comply

INDUSTRY REFERENCE PAPER
AUGUST 2026

BANKING SECTOR · QUANTUM-SAFE CRYPTOGRAPHY

A Quantum-Safe Migration Roadmap for a Swiss Bank

What supervisors now expect a Swiss bank to have in place, what the migration actually involves, and who inside the organisation owns each part of it. A reference architecture, and a three-phase plan that starts with a scan.

72%
of 60 surveyed Swiss financial institutions had planned or implemented no quantum-safe measures

8%
had a specific roadmap for quantum-safe encryption

10 months
from this paper to FINMA's recommended date for a PQC roadmap

2030–32
G7 window for migrating the financial sector's most critical systems

Sources: FINMA Guidance 05/2026 (9 July 2026); G7 Cyber Expert Group, January 2026. Full source list on page 9.

Ten months to the roadmap date. The inventory takes longer than that

Two clocks run against a Swiss bank. FINMA wants a post-quantum roadmap drawn up by mid-2027 — ten months from the date on this paper.[1] The bank's own data runs on the longer clock: anything encrypted this morning that must stay confidential into the 2040s can be captured today and decrypted later.[1,2] This page carries the argument in full; the rest of the paper is the evidence underneath it.

01 · Where the sector is

Almost nobody has started

FINMA surveyed 60 authorised institutions. 72% had planned or taken no quantum-safe measures; 8% held a specific roadmap.[1] Being behind the curve is the norm here. It is not a defence, and it will not read as one in an audit file.

→ PAGE 4 · THE CLOCK

02 · Why "not binding" is not "not yet"

The obligations already bite

No supervisor has issued a binding quantum-safe rule for banks. DORA's technical standards already require monitoring of cryptographic threats including quantum advances, and FINMA holds that its governance principles already reach quantum risk.[1,6] Guidance dates become audit dates.

→ PAGE 5 · REGULATORY PRESSURE

03 · The critical path

Discovery is the long pole, and it starts now

The roadmap due by mid-2027 cannot be written without an inventory of the cryptography actually in use. NCSC sets a *completed* discovery phase at 2028 — a completion date, not a starting gun.[3] Scanning does not wait on the board decision; it is the input that decision needs.

→ PAGES 6 AND 7

04 · Scope

Most of the estate belongs to somebody else

Responsibility for an outsourced function stays with the bank. FINMA recommends crypto-agility as a prerequisite in all new outsourcing arrangements for software and data.[1] Vendor PQC roadmaps take a procurement cycle to extract, which is why the contract clause is a Phase 1 item, not a Phase 3 one.

→ PAGE 7 · THIRD PARTIES

05 · The real failure mode

Ownership, not disagreement

Nobody in these conversations argues the threat is imaginary. What is missing is a named accountable executive sitting between the CISO who can see the exposure and the business unit that would have to fund the change.

→ PAGE 8 · ACCOUNTABILITY

06 · What the evidence supports

Feasible, but not free

BIS Project Leap put post-quantum signatures through TARGET2 liquidity transfers with four central banks and Swift. Every scenario passed — after numerous components were modified, and with signatures roughly 13× larger inside the ISO 20022 header.[7,8] Treat that as capacity planning, not as a blocker.

→ PAGE 7 · A LIVE PAYMENTS TEST

The one thing to take from this page: start scanning now

A cryptographic inventory is the only deliverable here that cannot be compressed, and it feeds every other one — the risk analysis, the roadmap itself, the target dates, the contract clauses, the tiering. Ten months remain before FINMA's date. A bank that opens discovery in 2027 will arrive at mid-2027 with a roadmap it cannot evidence.

WHAT GOOD LOOKS LIKE TWELVE MONTHS FROM NOW

A board-approved quantum-safe strategy with one named owner and funding across two investment cycles. A machine-readable cryptographic inventory that refreshes itself. A register of the data that has to outlive RSA, with owners against each entry. Crypto-agility written into every software and data contract signed since today. **The first ninety days are set out on page 8.**

If you can answer these nine questions, you can stop reading here

Every question below is answered somewhere in the pages that follow. Most institutions can answer two or three of them without opening a file. The remainder are where the work sits, and the page references take you straight to it.

