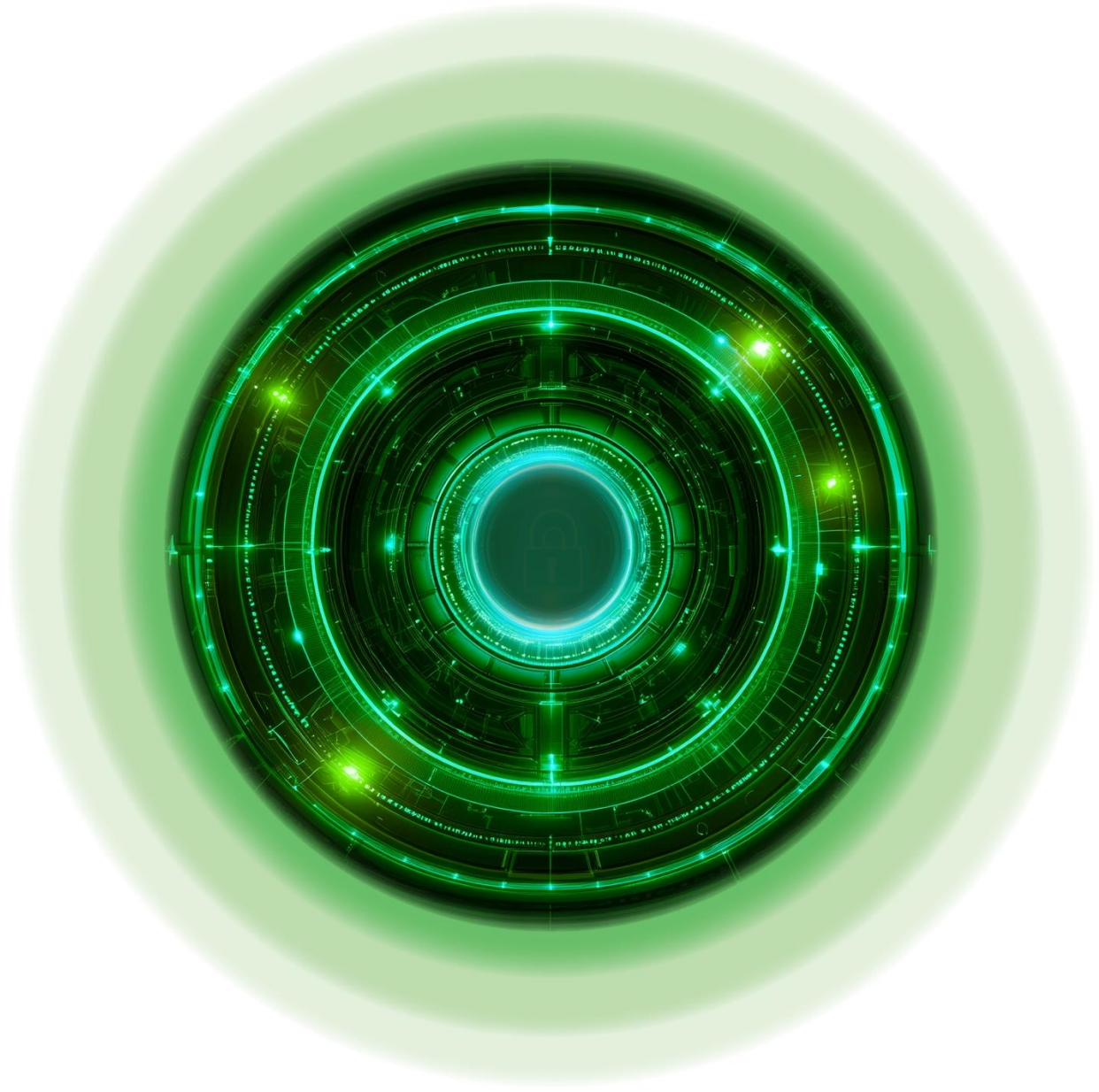




Post-Quanten- Bereitschaft für Schweizer Finanzinstitute

Cyber Switzerland

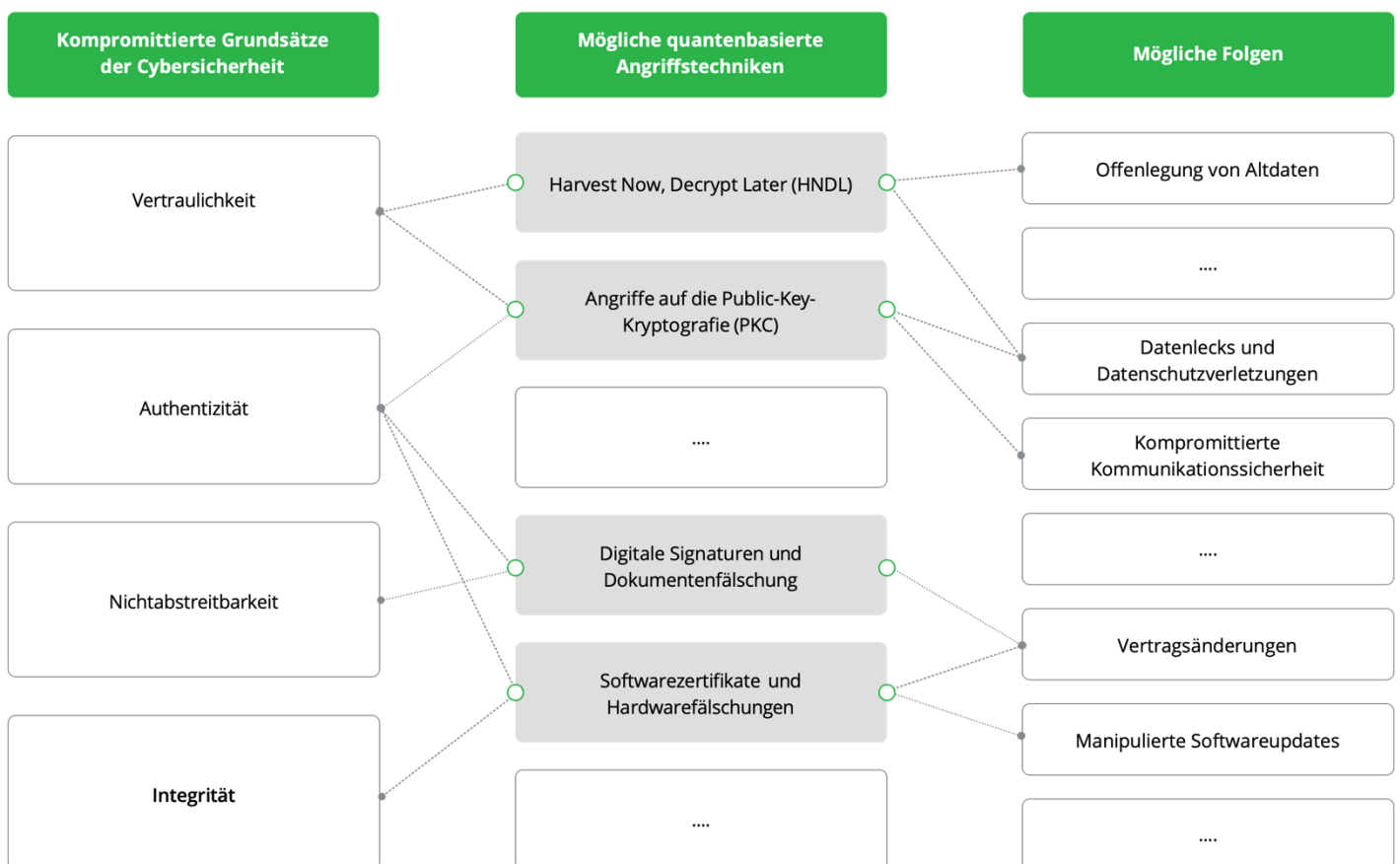


Abschnitt 1

Die FINMA setzt neue Massstäbe: Schweizer Finanzinstitute müssen jetzt vom Bewusstsein ins konkrete Handeln kommen.

Quantencomputing stellt eine unmittelbare kryptografische Bedrohung für Finanzinstitute dar. Quantencomputer mit ausreichender Rechenleistung werden die heute gängige Public-Key-Kryptografie (PKC) untergraben, die eine Vielzahl wichtiger Anwendungen absichert, darunter die digitale Kommunikation, die elektronische Signatur von Dokumenten, die Überprüfung der Softwareintegrität und den Schutz gespeicherter sensibler Daten.

Kryptografisch relevante Quantencomputer sind zwar noch nicht auf dem Markt, doch bereits heute bestehen damit verbundene Risiken. Die FINMA-Aufsichtsmittelung 05/2026 hebt insbesondere «Harvest Now, Decrypt Later»-Angriffe (HNDL) hervor, bei denen verschlüsselte Daten bereits heute gesammelt und erst in Zukunft entschlüsselt werden, sobald die Quanteninformatik ausgereift ist. HNDL ist jedoch nicht das einzige Problem für Finanzinstitute. Quantenbasierte Angriffe gefährden nicht nur die Vertraulichkeit als Sicherheitseigenschaft, sondern auch die Eigenschaften Integrität, Authentizität und Nichtabstreitbarkeit.



Der Übergang zur quantensicheren Kryptografie wird als komplexes Unterfangen mehrere Jahre in Anspruch nehmen. Die FINMA-Aufsichtsmittelung 05/2026 verdeutlicht diesen Punkt durch die Einführung des Konzepts der «Krypto-Agilität», das über die Post-Quanten-Kryptografie (PQC) hinausgeht. Krypto-Agilität ist die Fähigkeit, kryptografische Algorithmen, Parameter und Implementierungen effizient zu ersetzen, wenn sich Risiken, Standards oder geschäftliche Anforderungen ändern. Allerdings wird es aufgrund der Komplexität heterogener Technologielandschaften einige Zeit dauern, bis ein ausreichendes Mass an Krypto-Agilität erreicht ist.

