

FINMA & QUANTUM COMPUTING -FLASH

Die neue FINMA-Aufsichtsmitteilung 05/2026 zu **Quantum Computing** und ihre Bedeutung für Schweizer Finanzinstitute

2026 · QUANTUM COMPUTING UND POST-QUANTUM KRYPTOGRAPHIE-FLASH · CA. 12 MIN. LESEZEIT · DR. IUR. DIRK SPACEK

1. Ausgangslage

Am 9. Juli 2026 hat die Eidgenössische Finanzmarktaufsicht FINMA die Aufsichtsmitteilung 05/2026 zum Thema Quantum Computing veröffentlicht. Sie fasst die Ergebnisse einer zwischen November 2025 und Januar 2026 durchgeführten Umfrage bei 60 Schweizer Finanzinstituten – bewilligte Banken, Versicherungsunternehmen, Verwalter von Kollektivvermögen und Finanzmarktinfrastrukturen – zusammen und leitet daraus aufsichtsrechtliche Erwartungen ab. Im Zentrum steht nicht der künftige produktive Einsatz von Quantencomputern selbst, sondern deren absehbare Fähigkeit, die heute im Finanzsektor breit eingesetzte Kryptografie zu brechen. Eine vollständige Migration auf quantensichere Verfahren wird daher nötig sein und eine solche kann angesichts heterogener, historisch gewachsener IT-Landschaften (legacy IT) mehrere Jahre dauern. Hier liegt ein zeitlicher Risikofaktor: Wer erst reagiert, wenn leistungsfähige Quantencomputer verfügbar sind, dürfte die erforderliche Transformation nicht mehr rechtzeitig schaffen.

2. Was ist Quantum Computing – und weshalb betrifft es Finanzinstitute?

Quantum Computing bezeichnet eine Informationsverarbeitung auf Basis der Quantenmechanik. Während klassische Computer binär mit Bits (0 oder 1) rechnen, arbeiten Quantencomputer mit sogenannten Qubits, die sich in einer **Überlagerung** (Superposition) beider Zustände befinden, d.h. ein Qubit kann gleichzeitig ein bisschen «0» und ein bisschen «1» sein, wie eine Münze, die noch in der Luft dreht vor der Landung. Qubits können auch **miteinander verschränkt** sein, d.h. das Ergebnis eines Qubits hängt sofort vom Zustand des anderen ab, egal wie weit sie auseinander liegen. So können viele Qubits zusammen viel mehr Informationen verarbeiten als einzelnen Bits. Im Finanzdienstleistungskontext lassen sich so bestimmte Berechnungen – insbesondere kombinatorische Optimierungsprobleme, Simulationen und zahlentheoretische Probleme – effizienter lösen als mit klassischen Computerprogrammen.

Für den Finanzsektor ergeben sich daraus zwei sehr unterschiedliche Dimensionen. Auf der **Chancenseite** wird ein erheblicher wirtschaftlicher Nutzen erwartet, insbesondere im *Risikomanagement* (schnellere und präzisere Simulation komplexer Abhängigkeiten zwischen Vermögenswerten, Value-at-Risk- und Stresstest-Berechnungen), in der *Portfolio-Optimierung* (bessere Allokationseinschätzung über verschiedene Anlagekategorien), bei der *Bewertung von Derivaten* sowie bei der *Betrugserkennung* und im Handel. Grosse internationale Banken und der

hiesige Bankensektor (u. a. gemäss Expertenbericht der Schweizerischen Bankiervereinigung) investieren deshalb bereits heute in Quantenmechanik-Pilotprojekte, obwohl ein breiter produktiver Einsatz mehrheitlich erst in den 2030er-Jahren erwartet wird.