01	**Which systems in your estate are running RSA-2048 this morning — and could you produce that list by Friday?** Discovery is the gate every published roadmap puts first, and the only one that cannot be shortened by spending more.	**p.7** Discovery, tiering and third parties
02	**How much of what you encrypted this morning still has to be secret in 2040?** Harvest now, decrypt later turns today's captured traffic into a breach dated whenever a CRQC arrives. FINMA calls the risk already very real.	**p.4** The clock
03	**FINMA wants the roadmap by mid-2027. When does the inventory that feeds it have to begin?** Ten months remain. Whatever the answer is, it is not 2027.	**p.6** The roadmap
04	**No supervisor has issued a binding quantum-safe rule. Does that leave you unexposed?** DORA's technical standards already name quantum advances, and five regimes converge on the same three dates.	**p.5** Regulatory pressure
05	**Who owns quantum risk by name — and does the budget sit with the same person?** The gap is almost always between the CISO who sees the exposure and the business that would fund the change.	**p.8** Accountability
06	**Your core banking platform is a vendor product. Do you hold its PQC roadmap, or only its assurance that one exists?** Responsibility for an outsourced function does not transfer with the function. Smaller institutions carry the highest vendor dependency.	**p.7** Third parties
07	**Post-quantum signatures grew an ISO 20022 message header roughly 13×. Are your buffers sized for that?** BIS Project Leap passed every test scenario — and had to modify numerous system components to get there.	**p.7** A live payments test
08	**If the board asked today for your target date for full migration, what date would you give?** FINMA leaves the target dates to the institution. That is the part most institutions find hardest to answer.	**p.6** The roadmap
09	**Which numbers in this paper are sourced, and which are worked examples?** Five of the ten sources were read in full as primary documents. The paper says which, and marks the rest.	**p.9** Evidence base

How to read the rest of this paper

Sections 03 to 05 establish the deadlines and the plan; sections 06 and 07 are the operational detail a programme team will need. If you have twenty minutes, read page 2 and page 6. If you have five, read page 2.

Two deadlines, and only one of them is a compliance date

A bank faces two independent clocks. The first is regulatory: supervisors have published dates by which cryptography must be inventoried, prioritised and replaced. The second is the shelf life of the bank's own data. Encrypted traffic captured today can be stored and decrypted once a cryptographically relevant quantum computer (CRQC) exists — the "harvest now, decrypt later" scenario. FINMA names this as an *already very real risk* and asks institutions to give priority to data that must stay protected in the long term.[1] The G7 Cyber Expert Group puts it the same way: data may be at risk even if it is intercepted well before a CRQC emerges.[2]

Where the exposure sits

Any record whose confidentiality or non-repudiation must survive past the arrival of a CRQC is exposed today. Around two-thirds of the institutions FINMA surveyed expect a quantum computer to break RSA-2048 within 24 hours inside ten years at the latest.[1]

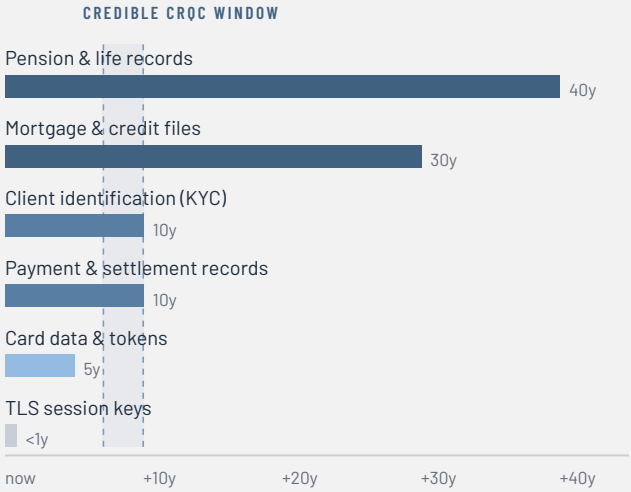

Figure 1. Retention periods are *illustrative planning figures*, not sourced — replace them with your own retention schedule. The shaded band marks the seven-to-ten-year arrival expectation reported by FINMA's respondents,[1] not a prediction. Any bar that crosses it is exposed to capture today.

