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-Aufsichtsmitteilung 05/2026

Quantum Computing

9. Juli 2026

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

Inhaltsverzeichnis

1 Einleitung 3

2 Umfrageergebnisse 3

3 Empfehlungen 6

3.1 Strategie und Roadmap 6

3.2 Risikoanalyse und Inventar 6

3.3 Kritische Daten 7

3.4 Kryptoagilität 7

3.5 Externe Dienstleister 8

4 Ausblick 8

1 Einleitung

Die Eidgenössische Finanzmarktaufsicht FINMA hat Ende 2025 bei 60 Schweizer Finanzinstituten eine Umfrage zu den Chancen und Risiken von Quantum Computing (QC) durchgeführt. Die Institute sind sich der Cyberrisiken von kryptografisch relevanten Quantencomputern bewusst. Meist fehlt aber eine klare Roadmap und eine ausreichend vorausschauende Planung für die Migration zu quantensicherer Verschlüsselung.

Im Finanzmarktrecht erfassen die technologieneutralen, prinzipienbasierten aufsichtsrechtlichen Anforderungen an eine wirksame Governance und ein wirksames Risikomanagement auch die Risiken, welche sich aus dem Aufkommen leistungsfähiger Quantencomputer ergeben. Wie auch im internationalen Umfeld gefordert, erwartet die FINMA, dass sich die Beaufsichtigten mit diesen Risiken rechtzeitig auseinandersetzen und ihre Governance und ihr Risikomanagement entsprechend ausrichten.

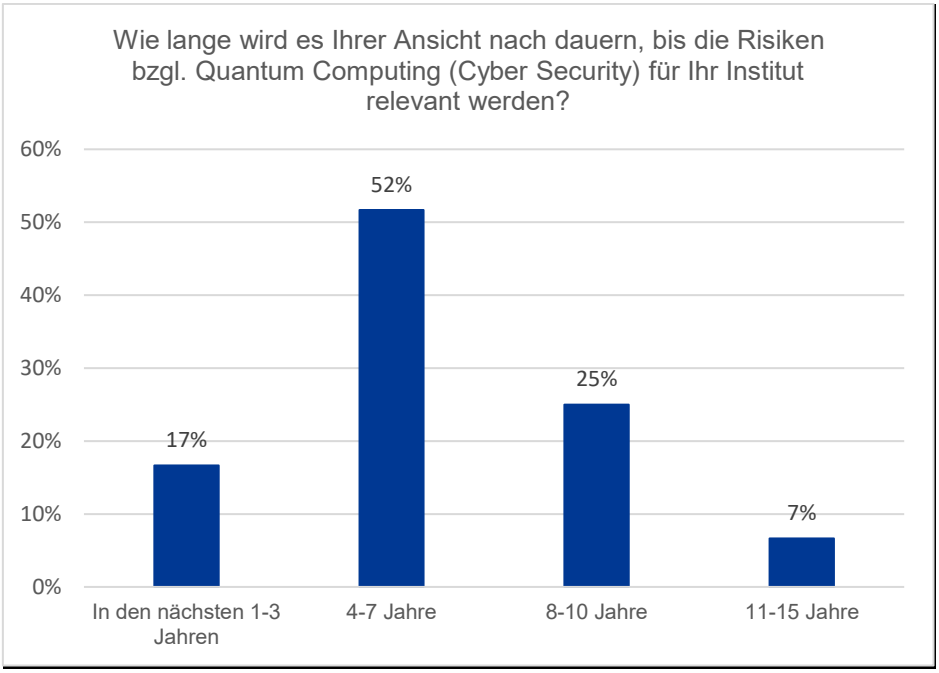
Aus ihrer Aufsichtstätigkeit leitet die FINMA ab, dass eine Weiterentwicklung des Risikomanagements für viele Institute sinnvoll wäre, um die laufende Erfüllung der Vorgaben zu operationellen Risiken und Resilienz abzusichern.

