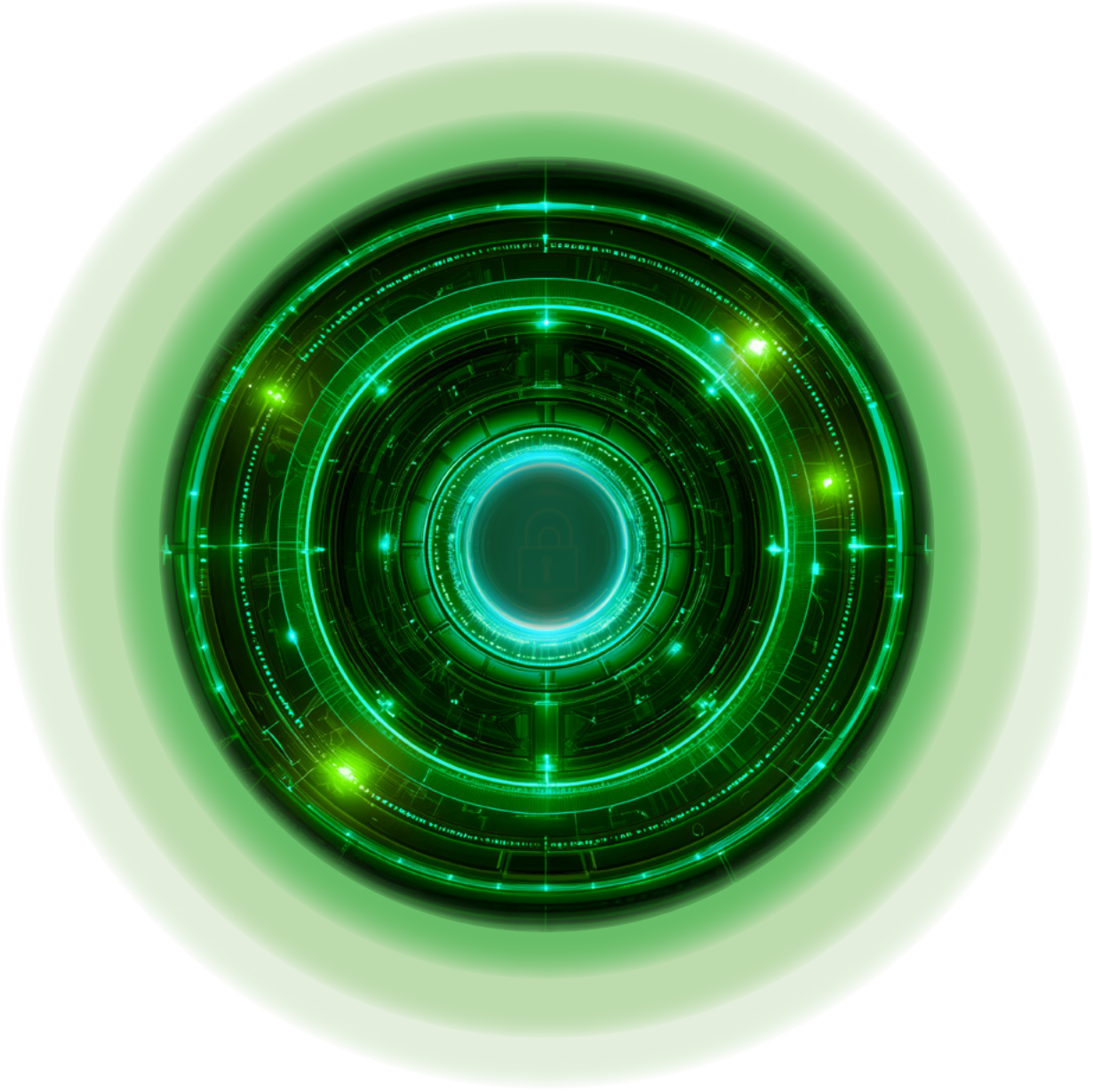
Deloitte.