Wie in der FINMA-Aufsichtsmittelung 05/2026 dargelegt, sind sich die Schweizer Finanzinstitute der quantenbezogenen Cybersicherheitsrisiken bewusst. Viele stehen jedoch noch am Anfang, wenn es darum geht, aus diesem Bewusstsein konkrete Massnahmen abzuleiten. Der Übergang zur quantensicheren Kryptografie ist komplex und zeitaufwendig – genau deshalb sollten Finanzinstitute bereits jetzt damit beginnen, wirkungsvolle Massnahmen nach Risikograd zu priorisieren und die für eine nachhaltige kryptografische Resilienz erforderlichen Fähigkeiten zu entwickeln.

Warum Krypto-Agilität bereits heute wichtig ist: Unabhängig von der Post-Quanten-Bedrohung gewinnt die Fähigkeit, Kryptografie schnell anzupassen, zunehmend an Bedeutung, da künstliche Intelligenz (KI) die Entdeckung und Ausnutzung von Sicherheitslücken in Software beschleunigt, einschliesslich anfälliger Implementierungen kryptografischer Algorithmen. Nur krypto-agile Organisationen sind in der Lage, kryptografische Risiken rasch zu erkennen, zu bewerten und zu beheben. Bei nicht krypto-agilen Organisationen kann die Behebung solcher Risiken bis zu mehreren Jahren dauern, wie im Falle der SHA-1-Umstellung beobachtet wurde.





Abschnitt 2

Die FINMA-Aufsichtsmitteilung verlagert die Diskussion von «Wann wird die Quantentechnologie Einzug halten?» hin zu «Sind wir darauf vorbereitet?»

Eine Umfrage der FINMA unter 60 Schweizer Finanzinstituten deckt eine kritische Lücke auf: Zwar sind sich die meisten Finanzinstitute quantenbezogener Cyberrisiken bewusst, doch nur wenige haben dieses Bewusstsein in konkrete Massnahmen umgesetzt. Nur 8 Prozent verfügen über eine konkrete Roadmap, und die FINMA erwartet von den Finanzinstituten, dass sie diese Lücke bis spätestens Mitte 2027 schliessen. Im Folgenden werden auf der Grundlage der Empfehlungen der FINMA fünf wesentliche Massnahmen vorgeschlagen, die jeweils darlegen, was Finanzinstitute bei der Entwicklung einer kryptografischen Resilienz berücksichtigen sollten, die nicht nur die Bedrohungen durch Post-Quanten-Computing abdeckt.

Festlegung von Strategie und Roadmap

Die FINMA empfiehlt, dass der Übergang zur quantensicheren Verschlüsselung auf einer vom Verwaltungsrat genehmigten Strategie beruhen sollte, die einen Umsetzungsplan mit Meilensteinen und Prioritäten umfasst. Für die gesamte Migration sowie separat für kritische Geschäftsprozesse sollten Zieltermine festgelegt werden.

Für Finanzinstitute sollte eine konkrete und solide Strategie Antworten auf die folgenden zentralen Fragen liefern:

- Welche kryptografischen Risiken sind für unsere Kundinnen und Kunden, unsere Geschäftspartnerinnen und -partner und unser eigenes Unternehmen besonders relevant?
- Wie wirken sich diese kryptografischen Risiken auf das aktuelle und zukünftige Geschäfts- und Betriebsmodell aus?
- Welche Geschäftsdienste, Anwendungen, Datenflüsse und Abhängigkeiten von Drittanbietenden fallen in den Geltungsbereich?
- Welche Vermögenswerte und Daten müssen über den erwarteten Zeithorizont der Quantenbedrohung hinaus geschützt werden?
- Welche Änderungen lassen sich in bestehende Programme im Zusammenhang mit Technologieerneuerung, Cloud, Kernsystemen, Identitäts- und Zertifikatsverwaltung oder Cyberresilienz integrieren?
- Welche Entscheidungen müssen die Geschäftsleitung und der Verwaltungsrat treffen?

Eine umsetzbare Roadmap sollte risikoorientiert sein und eine klare Ausrichtung, Zuständigkeiten, eine Priorisierungslogik sowie Entscheidungspunkte festlegen, ohne dass jede technische Lösung im Voraus vorgegeben werden muss.



Durchführung einer Risikoanalyse und einer Krypto-Bestandsaufnahme

Die FINMA beschreibt die Risikoanalyse und Bestandsaufnahme als ersten Schritt des Übergangs. Finanzinstitute sollten Verschlüsselungs-, digitale Signatur- und Authentifizierungstechnologien identifizieren, die in Geschäftsprozessen, IT-Systemen, der lokalen Infrastruktur, Cloud-Diensten und Integrationen von Drittanbietenden zum Einsatz kommen.