2 Umfrageergebnisse

Von November 2025 bis Januar 2026 befragte die FINMA 60 bewilligte Banken, Versicherungsunternehmen, Verwalter von Kollektivvermögen und Finanzmarktinfrastrukturen zu den Chancen und Risiken von QC. Die Umfrageergebnisse zeigen, dass Schweizer Finanzinstitute sich generell der Cyberrisiken von Quantencomputern, insbesondere potenziell gefährdeter Sicherheit von Verschlüsselungstechnologien, bewusst sind, sie jedoch bei der Transition zu quantensicherer Verschlüsselung meist noch am Anfang stehen.

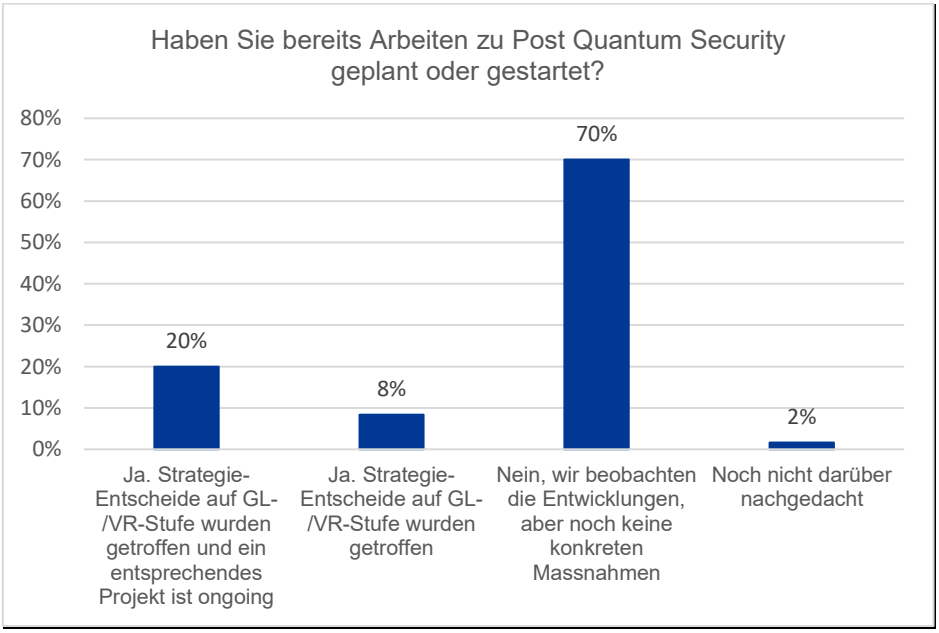
Institute sind sich der Cyberrisiken durch QC bewusst

Rund zwei Drittel der von der FINMA befragten Institute rechnen damit, bis in sieben Jahren direkt von den Cyberrisiken durch QC betroffen zu sein. Ebenfalls rechnen rund zwei Drittel damit, dass ein Quantencomputer bis in spätestens zehn Jahren innerhalb von 24 Stunden eine RSA-2048-bit Verschlüsselung knacken kann. Entsprechend sehen die befragten Institute die grössten Risiken durch Quantencomputer bei der Datensicherheit. Weitere hohe Risiken werden bei einer unvollständigen Migration zu quantensicherer Verschlüsselung, fehlendem Know-How, «harvest now, decrypt later» Angriffen sowie bei der Interoperabilität mit Legacy-Systemen gesehen.



Nur wenige Institute mit Roadmap zu quantensicherer Verschlüsselung

Von den befragten Instituten gaben 72 % an, noch keine Massnahmen zu quantensicherer Verschlüsselung geplant oder getroffen zu haben. 28 % haben einen entsprechenden Strategie-Entscheid getroffen, 20 % haben auch ein laufendes Projekt dazu.