Auf der **Risikoseite** steht die Kryptografie: Weit verbreitete asymmetrische Verschlüsselungsverfahren mit zwei Schlüsseln wie RSA, ECDSA, EdDSA oder (EC-)Diffie-Hellman beruhen auf mathematischen Rechenaufgaben, die in eine Richtung leicht, in die andere Richtung schwer zu lösen sind. Der öffentliche Schlüssel enthält z.B. eine riesige Zahl (als Ergebnis einer Multiplikation). Wer sie entschlüsseln will, ohne den privaten Schlüssel mit den ursprünglichen Multiplikationsfaktoren zu kennen, müsste diese riesige Zahl in ihre beiden ursprünglichen Faktoren zurückrechnen. Das ist fast nicht möglich, solange man keine viel stärkere Rechenleistung hat. Hier können Quantencomputer gefährlich werden: Ein Quantencomputer kann dank Superposition und Verschränkung (siehe oben) genau diese Art von Rückwärtsrechnung viel schneller lösen als ein normaler Computer. So liessen sich Verschlüsselung, digitale Signaturen und Authentifizierung – die Grundlage von Online-Banking, Zahlungssystemen, TLS/HTTPS-Verbindungen, elektronischen Signaturen und auch von Kryptowerten – kompromittieren. Das ist im Grunde ein altbekanntes Muster. Technische Verbesserungen/Neuerungen bringen immer auch neue Risiken mit sich. Besonders brisant ist das Risiko sogenannter «*Harvest now, decrypt later*»-Angriffe durch Quantum Computing: Bereits heute verschlüsselte Daten können abgefangen und gespeichert werden, um sie zu einem späteren Zeitpunkt mit künftiger Quantenrechenleistung zu entschlüsseln – ein Risiko, das schon jetzt real ist, auch wenn der leistungsfähige Quantencomputer in Idealform selbst noch nicht existiert.

3. Kernaussagen der FINMA-Aufsichtsmitteilung 05/2026

Rechtlich stützt sich die Mitteilung nicht auf eine neue Rechtsgrundlage, sondern auf die bestehenden, technologieutralen und prinzipienbasierten Anforderungen an Governance und Risikomanagement für operationelle Risiken und Resilienz. Diese Prinzipien sind sinngemäss schon festgehalten in dem FINMA Rundschreiben 2023/1 – Operationelle Risiken und Resilienz – Banken, im FINMA Rundschreiben 2018/3 – Outsourcing Banken und Versicherer oder die FINMA-Aufsichtsmitteilung 08/2024 Governance und Risikomanagement beim Einsatz von Künstlicher Intelligenz.

Die FINMA hält in der neuen Aufsichtsmitteilung fest, dass Anforderungen an Governance und Risikomanagement auch die aus Quantum Computing resultierenden Risiken miterfassen muss. Sie zeigt Empfehlungen zur Berücksichtigung im internen Risikomanagement. Die Empfehlungen beschränken sich aber vor allem auf die Migration zu quantensicheren Algorithmen (Post-Quantum-Kryptografie, «**PQC**», siehe mehr Details dazu unten). Zum Thema Quantum Key Distribution – d.h. der konkrete Einsatz von Quantum Computing, um einen geheimen Schlüssel zwischen zwei Parteien auszutauschen – und Fragen rund um den produktiven Einsatz von Quantencomputer-Anwendungen äussert sich die FINMA nicht.

Aus der der Aufsichtsmitteilung zugrundeliegenden Umfrage geht hervor, dass sich die Institute der Risiken zwar bewusst sind – rund zwei Drittel rechnen damit, innert sieben Jahren direkt betroffen zu sein, ebenso viele halten es für plausibel, dass z.B. eine RSA-2048-Verschlüsselung –

ein Verfahren, das auf einer riesigen Zahl beruht, die aus zwei geheimen Primzahlen multipliziert wurde – binnen zehn Jahren innert 24 Stunden geknackt werden könnte. Konkrete Massnahmen seien aber erst vereinzelt getroffen wurden: 72 % der Institute haben noch keine Massnahmen geplant oder umgesetzt, und lediglich 8 % verfügen bereits über eine konkrete Roadmap. Daraus diagnostiziert die FINMA einen branchenweiten Nachholbedarf.