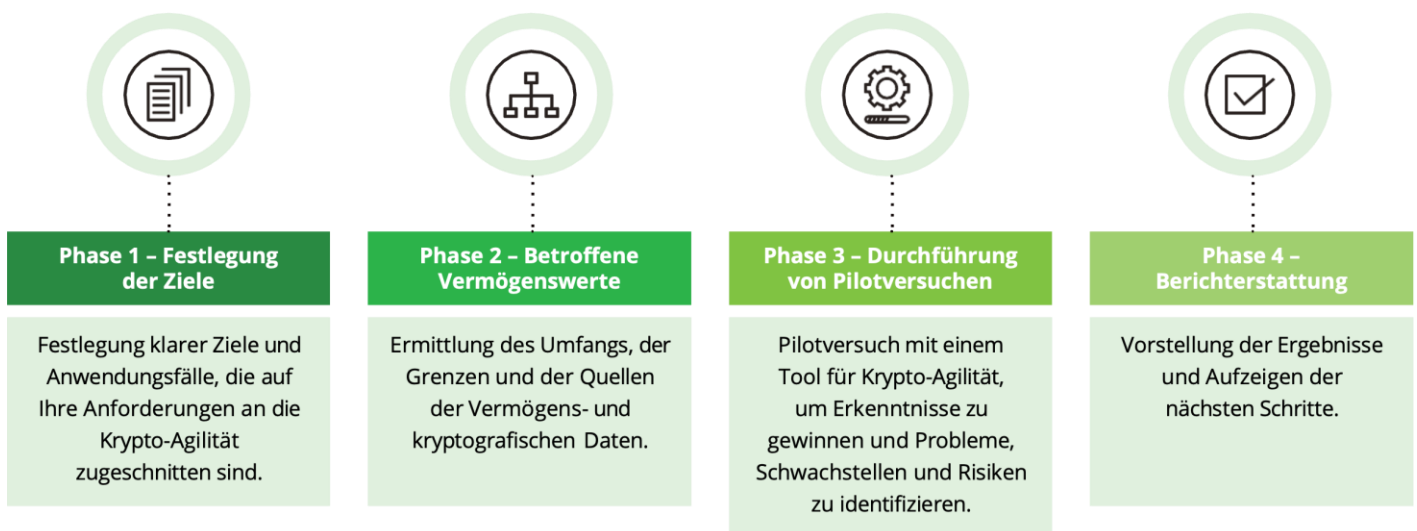
Genau hier unterschätzen viele Organisationen die Herausforderung. Kryptografie ist oft tief in Anwendungen, Protokollen, Zertifikaten, Hardware, Middleware, Cloud-Diensten und Arbeitsabläufen eingebettet. Ohne eine Bestandsaufnahme kann ein Unternehmen nicht zuverlässig beantworten, welche Systeme quantenanfällige Algorithmen verwenden, welche Daten gefährdet sind, welche Drittanbietenden beteiligt sind oder wo die Migration am schwierigsten sein wird.

Die Bestandsaufnahme sollte umfassend sein und folgende Aspekte abdecken:

- Verschlüsselung von Daten während der Übertragung;
- Verschlüsselung von gespeicherten Daten;
- digitale Signaturen;
- Authentifizierungsmechanismen;
- wichtige Verwaltungsprozesse;
- Zertifikate und Zertifikatslebenszyklusverwaltung;
- Abhängigkeiten von Software, Plattformen und Managed Services von Drittanbietenden;
- Kryptografische Algorithmen, die potenziell anfällig für Quantenangriffe sind.

Diese Bestandsaufnahme sollte laufend gepflegt und aktualisiert werden, um Änderungen an Systemen, Anwendungen und Abhängigkeiten von Drittanbietenden Rechnung zu tragen. Zwar kann dies aufwendig sein, doch es gibt Schlüsseltechnologien für Krypto-Agilität, mit denen sich der Grossteil der damit verbundenen Aktivitäten automatisieren lässt.

Vorbereitung der Krypto-Bestandsaufnahme



Priorisierung kritischer Daten und langfristiger Schutzanforderungen

Die FINMA legt den Schwerpunkt auf kritische Daten und das «Harvest Now, Decrypt Later»-Risiko (HNDL). Die praktische Frage, die sich Finanzinstitute im Zusammenhang mit HNDL stellen sollten, lautet: «Welche Daten würden auch dann noch inakzeptablen Schaden anrichten, wenn sie erst in einigen Jahren entschlüsselt würden?»