Über eine konkrete Roadmap zu quantensicherer Verschlüsselung verfügen lediglich acht Prozent der Befragten. Dabei wird jeweils ein Zeitplan von vier bis fünf Jahren eingeplant, bis kritische Daten und Prozesse quantensicher sein sollen. Rund die Hälfte der befragten Institute plant in den nächsten ein bis drei Jahren eine Roadmap aufzusetzen, 43 % haben diesbezüglich noch nichts festgelegt.

Kryptoagilität, Inventar und externe Partner sind wichtig

Einigkeit besteht bei den Befragten zur Wichtigkeit zweier Faktoren bei der Transition zu Post-Quantum-Kryptografie (PQC): Einerseits wird die Kryptoagilität – also die Fähigkeit von IT-Systemen, Verschlüsselungsalgorithmen schnell und flexibel auszutauschen – verbreitet als wichtig oder sehr wichtig betrachtet (73 %). Andererseits wird auch ein hoher oder sehr hoher Mehrwert in der Erstellung eines Inventars der verwendeten kryptografischen Verfahren gesehen (76 %). Ob sie für die Arbeiten zur PQC-Migration Dienstleistungen von Dritten in Anspruch nehmen wollen, haben die Institute mehrheitlich noch nicht festgelegt. Externe Partner und Softwarelieferanten sind aber in jedem Fall zentral, da auch dort bzw. bei den Schnittstellen Cyberrisiken relevant sind. Von den Befragten sind daher 60 % bereits in Kontakt mit Softwarelieferanten oder haben dies geplant.

Zwei Drittel rechnen mit QC-Einsatz in ihrer Firma in frühestens acht Jahren

Den grössten Business Value von Quantencomputern sehen die befragten Institute bei der Risiko- und Portfolioanalyse, sowie bei der Transaktionsüberwachung, dem algorithmischen Trading und bei der Generierung besserer Zufallszahlen. Viele Institute sehen den aktuellen Reifegrad der meisten Anwendungen in ihrer Branche aber noch im Forschungs- oder frühen Entwicklungsstadium. Jenes Drittel der Befragten, welches sich bereits Gedanken zum Einsatz von Quantencomputern in ihrer Firma gemacht hat, sieht die wichtigsten Voraussetzungen dafür im Zugang zu Know-How und Fachkräften sowie in der Verfügbarkeit stabiler Hardware. Fast zwei Drittel der Befragten rechnen damit, QC-Anwendungen erst in acht oder mehr Jahren selbst einzusetzen.

Fazit zur Umfrage

Generell zeigt die Umfrage, dass viele Beaufsichtigte die zukünftigen Risiken durch QC zwar erkennen, konkrete Massnahmen zur Adressierung dieser Risiken hingegen erst vereinzelt ergriffen werden. Die FINMA weist in diesem Kontext auf die technischen Fortschritte in der Forschung, die lange Dauer von Migrationsprojekten, sowie auf erhebliche Unsicherheiten in Bezug auf die verbleibende Zeit bis zur Entwicklung kryptografisch relevanter Quantencomputer hin.

3 Empfehlungen

Die folgenden Empfehlungen stützen sich auf die Aufsichtstätigkeit der FINMA. Die FINMA bringt sie den betroffenen Beaufsichtigten zur Kenntnis und empfiehlt deren Berücksichtigung im internen Risikomanagement.

Die Empfehlungen beschränken sich auf die Migration zu quantensicheren Algorithmen[1] und gehen nicht auf den Einsatz von *Quantum Key Distribution* (QKD), sowie auf Fragen, die aus Quantencomputing-Anwendungen hervorgehen können, ein.

3.1 Strategie und Roadmap

Die FINMA empfiehlt als Grundlage der Migration zu quantensicherer Verschlüsselung, dass sich die Arbeiten auf eine vom Oberleitungsorgan verabschiedete Strategie stützen, aus der ein Umsetzungsplan mit Meilensteinen und Prioritäten abgeleitet wird. Ratsam ist dabei insbesondere die Festlegung von Zieldaten für die vollständige Migration sowie für die Migration der kritischen Geschäftsprozesse zu quantensicherer Kryptografie. Die FINMA legt die Erarbeitung einer PQC-Roadmap bis spätestens Mitte 2027 nahe.