Together makes progress



Post-quantum readiness for Swiss financial institutions

Cyber Switzerland

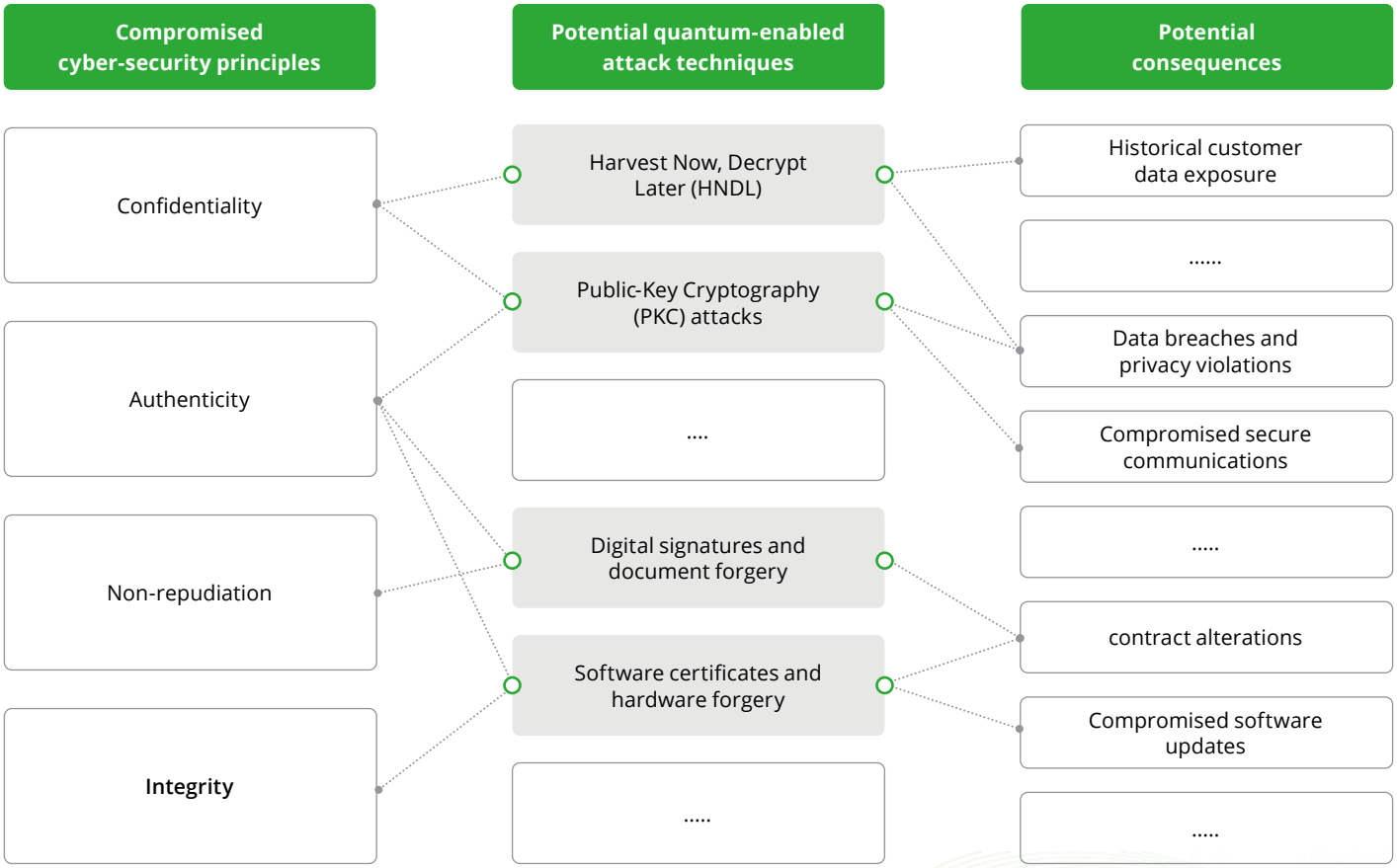
2026

Section 1

FINMA has raised the bar, Swiss based financial institutions should now turn awareness into action

Quantum computing poses an imminent cryptographic threat to financial institutions. Sufficiently powerful quantum computers will undermine today's commonly used Public-Key Cryptography (PKC) that secures a wide range of essential practices, such as digital communications, electronic document signing, software integrity checking, and protecting sensitive data at rest.