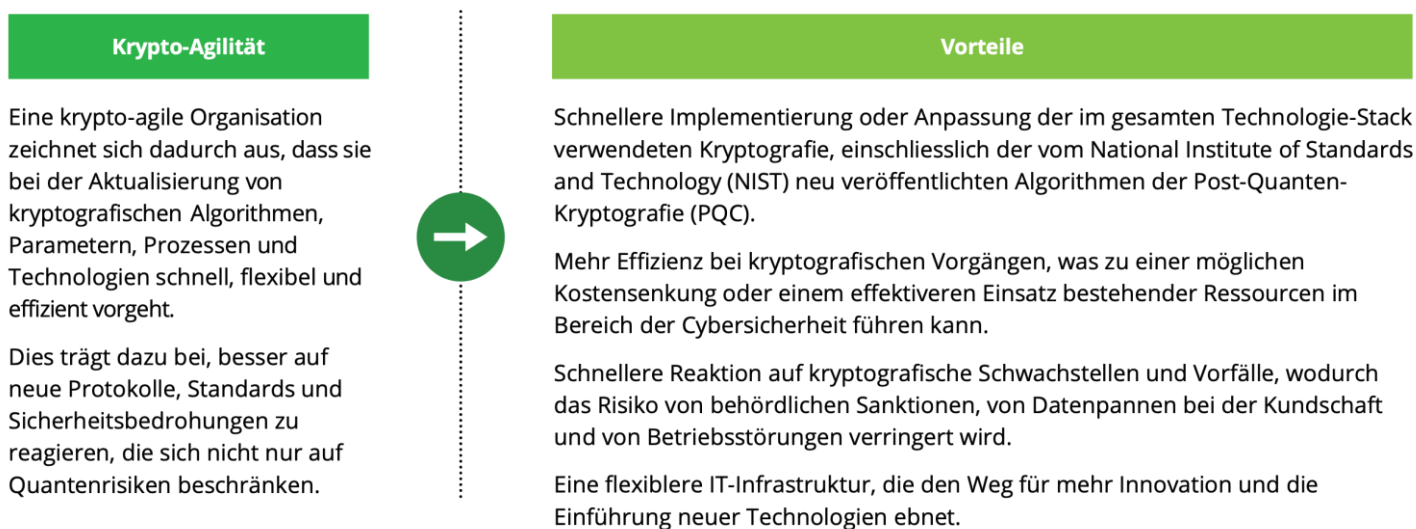
Finanzinstitute sollten daher ermitteln, welche Daten langfristig Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit erfordern. Dazu können Daten von Kundinnen und Kunden, Transaktionsdaten, rechtliche Vereinbarungen, vertrauliche Korrespondenz sowie Unterlagen gehören, für die lange Aufbewahrungsfristen gelten.

Die FINMA stellt fest, dass verschiedene Organisationen kurz- bis mittelfristig Hybridlösungen empfehlen, bei denen traditionelle und Post-Quanten-Algorithmen kombiniert werden. Dies kann zusätzliche Sicherheit bieten, während sich Post-Quanten-Algorithmen weiterentwickeln, erhöht aber auch die Komplexität der Umsetzung.

Datenschutzkonzepte für kritische Daten



Sicherstellung von Krypto-Agilität – nicht nur aufgrund von Post-Quanten-Risiken



Die FINMA empfiehlt Krypto-Agilität als Anforderung für Anwendungen und andere IT-Systeme, die beschafft oder entwickelt werden sollen. Selbst nach der Einführung von Post-Quanten-Algorithmen müssen einige davon später möglicherweise ersetzt werden. Unabhängig von den Fortschritten im Bereich des Quantencomputings können kryptografische Schwachstellen durch Mängel im Algorithmen-Design, mangelhafte Implementierung, veraltete Programmbibliotheken, fehlerhafte Konfigurationen oder anfällige Softwarelieferketten entstehen. Es kommt häufig vor, dass ein Algorithmus oder dessen Implementierung von Zeit zu Zeit anfällig wird und ersetzt werden muss. Zu den Beispielen aus der Vergangenheit zählen SHA-1 (eine veraltete Hash-Funktion), MD5 (ein geknackter kryptografischer Hash) und RC4 (ein kompromittiertes Verschlüsselungsverfahren), deren Ersatz bei einigen Organisationen aufgrund der mangelnden Krypto-Agilität mehrere Jahre in Anspruch nahm.

Ein krypto-agiles Unternehmen ist besser aufgestellt, um zu reagieren, wenn solche Schwachstellen entdeckt werden – ganz gleich, ob der Auslöser nun Fortschritte in der Quanteninformatik, KI-gestützte Bedrohungsaktivitäten, ein neuer Standard oder eine Schwachstelle in einer kryptografischen Komponente ist.

Für Finanzinstitute sollte die Krypto-Agilität in die Architektur, die Beschaffung, die sichere Entwicklung, das Lebenszyklusmanagement von Schlüsseln und Zertifikaten sowie die Governance des technologischen Wandels integriert werden. Es sollte zudem zu einer grundlegenden Anforderung bei der Entwicklung neuer Systeme werden und nicht erst dann in Betracht gezogen werden, wenn eine Migration erforderlich wird.

Frühzeitige Einbeziehung externer Dienstleistender und anderer Dritter

Die FINMA weist ausdrücklich darauf hin, dass die Umstellung auf Post-Quanten-Systeme zu Abhängigkeiten von externen Dienstleistenden führen wird. Dies ist für Finanzinstitute von entscheidender Bedeutung, da ein grosser Teil der kryptografischen Risiken möglicherweise in extern verwalteten Infrastrukturen liegt, wie beispielsweise Kernplattformen, Zahlungsdiensten, Cloud-Umgebungen und bei Identitätsanbietenden.

Finanzinstitute sollten Gespräche mit externen Dienstleistenden aufnehmen, um sich ein Bild von deren Post-Quanten-Bereitschaft, den unterstützten Algorithmen, den Produkt-Roadmaps, den Veröffentlichungszeitplänen und den Migrationsabhängigkeiten zu machen.