Where the sector actually is

FINMA surveyed 60 authorised banks, insurers, asset managers and financial market infrastructures between November 2025 and January 2026. Awareness was high. Execution was not.[1]

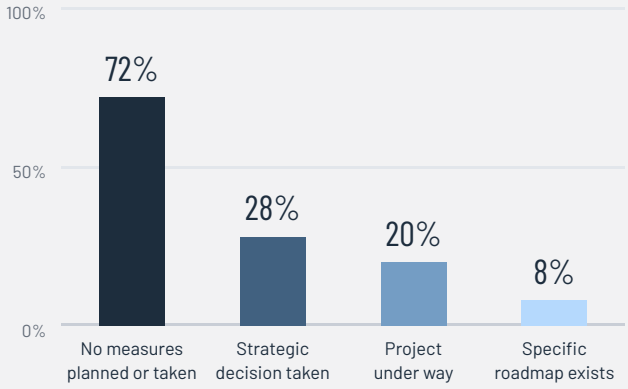

Figure 2. FINMA Guidance 05/2026, survey of 60 Swiss financial institutions, Nov 2025 – Jan 2026. Categories overlap: the 20% with a live project are a subset of the 28% that had taken a strategic decision.[1]

> "In most cases… there is a lack of a clear roadmap and sufficiently forward-looking planning for the migration to quantum-safe encryption. FINMA considers that action is needed in the risk management process of numerous institutions."
>
> FINMA GUIDANCE 05/2026, 9 JULY 2026[1]

Five regimes, one converging set of dates

No supervisor has yet issued a binding quantum-safe rule for banks. What exists instead is guidance layered on technology-neutral obligations that already bite. DORA's technical standards require financial entities to monitor cryptographic threats *including threats from quantum advancements*,[6] and FINMA holds that its governance and risk-management principles already cover quantum risk.[1] The dates below are planning anchors — and the dates auditors, procurement and insurers will read against.

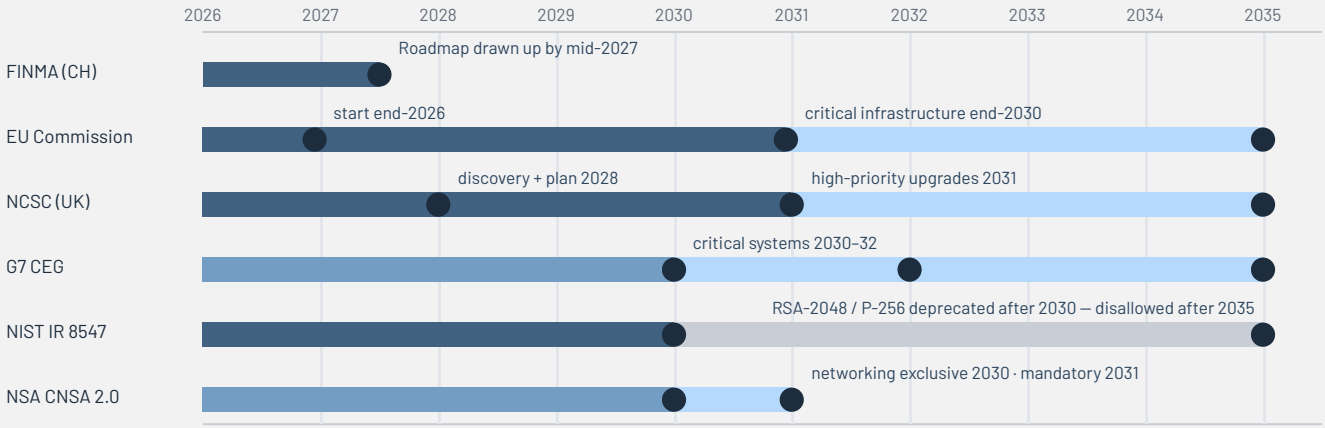

Figure 3. Published milestones, as at August 2026. Solid marks are dates stated in the source documents; bar extents are drawn to those dates and are not themselves prescriptive. Sources 1–5 and 10.