Cryptographically relevant quantum computers are not yet on the market, but several risks already exist today. FINMA Guidance 05/2026 specifically highlights "Harvest Now, Decrypt Later" (HNDL) attacks, where encrypted data is collected now and decrypted in the future, once quantum capabilities mature. However, HNDL is not the only concern for financial institutions. Quantum-enabled attacks compromise not only the confidentiality security property, but also the properties of integrity, authenticity and non-repudiation.



The transition to quantum-safe cryptography will be a complex and multi-year effort. The FINMA Guidance 05/2026 makes this point clear by introducing the concept of crypto-agility that extends beyond Post-Quantum Cryptography (PQC). Crypto-agility is the ability to replace cryptographic algorithms, parameters and implementations efficiently when risks, standards or business requirements change. However, achieving a sufficient level of crypto-agility will require time, due to its complexity found in heterogeneous technology landscapes.

As outlined in the FINMA Guidance 05/2026, Swiss financial institutions demonstrate awareness of quantum-related cybersecurity risks, yet many remain at an early stage in translating awareness into concrete action. The transition to quantum-safe cryptography is complex and time-intensive, which is precisely why financial institutions should start now to prioritize impactful actions by risk and build the capabilities required for sustained cryptographic resilience.

Why crypto-agility already matters today: Independent of the post-quantum threat, the ability to adapt cryptography quickly becomes increasingly important, as Artificial Intelligence (AI) accelerates vulnerability discovery and exploitation of software, including vulnerable implementations of cryptographic algorithms. Only crypto-agile organizations can rapidly detect, assess, and remediate cryptographic risks. Non-crypto-agile organizations might take up to several years to remediate such risks, as it has been observed in the case of the SHA-1 remediation.

Section 2

FINMA Guidance changes the conversation from “when will quantum arrive?” to “are we prepared?”

FINMA's survey of 60 Swiss financial institutions reveals a critical gap: while most financial institutions recognize quantum-related cyber risks, few have translated awareness into concrete planning. Only 8% have a specific roadmap, and FINMA expects financial institutions to close this gap by mid-2027 at the latest. Below, five critical actions are proposed based on FINMA's recommendations, each outlining what financial institutions should consider for building cryptographic resilience reaching beyond post-quantum computing threats.

Define a strategy and roadmap

FINMA recommends the transition to quantum-safe encryption to be based on a strategy approved by the board of directors, with an implementation plan setting out milestones and priorities. Target dates should be defined for the complete migration, and separately for critical business processes.

For financial institutions, a concrete and robust strategy should answer the following key questions:

- Which cryptographic risks matter most to our customers, our business partners and our own organization?
- How do these cryptographic risks influence the current and future business and operating model?
- Which business services, applications, data flows and third-party dependencies are in scope?
- Which assets and data require protection beyond the expected quantum threat horizon?
- Which changes can be embedded into existing technology refresh, cloud, core systems, identity, certificate management or cyber resilience programs?
- What decisions are required from executive management and the board?

An actionable roadmap should be risk driven and establish clear direction, ownership, prioritization logic and decision points without the need to prescribe every technical answer upfront

Conduct a risk analysis and build a crypto-inventory

FINMA describes risk analysis and inventory as the first step in the transition. Financial institutions should identify encryption, digital signature and authentication technologies spanning across business processes, IT systems, on-premises infrastructure, cloud services, and third-party integrations.