Anforderungen hinsichtlich Post-Quanten-Sicherheit und Krypto-Agilität sollten in folgende Bereiche integriert werden:

- neue Anforderungen an Outsourcing und Beschaffung;
- Cyber-Risikobewertungen durch Dritte;
- Vertragsverlängerungen und Gespräche über die Leistungserbringung;
- Architektur- und Integrationsstandards;
- Release-Planungs- und Testzyklen.

In der Praxis sind drei Dinge erforderlich:

1. Einblick in die Roadmaps und Abhängigkeiten der Lieferantinnen und Lieferanten;
2. vertragliche Klarheit hinsichtlich der Post-Quanten-Anforderungen und Zeitpläne;
3. Einfluss auf die Release-Planung, um diese an den Migrationszeitplan des Finanzinstituts anzupassen.

Ohne diese Massnahmen laufen Finanzinstitute Gefahr, von den Zeitplänen ihrer Lieferantinnen und Lieferanten abhängig zu sein, anstatt ihre eigene Post-Quanten-Umstellung selbst voranzutreiben.

Um Finanzinstituten bei der Beurteilung der Bereitschaft ihrer Lieferantinnen und Lieferanten zu helfen, veranschaulicht das nachstehende Reifegradmodell den Entwicklungsprozess von «kein formaler Prozess» bis hin zu «vollständig integrierte Post-Quanten-Anforderungen» im Drittanbietermanagement.

Vorbereitung der Krypto-Bestandsaufnahme

Nicht definiert	Manuell	Grundlegend	Fortgeschritten	Integriert
Verfügt der Drittanbietende über Verfahren im Bereich der Post-Quanten-Kryptografie?	Verwendet der Drittanbietende Tabellenkalkulationen, um Schlüssel oder Zertifikate zu verwalten?	Verfügt der Drittanbietende über Tools zur Verwaltung von Schlüsseln und Zertifikaten?	Wird die Automatisierung für die Beantragung, Bereitstellung und Erneuerung von Zertifikaten genutzt?	Sind die Tools und Prozesse in andere Systeme integriert?

Abschnitt 3

Erste sowie empfohlene weitere Schritte

Der erste Schritt eines Post-Quanten-Programms besteht darin, sich einen Überblick über die aktuelle Situation des Finanzinstituts zu verschaffen, indem «diagnostische» Fragen beantwortet werden, anhand derer sich der am besten geeignete Weg ermitteln lässt. Beispiele für Fragen:

- Wissen Sie, welche kryptografischen Risiken für Ihre Kundinnen und Kunden, Ihre Geschäftspartnerinnen und -partner und Ihr Unternehmen besonders relevant sind?
- Haben Sie analysiert, wie sich diese kryptografischen Risiken auf Ihr aktuelles und zukünftiges Geschäfts- und Betriebsmodell auswirken?
- Gibt es eine PQC-Strategie und eine PQC-Roadmap, die vom Verwaltungsrat genehmigt wurden?
- Haben Sie eine umfassende Bestandsaufnahme der kryptografischen Ressourcen im gesamten Unternehmen durchgeführt, einschliesslich der Abhängigkeiten von Drittanbietenden?
- Haben Sie ermittelt, welche Daten langfristig geschützt werden müssen?
- Sehen Ihre Beschaffungs- und Architekturstandards Krypto-Agilität für neue Systeme und Outsourcing-Vereinbarungen vor?
- Haben Sie mit wichtigen Lieferantinnen und Lieferanten Kontakt aufgenommen, um sich über deren Post-Quanten-Bereitschaft und Produkt-Roadmaps zu informieren?

Die Antworten geben Aufschluss darüber, welcher der beiden unten aufgeführten Wege für eine bestimmte Organisation am besten geeignet ist.

Weg A: Erste Schritte für Finanzinstitute mit begrenzter oder nicht vorhandener Post-Quanten-Bereitschaft

Wenn die Antwort auf die meisten dieser Fragen «Nein» lautet, sollte der Schwerpunkt darauf gelegt werden, die Grundlagen für die Post-Quanten-Bereitschaft zu schaffen. Die folgenden Schritte bieten einen strukturierten Ansatz zur Grundlagenentwicklung:

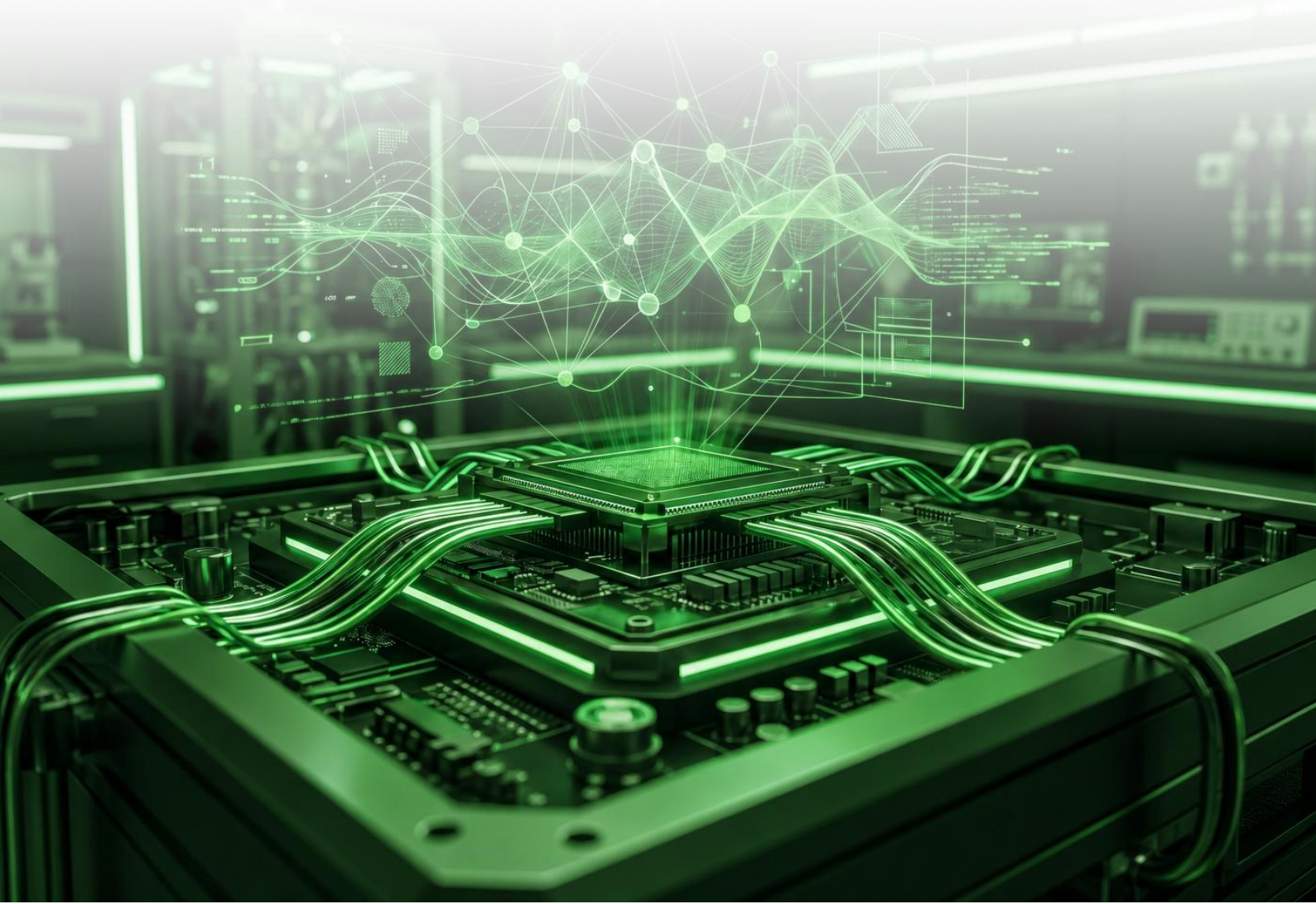
- Schritt 1** Schaffung von Verantwortlichkeiten und Eigenverantwortung innerhalb der Organisation und der Geschäftsfunktion.
- Schritt 2** Entwicklung einer Roadmap für die Post-Quanten-Strategie, die Meilensteine, Abläufe, Entscheidungspunkte, Abhängigkeiten und Zieltermine umfasst und sich an der Empfehlung der FINMA für Mitte 2027 orientiert.
- Schritt 3** Festlegung eines Risikomanagement-Rahmenwerks zur Identifizierung, Bewertung und Behebung von Post-Quanten-Risiken.
- Schritt 4** Festlegung der betroffenen Systeme, Anwendungen und Daten und Ermittlung der wichtigsten Risiken im Hinblick auf Vertraulichkeit, Integrität, Authentifizierung und Resilienz.
- Schritt 5** Durchführung einer diagnostischen Bewertung, um den Umfang und die Tiefe der kryptografischen Sicherheitsrisiken zu erfassen; Schaffung einer Grundlage für die Priorisierung der Bereiche, in denen eine eingehendere Analyse erforderlich ist.
- Schritt 6** Krypto-Bestandsaufnahme, beginnend bei Umgebungen mit hoher Priorität (je nach Risiko und Kritikalität).
- Schritt 7** Integration von Krypto-Agilität, um sicherzustellen, dass künftige Änderungen an kryptografischen Standards keine einschneidenden Nacharbeiten erfordern.