INSTRUMENT	STATUS	WHAT IT ASKS A BANK TO DO	KEY DATES
FINMA Guidance 05/2026 Switzerland	Recommendation under binding principles	Board-adopted PQC strategy with an implementation plan; risk analysis of cryptography in use and of long-lived data; a continuously updated cryptographic inventory; hybrid protection for critical data; crypto-agility in procurement and outsourcing contracts.[1]	Roadmap by **mid-2027**; migration target dates set by the institution
DORA + RTS 2024/1774 EU	Binding	ICT risk management including encryption and key-management policy, a certificate register for critical or important functions, and monitoring of cryptographic developments — explicitly including quantum advances.[6]	In force since **Jan 2025**
EU coordinated PQC roadmap Rec. (EU) 2024/1101 + NIS CG	Non-binding; binding acts held in reserve	Member States to begin transition, secure high-risk systems including critical financial infrastructure, then complete as far as practically feasible. Endorses hybrid PQ/classical deployment.[5]	Start **end-2026** · critical **end-2030** · complete **2035**
NCSC migration timelines UK, March 2025	Guidance	Three phases: full discovery of cryptographic assets and dependencies plus an initial plan; highest-priority upgrades with the plan refined as PQC matures; then full migration across systems, services and products.[3]	**2028 · 2031 · 2035**
NIST IR 8547 US, initial public draft	Draft; not finalised as at mid-2026	Names the algorithms to retire (RSA, ECDSA, ECDH, DSA, FFDH) and the FIPS 203/204/205 replacements; supports hybrid during transition.[4]	112-bit strength **deprecated after 2030**, **disallowed after 2035**
G7 CEG roadmap Financial sector, Jan 2026	Not guidance or a regulatory expectation	Six migration activities from awareness through validation, with three continuous lines of effort: governance and risk management, management of external dependencies, and stakeholder dialogue.[2]	Critical systems **2030–32**; overall horizon **2035**

Three phases, two of which have to start this quarter

The plan below compresses the published timelines into the window a bank can actually govern: mandate and evidence together, then execution on the systems that matter. Discovery runs from today rather than from the board decision, because it does not depend on one. The G7 notes that migration activities are not linear and that many run in parallel;[2] NCSC frames migration as an effort spanning more than one investment cycle.[3]

Figure 4. Reference plan, drawn from August 2026. Phase 1 and Phase 2 open together by design: the inventory is an input to the strategy, not an output of it. Structure follows the G7 CEG's six activities;[2] the August start is our own reading of what the mid-2027 deadline requires, not a sourced instruction.

2028 is a completion date, not a starting gun

NCSC's first milestone is a *finished* discovery phase and an initial migration plan by 2028.[3] FINMA wants the roadmap drawn up by mid-2027.[1] Neither is reachable by opening discovery in 2027. Across an estate of any size a first inventory pass runs into quarters, not weeks, and it is the input the board needs before it can set the target dates FINMA leaves to the institution. Scanning is the only item on this page with nothing in front of it.

PHASE 1 · NOW TO MID-2027

Mandate

Get the decision made at the level that can fund it. FINMA expects the strategy to be adopted by the board of directors, with an implementation plan setting out milestones and priorities derived from it.[1]

- Board-approved quantum-safe strategy, or a named section inside the existing cyber-risk strategy
- Accountable executive named; programme funded across at least two investment cycles
- Quantum risk added to the risk taxonomy and risk-appetite statement
- Target dates set for critical business processes and for full migration

EXIT TEST: A SUPERVISOR ASKING "WHO OWNS THIS AND BY WHEN" GETS ONE ANSWER

PHASE 2 · STARTS NOW → 2028

Evidence

Discovery is the gate every published roadmap puts first, and the one that cannot be compressed. It is also the only phase that can begin before the mandate exists — and it should.[3]

- Cryptographic inventory across all ICT systems and infrastructure — in-house, outsourced and as-a-service
- Machine-readable CBOM, refreshed continuously, not a one-off spreadsheet
- Long-lived data register: what must stay confidential, and for how long
- Systems tiered by quantum risk; per-tier migration plans proportionate to risk

EXIT TEST: EVERY QUANTUM-VULNERABLE ALGORITHM IN PRODUCTION HAS A NAMED SYSTEM AND OWNER

PHASE 3 · 2028–2030

Execution

Critical systems first. The G7 puts the migration of the most critical systems in 2030–32 to limit the downside if the threat lands early;[2] the EU roadmap puts critical infrastructure at end-2030.[5]