This is where many organizations underestimate the challenge. Cryptography is often embedded deep inside applications, protocols, certificates, hardware, middleware, cloud services, and workflows. Without an inventory, an organization cannot reliably answer which systems use quantum-vulnerable algorithms, which data is exposed, which third-parties are involved, or where migration will be most difficult.

The inventory should be comprehensive and cover aspects such as:

- encryption of data in transit;
- encryption of data at rest;
- digital signatures;
- authentication mechanisms;
- key management processes;
- certificates and certificate lifecycle management;
- dependencies on third-party software, platforms and managed services;
- cryptographic algorithms potentially vulnerable to quantum attacks.

This inventory should be maintained and updated continuously to reflect changes in systems, applications and third-party dependencies. While this can be an effort intensive undertaking, crypto-agility enabling technologies exist to automate the majority of related activities.

Enabling your crypto-inventory

Phase 1 - Define objectives	Phase 2 - In-scope assets	Phase 3 - Run pilots	Phase 4 - Reporting
Establish clear objectives and use cases tailored to your crypto-agility needs.	Determine the scope, boundaries, and sources of asset and cryptographic data.	Execute a pilot run of a crypto-agility tool to generate insights, identify issues, vulnerabilities and risks.	Report findings and provide next steps.

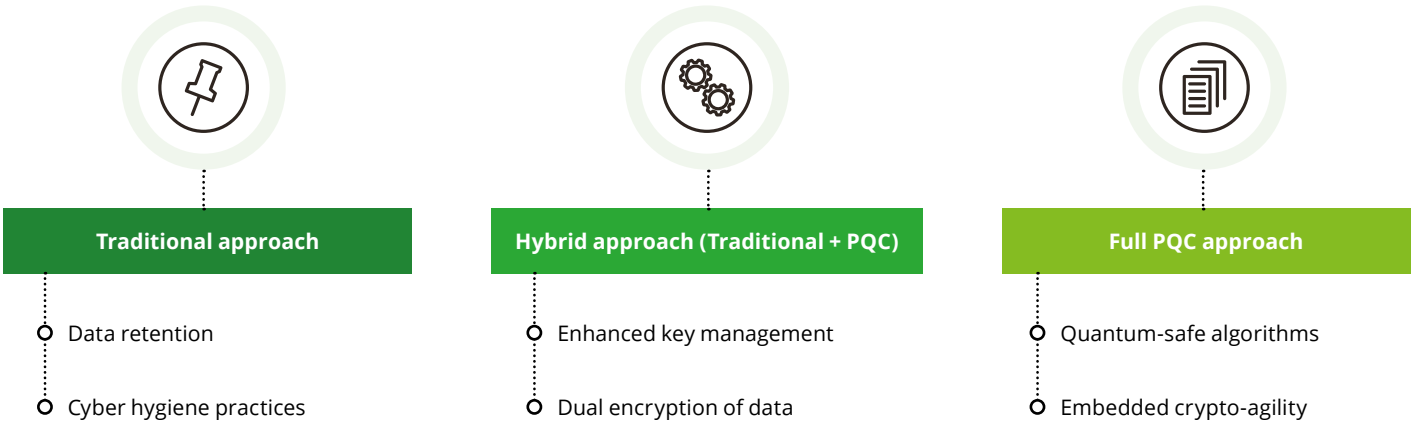
Prioritize critical data and long-term protection needs

FINMA places emphasis on critical data and the "Harvest Now, Decrypt Later" (HNDL) risk. The practical question financial institutions should answer regarding HNDL is: “which data would still create unacceptable harm if decrypted several years from now?”

Financial institutions should therefore identify which data requires long-term confidentiality, integrity, authenticity and non-repudiation. This may include customer records, transaction data, legal agreements, sensitive communications and records subject to long retention periods.