Die fünf Empfehlungsblöcke der FINMA

- **Strategie und Roadmap:** Die FINMA legt eine vom Oberleitungsorgan (Verwaltungsrat) verabschiedete Strategie mit Umsetzungsplan, Meilensteinen und Zieldaten nahe – mit **einer Roadmap für die PQC-Migration bis spätestens Mitte 2027**. Die Strategie kann Teil einer bestehenden Cyberrisiko-minimierungsstrategie sein. Unter PQC-Migration verstanden wird eine Migration bestehender kryptografischen Verfahren – also überall wo heute RSA, ECDSA verwendet wird, z.B. bei digitalen Signaturen bei der Übertragung von Daten über TLS/HTTPS-Verbindungen – in neue quantensichere Verschlüsselungsverfahren, die eben nicht auf mathematischen Problemlösungen basieren, die ein Quantencomputer z.B. mit dem Shor-Algorithmus effizient lösen könnte (Primfaktorzerlegung). **PQC-Verschlüsselungen** basieren auf anderen Problemlösungspfaden wie z.B. der **Gitterkryptographie** (mehrdimensionale Punktraster in hunderten von Dimensionen basierend auf Vektorberechnungen, die Verschlüsselung basiert hier auf einer «guten» und einer «schlechten» Beschreibung, die nur zusammen übereinstimmen können. Die US-Behörde NIST hat bereits 2024 3 solche Verfahren offiziell standardisiert:
 - ML-KEM (FIPS 203) für Schlüsselaustausch und Verschlüsselung;
 - ML-DAS (FIPS 204) für digitale Signaturen;
 - SLH-DAS (FIPS 205) – ebenfalls für Signaturen, falls sich gitterbasierte Verfahren später doch als angreifbar erweisen sollten.
- **Risikoanalyse und Inventar:** Grundlage bildet eine **Risikoanalyse sämtlicher Geschäftsprozesse** hinsichtlich eingesetzter Verschlüsselungs-, Signatur- und Authentifizierungstechnologien (inkl. ausgelagerter und bezogener Services sowie neuartiger Technologien wie verteilte elektronische Register). Daraus resultiert ein **laufend zu pflegendes kryptografisches Inventar**, das aufzeigt, welche Algorithmen quantenanfällig sind (z. B. RSA, ECDSA, EdDSA, DH, EC-DH) und ersetzt werden müssen.
- **Schützenswerte Daten:** Langfristig schützenswerte Daten sind prioritär zu identifizieren und vor «*Harvest now, decrypt later*»-Angriffen zu schützen. Mangels Langzeiterfahrung mit PQC-Algorithmen empfiehlt sich vorerst der Einsatz hybrider Lösungen, welche klassische und PQC-Algorithmen kombinieren.
- **Kryptoagilität:** Da auch künftige PQC-Verfahren ersetzt werden könnten, empfiehlt die FINMA Kryptoagilität – die Fähigkeit, kryptografische Algorithmen ohne tiefgreifende Architekturänderungen austauschen und erneuern zu können – als verbindliche Vorgabe für neue IKT-Systeme und Applikationen.

Externe Dienstleister: Die Verantwortung für ausgelagerte Funktionen verbleibt gemäss FINMA-Rundschreiben 2018/3 «Outsourcing» beim Institut. **Kryptoagilität** sollte bei neuen Auslagerungsbeziehungen im Software- und Datenbereich vorausgesetzt und bei bestehenden **Verträgen mit IT-Anbietern** zeitnah nachgefordert werden, idealerweise eingebettet in reguläre Release-Zyklen.

4. Einordnung und Handlungsbedarf

Auch wenn kryptografisch relevante Quantencomputer heute noch nicht existieren, betont die FINMA, dass sich die technologische Entwicklung beschleunigt und mit erheblicher Unsicherheit über den Zeitpunkt ihres Aufkommens zu rechnen ist. Rechtlich ist die **PQC-Migration** damit kein isoliertes IT-Projekt, sondern eine **institutsweite Aufgabe**, die Governance, Compliance, Risikomanagement, Informationssicherheit, Beschaffungswesen und Drittpartei-management gleichermassen betrifft und entsprechende Dokumentation gegenüber Verwaltungsrat und Aufsicht erfordert. Die FINMA kündigt zudem an, das Thema aktiv weiterzuverfolgen und verstärkt in ihre laufende Aufsichtstätigkeit einzubeziehen – eine **Prüfung im Rahmen künftiger Aufsichtsgespräche und Prüfberichte** ist damit **absehbar**.

Take Away für die Praxis: Für die Praxis ergeben sich daraus kurzfristig prioritäre Schritte für Finanzinstitute: 1) Die Auslösung bzw. Dokumentation eines Strategieentscheids auf Stufe Geschäftsleitung/Verwaltungsrat zu einer PQC-Roadmap, 2) der Aufbau eines kryptografischen Inventars, 3) die Identifikation langfristig schutzwürdiger Daten sowie 4) die vertragliche Absicherung von Kryptoagilität gegenüber Dienstleistern. Da die Frist für eine PQC-Roadmap («spätestens Mitte 2027») nicht mehr weit entfernt ist und die Migration selbst mehrere Jahre dauern könnte, empfiehlt sich ein zeitnaher Start. Ein *kombinierter Einbezug von IT/Verschlüsselungsexperten, Governancespezialisten und IT-Compliance-Rechtsspezialisten* ist deshalb nahegelegt.

Diese Kurzpublikation dient der allgemeinen Information und ersetzt keine Rechtsberatung im Einzelfall.

Dirk Spacek, Dr. iur., LL.M. ist Rechtsanwalt und Partner in Zürich. Er berät Unternehmen in allen vertrags- und handelsrechtlichen Belangen mit besonderem Fokus auf Fragen an der Schnittstelle von Technologie, Immaterialgüter- und Daten/Cyberrecht.