- Hybrid key exchange on external-facing channels and long-lived data at rest
- PKI re-keyed: root and issuing CAs, code signing, e-signature and archival timestamps
- Payment, custody and settlement interfaces migrated with counterparties, not alone
- Migrated functions tested; quantum-resilience added to scenario and crisis exercises

EXIT TEST: NO CRITICAL BUSINESS PROCESS DEPENDS ON RSA OR ECC ALONE

You cannot migrate what you cannot see

76% of FINMA's respondents rated a cryptographic inventory as high or very high value, and 73% said the same of crypto-agility.[1] FINMA is explicit about scope: encryption in transit and at rest, digital signatures, key management and authentication mechanisms, across all ICT systems, applications, infrastructure and distributed-ledger use, whether operated in-house, outsourced or consumed as a service.[1]

The inventory as a machine-readable artefact

A spreadsheet decays the week it is finished. The sector convention is a Cryptography Bill of Materials — algorithms, key sizes, certificates, protocols and libraries, plus the components that invoke them — standardised in CycloneDX 1.6 and now carried in Ecma International ECMA-424.[9] NIST's NCCoE practice guide SP 1800-38B treats cryptographic discovery as the prerequisite for migration and identifies the CBOM as its output.[9]

DISCOVERY LAYER	WHAT IT SURFACES — AND MISSES
Network / TLS scanning	Live protocol and cipher use at the perimeter; blind to internal batch and at-rest crypto
Source and dependency scan	Algorithm calls and library versions; blind to runtime configuration
Binary and container scan	Embedded crypto in images and third-party builds; noisy without triage
Certificate and key inventory	PKI hierarchy, expiry, key algorithms; needs HSM and CA cooperation
Vendor attestation	Crypto inside SaaS and appliances — the only route where you have no code

Layered scanning is the practical approach for an estate of any size; no single layer is sufficient. The coverage claim for each layer is our assessment, not a sourced figure.

Tiering: shelf life against effort

The G7 is explicit that not all systems face the same exposure, and that entities may run aggressive timelines on critical areas and extended ones elsewhere, using non-critical systems as early pilots.[2] Two axes are enough to sequence the work.

DATA SHELF LIFE · LONGER AT TOP

	low	medium	high
30y+ long	**Archived client records at rest** HYBRID NOW	**e-signature & timestamping** HYBRID NOW	**Core banking & custody keys** START EARLY
5–15y medium	**Internal VPN & admin access** PILOT HERE	**Payment & settlement links** WITH COUNTERPARTIES	**Cards, HSMs, terminals** VENDOR-LED
<2y short	**Public web TLS** AVAILABLE TODAY	**Session & token services** ROTATION COVERS IT	**Legacy batch & mainframe** DEFER, REPLACE

EFFORT →

Figure 5. Illustrative placement for a generic bank. The axes and the sequencing logic follow the G7's risk-based approach;[2] the cell contents are our own worked example. The blue outline marks the priority band: everything whose confidentiality has to outlive the credible CRQC window.

Third parties are most of the estate

Responsibility for an outsourced function stays with the outsourcing institution. FINMA recommends making crypto-agility a prerequisite for all new outsourcing arrangements in software and data, and folding it into existing arrangements at the earliest opportunity — planning the change into the provider's normal release cycles rather than raising it as an exception.[1] 60% of respondents were already in contact with software suppliers or planned to be.[1] The G7 notes that detailed vendor roadmaps for cloud and cryptographic services can be essential to planning, and that smaller institutions carry the highest vendor dependency.[2]

What a live payments test showed

BIS Project Leap Phase 2 replaced conventional digital signatures with post-quantum signatures on liquidity transfers in the Eurosystem's TARGET2 environment, with Banca d'Italia, Banque de France, Deutsche Bundesbank, Nexi-Colt and Swift. All test scenarios passed. The tests also revealed significant performance differences between traditional and post-quantum algorithms, and numerous system components had to be modified for compatibility.[7] Independent analysis of the report puts the signature growth inside the ISO 20022 message header at roughly 13× — 3,293 bytes against 256 for RSA-2048 — exceeding expected buffer sizes.[8] Read it as a capacity-planning warning, not a blocker.

Named roles, not a programme in search of an owner

The G7's first migration activity is executive-level risk awareness, an initial post-quantum resilience strategy, and *defined key roles*.[2] FINMA locates the strategy at board level and leaves target dates to the institution.[1] In practice the failure mode is not disagreement about the threat. It is that no single accountable owner exists between the CISO who sees the exposure and the business that funds the change.