Die PQC-Strategie kann Teil einer bestehenden Strategie sein (bspw. zu Cyberrisiken).

3.2 Risikoanalyse und Inventar

Am Anfang der Umstellung zu quantensicherer Verschlüsselung steht aus Sicht der FINMA eine Risikoanalyse – einerseits hinsichtlich verwendeter kryptographischer Verfahren, andererseits hinsichtlich kritischer und langfristig schützenswerter Daten.

Sie regt daher an, sämtliche Geschäftsprozesse im Detail auf verwendete Verschlüsselungs-, Signatur- und Authentifizierungstechnologien hin zu analysieren. Dabei sollten in der Einschätzung der FINMA sämtliche Informations- und Kommunikationstechnologie-Systeme (IKT-Systeme), Applikationen sowie Infrastruktur und neuartige Technologien wie verteilte elektronische Register (vgl. Art. 973*d* Abs. 2 Ziff. 2 Obligationenrecht [SR 220]) berücksichtigt werden, unabhängig davon, ob diese selbst betrieben werden, ausgelagert sind oder als Service bezogen werden.

Aus einer solchen Analyse der Geschäftsprozesse resultiert aus Sicht der FINMA ein umfassendes Inventar, welches alle verwendeten kryptograpfischen Verfahren auflistet. Dazu gehören die Verschlüsselung von Daten bei

[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

der Übertragung (bspw. VPN, TLS, HTTPS usw.) als auch gespeicherte Daten, die Verwendung von digitalen Signaturen, das Schlüsselmanagement und die eingesetzte Authentifizierungsmechanismen. Weiter ist aus einem solchen Inventar ersichtlich, ob die eingesetzten Algorithmen quantum-anfällig sind[2] und entsprechend ersetzt werden müssen. Für Systeme mit betroffenen Algorithmen ist es aus Sicht der FINMA angezeigt, dass entsprechend des damit verbundenen Risikos ein Migrationsplan festgelegt wird. Ein laufend gepflegtes kryptografisches Inventar, das den aktuellen Stand widerspiegelt, trägt dabei zur Wirksamkeit des Dispositivs bei.

3.3 Kritische Daten

Im Rahmen der Risikoanalyse empfielt es sich, auch den Schutzbedarf von kritischen Daten zu erheben und zu analysieren. Insbesondere wäre zu berücksichtigen, ob langfristige Sicherheitsgarantien in Bezug auf Vertraulichkeit und Integrität (oder auch *non-repudiation*, z.B. bei elektronischen Unterschriften) gewährleistet werden müssen. Dabei empfielt die FINMA, auch das Risiko von «harvest now, decrypt later» Angriffen zu berücksichtigen – das heisst, dass heute verschlüsselte Daten entwendet werden können, mit der Absicht, diese zu einem späteren Zeitpunkt mithilfe leistungsfähiger Quantencomputer zu entschlüsseln. Daten, die langfristig geschützt bleiben müssen, sollten prioritär behandelt und entsprechend durch PQC-Algorithmen geschützt werden.

Da noch keine Langzeiterfahrungen mit PQC-Algorithmen bestehen, empfehlen verschiedene Organisationen[3] in der kurzen bis mittleren Frist eine hybride Lösung gegenüber reinen PQC-Algorithmen. Dabei wird ein klassischer Algorithmus mit einem PQC-Algorithmus kombiniert, was die Sicherheit zusätzlich erhöht, bzw. die Sicherheit auch dann gewährleistet, wenn einer der beiden verwendeten Algorithmen sich als unsicher herausstellt. Die hybride Verschlüsselung wird insbesondere zum Schutz kritischer Daten vor «harvest now, decrypt later» Risiken häufig genannt. Allerdings führt dieser Ansatz auch zu einer erhöhten Komplexität, was Implementierungsrisiken mit sich bringt. Aus der internen Risikoanalyse kann auch der Einsatz hybrider Lösungen bei der Systemmigration hervorgehen.