FINMA notes that various organizations recommend hybrid solutions in the short to medium term, combining traditional and post-quantum algorithms. This can provide additional assurance while post-quantum algorithms continue to mature, but it also increases implementation complexity.

Data protection approaches for critical data



Build crypto-agility — not just because of post-quantum risks

Crypto-agility

A crypto-agile organization is one that is fast, flexible and efficient when updating cryptographic algorithms, parameters, processes and technologies.

This helps better respond to new protocols, standards, and security threats, which are not limited to quantum risk.

Benefits

Faster implementation or adjustment of cryptography used across the technology stack, including newly published Post-Quantum Cryptography (PQC) algorithms by National Institute of Standards and Technology (NIST).

More efficiency in cryptographic operations, leading to possible reduction of cost or more effective investment of existing cyber-security resources.

Faster response to cryptographic vulnerabilities and incidents, reducing exposure to regulatory sanctions, customer data breaches, and operational disruplion.

More flexible IT-infrastructure, opening the door to more innovation and implementation of new technologies.

FINMA recommends crypto-agility as a requirement for applications and other IT systems to be procured or developed. Even after post-quantum algorithms are adopted, some may later need to be replaced. Regardless of the advancements of quantum computing, cryptographic weaknesses can arise from weaknesses in the design of the algorithm, poor implementation, outdated libraries, incorrect configurations or vulnerable software supply chains. It is common that from time to time an algorithm or its implementation becomes vulnerable and requires to be replaced. Past examples include SHA-1 (a deprecated hash function), MD5 (a broken cryptographic hash) and RC4 (a compromised encryption cipher), which took some organizations several years to replace because they lacked crypto-agility.

A crypto-agile organization is better positioned to respond when such weaknesses are discovered, whether the trigger is quantum progress, AI-enabled threat activity, a new standard, or a vulnerability in a cryptographic component.

For financial institutions, crypto-agility should be embedded into architecture, procurement, secure development, key and certificate lifecycle management, and technology change governance. It should also become a design requirement for new systems, rather than an afterthought when migration pressure increases.

Engage external service providers and other third-parties early

FINMA explicit states that post-quantum migration will create dependencies on external service providers. This is critical for financial institutions because a large part of cryptographic exposure may sit within externally managed infrastructure, such as core platforms, payment services, cloud environments, and identity providers.

Financial institutions should initiate conversations with external service providers to understand their post-quantum readiness, supported algorithms, product roadmaps, release timelines, and migration dependencies.

Post-quantum and crypto-agility requirements should be integrated into:

- new outsourcing and procurement requirements;
- third-party cyber risk assessments;
- contract renewals and service level discussions;
- architecture and integration standards;
- release planning and testing cycles.

In practice, three things are required:

1. visibility into supplier roadmaps and dependencies;
2. contractual clarity on post-quantum requirements and timelines;
3. influence over release planning to align with the financial institution's migration schedule.

Without these, financial institutions risk being dependent on supplier timelines rather than driving their own post-quantum transition.

To help financial institutions assess supplier readiness, the maturity model below outlines the progression from no formal process to fully integrated post-quantum requirements in third-party management.

Data protection approaches for critical data

Undefined	Manual	Basic	Advanced	Integrated
Does the third-party have any processes for Post-Quantum Cryptography?	Does the third-party utilize spreadsheets to track keys or certificates?	Does the third-party have tools for managing, keys and certificates?	Is automation used to request, deploy and renew certificates?	Are tools and processes integrated with other systems?

Section 3

How to get started and recommended next steps

The first step of a post-quantum programme is to understand where the financial institution stands today by answering to "diagnostic" questions that help to determine which pathway is the most appropriate. Examples of questions include:

- Do you understand which cryptographic risks matter most to your customers, your business partners and your organization?
- Have you analyzed how these cryptographic risks influence your current and future business and operating model?
- Do you have PQC strategy and roadmap approved by the board of directors?
- Have you completed a comprehensive inventory of cryptographic assets across the organization, including third-party dependencies?
- Have you identified which data requires long-term protection?
- Do your procurement and architecture standards require crypto-agility for new systems and outsourcing arrangements?
- Have you engaged key suppliers to understand their post-quantum readiness and product roadmaps?