ROLE	ACCOUNTABLE FOR	EVIDENCE A SUPERVISOR OR AUDITOR CAN ASK FOR
Board / risk committee	Approving the quantum-safe strategy; setting risk appetite and target dates; funding across investment cycles	Minuted approval of the strategy; quantum risk visible in the risk taxonomy and appetite statement
CEO / ExCo sponsor	Naming the accountable executive; resolving contention between the programme and the change portfolio	Programme mandate with named owner, budget and milestones
CISO	Threat and exposure assessment; the long-lived-data register; hybrid protection decisions	Risk analysis covering both algorithms in use and data needing long-term protection
Head of cryptography / PKI	The cryptographic inventory and CBOM; algorithm standards; PKI re-keying and certificate automation	Continuously updated inventory; documented crypto standard naming FIPS 203/204/205 targets
CIO / CTO	Crypto-agility in architecture and procurement; migration delivery and testing	Crypto-agility as a stated requirement in new build and buy; test results for migrated functions
CRO / compliance	Regulatory mapping across jurisdictions; challenge and independent validation	Mapping of applicable dates per entity and jurisdiction; second-line review of the plan
Head of sourcing / vendor mgmt	Crypto-agility clauses; provider PQC roadmaps; interface dependency register	Clause in all new software and data outsourcing; documented provider roadmaps
Internal audit	Assurance over inventory completeness and programme progress	Audit opinion on the inventory and on the Phase 1 and Phase 2 exit criteria

The first ninety days

01 · Scan

Open discovery on two or three critical business processes. It needs no board decision, and its output is what the board decision is written from.

02 · Decide

Take the strategic decision at board or ExCo level and name one accountable executive with the budget attached.

03 · Register

List the data that must stay confidential or non-repudiable beyond ten years, with an owner against each entry.

04 · Contract

Add crypto-agility and a PQC roadmap commitment to every software and data contract now in negotiation.

Where every figure in this paper comes from

Five of the ten sources below were read in full as primary documents. The rest are reported through secondary analysis and are marked as such. Where sources disagree, the disagreement is stated rather than resolved.

1. FINMA, *Guidance 05/2026: Quantum computing*, 9 July 2026. finma.ch
2. G7 Cyber Expert Group, *Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector*, January 2026. home.treasury.gov
3. NCSC, *Timelines for migration to post-quantum cryptography*, March 2025. ncsc.gov.uk
4. NIST, *IR 8547 (initial public draft): Transition to Post-Quantum Cryptography Standards*, November 2024. nvlpubs.nist.gov
5. Commission Recommendation (EU) 2024/1101 and the NIS Cooperation Group coordinated implementation roadmap, June 2025, as summarised in Cryptomathic's compliance review and PostQuantum.com. Secondary source.
6. DORA (Regulation (EU) 2022/2554) and Commission Delegated Regulation (EU) 2024/1774 on ICT risk-management tools; quantum wording as reported by PostQuantum.com. Secondary source.
7. BIS Innovation Hub, *Project Leap phase 2: quantum-proofing payment systems*, 11 December 2025. bis.org
8. Independent analysis of the Project Leap Phase 2 report, PostQuantum.com, 2026. Secondary source; the byte figures are not quoted from the BIS report itself.
9. CycloneDX CBOM (ECMA-424) and NIST NCCoE SP 1800-38B, *Migration to Post-Quantum Cryptography*. cyclonedx.org · nccoe.nist.gov
10. NSA CNSA 2.0 category milestones, as summarised by The Quantum Insider, May 2026. Secondary source.

Confidence note

Sources 1, 2, 4, 7 and 9 are primary documents read in full. Sources 5, 6, 8 and 10 are reported through secondary analysis and should be confirmed against the primary text before use in a regulatory submission. Reporting in mid-2026 also describes new US federal instruments — an executive order and an OMB memorandum tightening the 2030 date — but secondary sources disagree on their identifiers and we could not verify them against a primary text, so they are excluded from Figure 3. Retention periods in Figure 1, the placements in Figure 5 and the August 2026 start date in Figure 4 are worked examples and our own reading, not sourced data.