Weg B: Nächste Schritte für bereits in Transformation zur Krypto-Agilität befindliche Finanzinstitute

Wenn die Antwort auf die meisten dieser Fragen «Ja» lautet, sind die Grundlagen wahrscheinlich geschaffen, und die nächsten Schritte sollten sich auf Beschleunigung, Vertiefung und Resilienz konzentrieren:

- Schritt 1** Verankerung der Krypto-Agilität in den Betriebsabläufen, indem Tools für das Lebenszyklusmanagement von Schlüsseln und Zertifikaten implementiert und das kryptografische Risikomanagement in die Prozesse zur Reaktion auf Vorfälle und zum Schwachstellenmanagement integriert werden.
- Schritt 2** Verbesserung der Transparenz mithilfe fortschrittlicher Bewertungstools, mit denen Systeme und Netzwerke gescannt werden können, um kryptografische Implementierungen zu identifizieren, die bei manuellen Bestandsaufnahmen möglicherweise übersehen wurden oder anfällig sind.
- Schritt 3** Entwicklung eines hybriden Ansatzes für kritische Daten, die einen sofortigen und langfristigen Schutz erfordern, unter Kombination traditioneller und post-quantensicherer Algorithmen.
- Schritt 4** Beschleunigung der Drittanbieter-Readiness, indem vertragliche Verpflichtungen für die Unterstützung post-quantensicherer Technologien ausgehandelt, bei der Prüfung und Validierung solcher Lösungen mit Lieferantinnen und Lieferanten zusammengearbeitet und die Anforderungen an post-quantensichere Technologien in Dienstleistungsvereinbarungen und Vertragsverlängerungsgespräche einbezogen werden.

Unabhängig vom gewählten Weg lautet das Grundprinzip: Jetzt damit beginnen, nach Risikograd priorisieren und die Post-Quanten-Bereitschaft in bestehende Transformationszyklen integrieren, statt sie als eigenständiges Projekt zu behandeln. Dieser Ansatz vermeidet zwei Extreme: zum einen, nichts zu unternehmen, bis die Bedrohung tatsächlich eintritt, und zum anderen, eine sofortige, umfassende transformative Veränderung vorzunehmen, die unnötige operative Risiken mit sich bringt.





Abschnitt 4

Fazit: Die Finanzinstitute, die jetzt handeln, haben später mehr Möglichkeiten

Die Post-Quanten-Kryptografie (PQC) ist ein technisches Thema, das ein umfassendes Verständnis der damit verbundenen Risiken erfordert. Die FINMA-Umfrage ergab, dass sich zwar die meisten Finanzinstitute der Bedrohung durch Quanteninformatik bewusst sind, jedoch nur wenige dieses Bewusstsein in konkrete Massnahmen umgesetzt haben, um kryptografische Resilienz zu erreichen. Die FINMA-Aufsichtsmittelung schliesst diese Lücke, indem sie fünf Empfehlungsbereiche aufzeigt, die das Engagement der Aufsichtsbehörden für einen sicheren und strukturierten Übergang in das Post-Quanten-Zeitalter zum Ausdruck bringen.

Für einen sichereren Übergang geht es vor allem darum, einen besseren Überblick darüber zu gewinnen, wo Kryptografie zum Einsatz kommt, sowie darum, Krypto-Agilität zu ermöglichen. Die Möglichkeit, kryptografische Algorithmen, Parameter und Implementierungen effizient zu ersetzen, ist bereits heute von grossem Wert, da Finanzinstitute aufgrund der KI-gestützten Erkennung von Sicherheitslücken gefordert sind, diese schneller zu finden und zu beheben.

Finanzinstitute, die frühzeitig mit der Umstellung auf Post-Quanten-Sicherheit beginnen, können die entsprechenden Anforderungen besser in ihre regulären Veränderungszyklen integrieren und so eine spätere, einschneidende und kostspielige Quantenmigration vermeiden.

Kontakt



Florian Widmer
Cyber Partner
fwwidmer@deloitte.ch
+41 58 279 69 10



Christian Daehler
Cyber Partner
cdaehler@deloitte.ch
+41 58 279 52 74



Deloitte.

Together makes progress

Diese Publikation wurde in allgemeiner Form verfasst. Wir empfehlen, vor einer auf den Inhalten dieser Publikation beruhenden Handlung oder Entscheidung fachlichen Rat einzuholen. Deloitte AG haftet nicht für Verluste oder Schäden jeglicher Art, die dadurch entstehen, dass eine Person aufgrund der Inhalte dieser Publikation handelt oder eine Handlung unterlässt.

Deloitte AG ist eine Tochtergesellschaft von Deloitte NSE LLP, einer Mitgliedsunternehmen von Deloitte Touche Tohmatsu Limited, einer britischen Gesellschaft mit beschränkter Haftung in Form einer Garantiegesellschaft («DTTL»). DTTL und ihre Mitgliedsunternehmen sind rechtlich selbstständige und unabhängige Unternehmen. DTTL und Deloitte NSE LLP erbringen selbst keine Dienstleistungen gegenüber Kundinnen und Kunden. Weitere Informationen zu unserem weltweiten Netzwerk von Mitgliedsunternehmen finden Sie unter www.deloitte.com/ch/about.

Deloitte AG ist eine von der Eidgenössischen Revisionsaufsichtsbehörde (RAB) und der Eidgenössischen Finanzmarktaufsicht (FINMA) zugelassene und beaufsichtigte Revisionsgesellschaft.

© 2026 Deloitte AG. Alle Rechte vorbehalten.