptography for federal systems/critical infrastructures?*
2. *How are relevant data and systems (and their risk and cryptographic systems) identified?*
3. *Is special attention paid to the urgency of certain scenarios such as "Harvest Now/Decrypt Later"?*
4. *What specifications are made for systems and products of the federal government (including Swisspass) that are affected by the threat and require long-term conversion processes?*
5. *How will the migration of systems and products from the federal government and industry be prioritized? Will guidelines be created?*
6. *How will the federal government deal with new procurements that are rolled out in the coming years and are affected by the threat? Are appropriate specifications already being made to prepare the systems and prevent reimplementation? (Examples are Swiss Government Cloud or the E-ID trust infrastructure)*
7. *Who is responsible for the strategy/policy regarding quantum safe/quantum-safe cryptography at the federal government?*
8. *Who is responsible for the implementation and monitoring of quantum safe/quantum-safe cryptography at the federal government?*
9. *Why should the federal government focus on post-quantum cryptography or quantum key distribution standards?*

The breakthrough of powerful quantum computers is getting closer and closer, and so are the associated security problems. Today's encryption technology is therefore vulnerable. Until now, several years of computing power were needed to decode an encryption. With quantum computers, this will change abruptly

[10] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20244398

[11] Original text in German translated into tentative English.

and make existing encryption vulnerable. Criminals are already stealing encrypted data today in order to decrypt it one day using quantum technology.

Federal Council's Answer[12]

Regarding 1, 2 and 5) The cryptographic protection of information is a central element of information security. The level of protection required is determined by the ***classification*** *of the information in accordance with Art. 13 of the Information Security Act (ISA; SR 128). When information is processed using IT tools, the* ***need for protection*** *of the information must also be determined, which then results in the* ***technical and organizational security requirements*** *for these tools (Art. 16-19 ISA). These procedures are also used to determine the level of cryptographic protection required and form the basis for decisions on any prioritization in the implementation of quantum-safe solutions. In its response to Parliament's Interpellation 23.3689, the Federal Council set out the measures for encrypting information classified as SECRET.*

Regarding 3) With regard to the 'Harvest now/decrypt later' scenario, it should be noted that the federal government has never been of the opinion that cryptographic protection alone is sufficient to fully guarantee the security of classified information throughout its entire lifespan. Access to such information must be protected by further technical and organizational measures to prevent it from being stolen by unauthorized persons. It is therefore important that the protection requirements and the classification of the information are correctly recorded.

Regarding 4, 6, 7 and 8) As the Federal Council stated in its response to parliamentary question 24.4215, ***international standardization efforts in the area of quantum-safe cryptography are making progress*** *but have not yet reached the point where binding timetables, requirements or guidelines can be defined.*

Based on Art. 21 and Art. 29 of the Information Security Ordinance (SR 128.1), the federal government's information security unit in the State Secretariat for Security Policy can introduce such requirements. It draws on the expertise of the Federal Office for Cyber Security, the army's cryptology unit and the Cyber-Defence Campus of the Federal Office for Defence Procurement armasuisse. The departments ensure that the requirements of the specialist unit are implemented and verify this. The requirements specify the minimum level of protection that must be met during operation and procurement.

Regarding 9) The federal government's ***focus is on post-quantum cryptography****. Procedures that use quantum key distribution do not offer a practical solution, at least not in their current state of development, and are not recommended by most international specialist units."*

[12] Emaphasis added by the FIND team.

4.2 Interpellation N.S. Gugger "Progress in the Implementation of Quantum-Secure Systems in Switzerland"

The following interpellation of 27 September 2024 of Mr. N.S. Gugger[13], member of the Swiss National Council, was answered by the Federal Council on 20 November 2024[14]:

"One year ago, the Federal Council responded to Interpellation 23.3689 regarding quantum-safe systems within the federal administration. Given the global developments in this field, the following questions arise:

1. *What concrete steps has the Federal Council taken to establish clear guidelines and timelines for Swiss IT companies seeking the status of "trusted provider" in the field of quantum-safe algorithms?*

2. *To what extent has a strategy been developed to leverage Switzerland's expertise in cryptography (particularly from institutions such as IBM Rüschlikon) to strengthen national cybersecurity?*

3. *What measures have been taken to accelerate the development and implementation of new quantum-safe encryption standards in Switzerland? How does the Federal Council ensure that Switzerland keeps pace with global developments?*

4. *How does the Federal Council assess Switzerland's progress in the field of quantum technology in an international comparison, particularly in light of developments in the United States and China?*

The United States has already introduced clear regulations for IT companies wishing to retain their status as trusted providers, including deadlines for the adoption of new quantum-safe algorithms. China, on the other hand, has already established new quantum-safe encryption standards and considers quantum computing a key technology in its efforts to surpass the West technologically. Given these global developments, it is imperative that Switzerland intensifies its preparations for the quantum computing era. The Neue Zürcher Zeitung *(NZZ) reported extensively on this topic in August: https://epaper.nzz.ch/article/8/8/2024-08-04/25/329591009*

Federal Council's Answer[15]

1) There is no federally granted status of "trusted provider" in Switzerland. Consequently, the federal government cannot set specific requirements for obtaining such a designation.