3.4 Kryptoagilität

Auch in Zukunft muss damit gerechnet werden, dass heute als sicher erachtete (PQC-) Algorithmen ersetzt werden müssen. Beispielsweise könnten sich gewisse PQC-Algorithmen unerwarteterweise nicht bewähren.

[2] Bspw. RSA, ECDSA, EdDSA, DH, EC-DH

[3] "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptograph. 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

Kryptoagilität beschreibt die Fähigkeit eines IKT-Systems oder einer Applikation, kryptografische Algorithmen flexibel austauschen zu können. Dies geht über eine Migration zu PQC-Algorithmen hinaus und betrifft sämtliche verwendeten Algorithmen. Kryptoagilität als Vorgabe für neu anzuschaffende oder zu entwickelnde IKT-Systeme und Applikationen wird entsprechend empfohlen. Damit wird sichergestellt, dass IKT-Systeme flexibel und ohne tiefgreifende Änderungen an der Softwarearchitektur auf neue Verschlüsselungsalgorithmen umgestellt werden können.

3.5 Externe Dienstleister

Sowohl bei Auslagerungen von Funktionen als auch bei externen Kommunikationsschnittstellen bestehen in der Regel bei der PQC-Migration Abhängigkeiten zu externen Dienstleistern. Diese Dienstleister müssen in ihren Systemen ebenfalls eine Umstellung auf quantensichere Kryptografie vornehmen, um beim Aufkommen leistungsfähiger Quantencomputer weiterhin die notwendige Sicherheit gewährleisten zu können. Um diese Umstellung sachgemäss und kosteneffizient planen und umsetzen zu können, ist es meist sinnvoll, diese in reguläre Release-Zyklen zu integrieren. Dies bedingt eine längerfristige Planung in Zusammenarbeit mit dem externen Dienstleister betreffend neuen Anforderungen.

Die Verantwortung für die ausgelagerte Funktion liegt in jedem Fall beim auslagernden Institut (vgl. hierzu das FINMA-Rundschreiben 2018/3 «Outsourcing»). Auch künftige Risiken – etwa solche durch leistungsfähige Quantencomputer – können bereits heute antizipiert und Massnahmen mit den Dienstleistern vertraglich festgelegt werden.

Es wird empfohlen, bei allen neuen Outsourcing-Geschäftsbeziehungen im Software- und Daten-Bereich Kryptoagilität vorauszusetzen[4], bzw. bei bestehenden Auslagerungen diese zeitnah in die Anforderungen aufzunehmen.

4 Ausblick

Kryptografisch relevante Quantencomputer existieren heute noch nicht. Die technischen Fortschritte haben aber an Dynamik gewonnen und es ist in den kommenden Jahren mit deren Entwicklung zu rechnen. Ein angemessenes Risikomanagement des Cyberrisikos durch Quantencomputer ist daher notwendig.

Die FINMA regt im Hinblick auf die entstehenden Risiken durch Quantencomputer eine frühzeitige Auseinandersetzung und Mitigation dieser Risiken

[4] Fähigkeit von IT-Systemen, ihre Verschlüsselungsalgorithmen flexibel und ohne tiefgreifende Änderungen an der Softwarearchitektur austauschen zu können.

an – dies insbesondere aufgrund der Komplexität und des Zeitbedarfs der Migration zu quantensicheren Verschlüsselungstechnologien, der Interdependenzen zwischen Dienstleistern und Finanzinstituten sowie aufgrund des heute bereits realen Risikos von «harvest now, decrypt later» Angriffen.

Die FINMA wird die Entwicklungen im Bereich QC aktiv weiterverfolgen und das Thema verstärkt in ihre laufenden Aufsichtstätigkeit aufnehmen.