Based on the answers, one of the two pathways below will be most relevant for a given organization.

Pathway A: Getting started for financial institutions with limited or no post-quantum readiness

If the answer is "no" to most of these questions, the focus should be on establishing the foundation for post-quantum readiness. The following steps provide a structured approach to build the foundations:

Step 1: Establish governance and ownership within the organization and business function.

Step 2: Design the post-quantum roadmap to include milestones, sequencing, decision points, dependencies and target dates, aligning with FINMA's mid-2027 recommendation.

Step 3: Define a risk management framework for identifying, assessing and remediating post-quantum risks.

Step 4: Define the in-scope systems, applications and data, and identify the risks that matter most from a confidentiality, integrity, authentication and resilience perspective.

Step 5: Conduct a diagnostic assessment to understand the breadth and depth of the cryptographic exposure, providing the foundation for prioritizing where to invest in deeper analysis.

Step 6: Build or enhance the crypto-inventory, starting from high-priority environments based on exposure and criticality.

Step 7: Embed crypto-agility to ensure that future changes to cryptographic standards do not require disruptive rework.

Pathway B: Going deeper for financial institutions already in transition

If the answer is "yes" to most of these questions, the foundations are likely established, and the next steps should focus on acceleration, depth and resilience:

- **Step 1:** Embed crypto-agility into operations by implementing key and certificate lifecycle management tools and by integrating cryptographic risk management into incident response and vulnerability management processes.
- **Step 2:** Enhance visibility with advanced assessment tools to scan systems and networks to identify cryptographic implementations that may have been missed in manual inventories or vulnerable.
- **Step 3:** Develop a hybrid approach for critical data requiring immediate long-term protection combining traditional and post-quantum algorithms.
- **Step 4:** Accelerate third-party readiness by negotiating contractual commitments for post-quantum support, by collaborating with suppliers on testing and validation of post-quantum solutions, and by integrating post-quantum requirements into service level agreements and renewal discussions.

Regardless of the pathway, the underlying principle is to start now, prioritize by risk, and integrate post-quantum readiness into existing transformation cycles rather than treating it as a standalone project. This approach avoids two extremes: doing nothing until the threat materializes or attempting an immediate full-scale transformation that creates unnecessary operational risk.

Section 4

Conclusion: The financial institutions that start now will have more options later

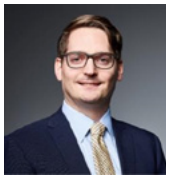
Post-Quantum Cryptography (PQC) is a technical topic that requires a robust understanding of the risks it introduces. The FINMA survey revealed that while most financial institutions recognise the quantum threat, few have translated awareness into concrete action to strive for cryptographic resilience. FINMA Guidance addresses this gap by outlining five recommendation areas, reflecting regulators' commitment to supporting a safe and structured transition to the post-quantum era.

For a safer transition, the priorities are to build better visibility on where cryptography is used and to enable crypto-agility. The ability to replace cryptographic algorithms, parameters and implementations efficiently is valuable already now, as AI-enabled vulnerability discovery requires financial institutions to be faster in finding and patching vulnerabilities.

Financial institutions that start the post-quantum journey early will be better positioned to integrate post-quantum requirements into normal change cycles rather than force a disruptive and costly quantum-migration later.

Get in touch

Florian Widmer
Cyber Partner
fwwidmer@deloitte.ch
+41 58 279 6910



Christian Daehler
Cyber Partner
cdaehler@deloitte.ch
+41 58 279 5274

Deloitte.

Together makes progress

Designed by CoReCreative Services. RITM2587457