[13] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20244215

[14] Original text in German translated into tentative English.

[15] Emphasis added by the FIND team.

2) The federal government regularly exchanges information with experts on cybersecurity issues, including specifically on quantum-resistant encryption. This cooperation is needs-based. However, no dedicated strategy has been developed for this purpose.

3) International standardization bodies have identified algorithms suitable for quantum-resistant encryption. In mid-August 2024, the U.S. National Institute of Standards and Technology (NIST) published three relevant standards (FIPS 203, FIPS 204, and FIPS 205) for the key encapsulation mechanism ML-KEM and the two signature schemes ML-DSA and SLH-DSA. However, further standardization efforts are necessary before binding guidelines and timelines can be introduced.
In parallel, authorities and companies must assess their own risks, evaluate their currently deployed encryption technologies, and determine where a transition to quantum-safe algorithms is necessary. The Federal Office for Cybersecurity helps raise awareness among companies and authorities and has issued technical recommendations on the topic. For in-depth analyses and the implementation of technical measures, a strong offering of private consulting services is available in Switzerland. Furthermore, international software providers are increasingly integrating quantum-safe solutions into their products, which will significantly drive the adoption of such technologies. The Federal Council sees no reason why Switzerland should not be able to keep pace with international developments and does not identify a need for additional federal measures.

4) In its response to Interpellation 23.3614 by Schneider-Schneiter, the Federal Council highlighted that Switzerland is well-positioned in the field of quantum technologies in international comparison, thanks to numerous initiatives at Swiss universities."

4.3 Interpellation J. Bellaiche "Quantum-Safe Systems in the Federal Government"

The following interpellation of Judith Bellaiche of 14 June 2023[16], member of the Swiss National Council, was answered by the Federal Council on 23 August 2023[17]):

"Research in quantum computing is currently making great strides. While it is not possible to predict when the breakthrough of powerful and stable quantum computers will occur, there is consensus about the new security problems associated with them. Certain encryption technology will be vulnerable to large-scale attacks by quantum computers, and it is suspected that criminals are already stealing encrypted data in order to decrypt it with quantum technology in the future (steal now, decrypt later). In this context, the Federal Council is asked to answer the following questions:

1. Has the Federal Council addressed the risks of quantum computing for the encrypted data of the administration and authorities, including the army, state-owned enterprises and system-critical institutions such as the SNB?

2. In which areas does the Federal Council identify a need for action in connection with this threat?

3. Is the Federal Council prepared to check the technologies, databases and systems currently in use for quantum-safe standards or to align them with them in principle?

4. In what time frame does the Federal Council plan to carry out this check or conversion?

Federal Council's Answer[18]

1./2. The Federal Council is aware of the risks posed by quantum computing, particularly for some cryptographic methods that are widely used today. The federal cryptology unit has defined internal security requirements and has been recommending for ten years that only methods that, according to current knowledge, provide sufficient protection against quantum computers be used to protect information classified as SECRET. Specifically, since 2014, newly procured encryption systems for the SECRET classification level have been based on symmetric methods with a key length of at least 256 bits. This minimizes the risk of highly sensitive information being recorded and later decrypted.

In view of the constant technological change in this area, the federal government is systematically monitoring developments and researching the cryptologically relevant issues. With the National Strategy for the Protection of Switzerland against Cyber-Risks (NCS) for the years 2018-2022, a monitoring system for the relevant technologies in the field of cyber security has been established. The monitoring is carried out by the Cyber-Defence Campus (CYD) of armasuisse Science and Technology in cooperation with the National Cybersecurity Centre (NCSC). The Cyber-Defence Campus will introduce monitoring specifically for the topic of quantum computing from fall 2023.

---

[16] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233689

[17] Original text in German translated into tentative English.

[18] Emphasis added by the FIND team.

In addition, the federal government is investigating the opportunities and risks of a switch to quantum computing as part of the Cyberspace research program at armasuisse Science and Technology, and is analyzing the feasibility and security of current and new encryption methods.

3./4. As mentioned, the Federal Council is closely monitoring developments. Since 2017, Swiss research institutes have been involved in the selection process conducted by the National Institute of Standards and Technology (NIST, USA) to standardize post-quantum cryptography. This selection process is expected to be completed in 2024. It can be assumed that the new standards will then be increasingly implemented in both industrial products and open-source solutions. The Federal Council will examine the extent to which these new solutions should also be used for information with lower classifications in order to ensure that this information is protected against attacks enabled by quantum computers."

5 Impressum

Publisher
Swiss Financial Innovation Desk (FIND)

Contact
info@find.swiss

The views expressed herein are those of the Swiss Financial Innovation Desk (FIND) and not necessarily those of the Swiss Federal Council, the Swiss Federal Department of Finance or the Swiss State Secretariat for International Finance. This publication is based on the best available data and insights at the time of writing. While every effort has been made to ensure accuracy, projections and analyses are subject to change as new information and developments arise. The publication may hence become outdated over time and there is no obligation to keep it updated.