PANOP

PANOP RESEARCH · AWARENESS BRIEFING

Post-Quantum Cryptography: Swiss and EU Deadlines

An awareness briefing on the regulatory timetable for the post-quantum transition in Switzerland and the European Union: what the EU coordinated roadmap expects and when, what FINMA now requires of supervised institutions, how ANSSI, BSI, the UK NCSC and NIST differ on hybrid cryptography and dates, and the ninety days of work that every one of those roadmaps starts with.

EDITION SEPTEMBER 2026

PANOP RESEARCH · PANOP.IO

PANOP

01 · EXECUTIVE SUMMARY

The quantum question stopped being if, and became by when

Nobody has a cryptographically relevant quantum computer. Several authorities now have deadlines, and two of them apply directly to organisations operating in Switzerland and the European Union. On 3 September 2026 the G7 Cyber Security Working Group, chaired by France's ANSSI and supported by the European Commission and ENISA, published *Preparing for the Post-Quantum Era: A Call to Action*, arguing that the threat has to be reframed from a distant future problem into a near-term one concerning every sector rather than critical infrastructure alone.

THE POSITION IN ONE PARAGRAPH

Public-key cryptography protects data in transit today, and an adversary can record that traffic now and decrypt it once a quantum computer exists. That is why the deadline is not the arrival of the machine. Any data whose confidentiality must outlast it is already exposed at capture time, and the migration of public key infrastructure and long-lived devices takes years. The regulatory response is a set of planning deadlines falling in 2026 and 2027, and migration deadlines for sensitive systems falling in 2030.

8%
Swiss financial institutions with a specific quantum-safe roadmap
FINMA survey of 60 institutions, 2025

43%
Of those institutions had taken no decision at all
FINMA survey of 60 institutions, 2025

mid-2027
FINMA milestone for a board-approved PQC roadmap
FINMA Guidance 05/2026

2030
EU target for migrating high-risk use cases
NIS Cooperation Group, 2025

THE TWO INSTRUMENTS THAT APPLY DIRECTLY

The EU coordinated roadmap

A Commission recommendation, not binding on private entities, but it sets **end-2026** for national roadmaps and **end-2030** for high-risk use cases. It sits on top of NIS2 and DORA cryptography duties that already bind, and the Cyber Resilience Act, which applies to products from December 2027.

FINMA Guidance 05/2026

A supervisory communication rather than new law, on the view that Switzerland's principles-based operational-risk requirements already cover quantum risk. It expects a PQC strategy **adopted by the board by mid-2027**, and says the topic will feature more prominently in ongoing supervision.

WHAT LEADERSHIP HAS TO DECIDE

01 **Which of our data must stay confidential past 2035?**
That answer sets the migration order. It is a business question about retention and sensitivity, not a cryptographic one.

02 **Do we have a cryptographic inventory?**
Every roadmap in this briefing depends on one, and most organisations have no consolidated view of which algorithms, keys and certificates are used where.

03 **Who owns the transition?**
A multi-year programme spanning PKI, TLS, code signing, identity and procurement needs a named owner and a board-level reporting line, not a distributed best effort.

04 **What are our suppliers doing?**
A large share of cryptographic exposure sits in infrastructure you do not run, so their product roadmap is your migration constraint. FINMA asks for that engagement explicitly.

05 **Are we buying tomorrow's legacy today?**
Procurement is the cheapest lever available. ANSSI has stated it will not be reasonable to buy products without post-quantum support after 2030.

The gap. The instruments are not comparable — state roadmaps, supervisory guidance, procurement gates and product regulation all behave differently — but the band is unmistakable. Planning work is due in 2026 and 2027. Migration of anything sensitive is due by 2030.

SOURCES G7 Cyber Security Working Group and CISA, Preparing for the Post-Quantum Era: A Call to Action, 3 September 2026. FINMA Guidance 05/2026, 9 July 2026. NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23 June 2025. Full references on page 9.

PANOP

02 · WHAT WE ARE ACTUALLY TALKING ABOUT

Five terms that decide how urgent this is

The vocabulary matters here, because the difference between a severity debate and a hard deadline sits inside two of these definitions.

PLAIN-LANGUAGE GLOSSARY

Cryptographically relevant quantum computer (CRQC)
A fault-tolerant quantum computer large enough to run Shor's algorithm against real key sizes, breaking RSA and elliptic-curve cryptography. None exists publicly. Germany's federal government works on the planning hypothesis that one may exist in the early 2030s — explicitly a risk-assessment reference point rather than a forecast.

Harvest now, decrypt later (HNDL)
Also called store-now-decrypt-later. An adversary records encrypted traffic today and decrypts it once a CRQC exists. This is why the deadline is not "whenever quantum computers arrive". Any data whose confidentiality must outlast the CRQC is already exposed, today, at the moment of capture.

Hybrid
Combining a post-quantum algorithm with a classical one so the result holds if either component is broken. European authorities lean strongly toward it and ANSSI makes it mandatory for certified products, while the US NSA treats standalone post-quantum cryptography as sufficient. It is the single largest divergence between jurisdictions.

Crypto-agility
Designing systems so a cryptographic algorithm can be swapped without re-architecting. It is the property that makes the *next* transition cheap, and most current guidance treats it as the real deliverable rather than any single algorithm replacement. In the FINMA survey, 73% of institutions rated it important or very important.

Cryptographic inventory
The record of which algorithms, keys and certificates are used where, increasingly expressed as a Cryptographic Bill of Materials (CBOM). Every roadmap in this briefing depends on one, and the G7 working group recommends building it outward from the asset inventory an organisation already maintains rather than as a greenfield exercise.

WHY THE DEADLINE DOES NOT WAIT FOR THE HARDWARE

Two independent lines of reasoning arrive at the same place. HNDL makes today's traffic a future liability, so the clock started when the data was captured. Separately, even with no adversary at all, public key infrastructure and long-lived devices take years to move, so the transition has to finish before the threat lands rather than when it does.

STEP 01
Capture today
Traffic is recorded now, while the protection on it is still classical.

→

STEP 02
Store
The adversary simply waits. No detection event occurs on your side.

→

STEP 03
CRQC arrives
Everything recorded becomes readable retroactively, at once.

→

STEP 04
Long migration
Independently, PKI and embedded devices may simply not finish in time.

Why it matters. HNDL converts a future capability into a present obligation, and migration duration converts that obligation into a multi-year programme. Neither argument depends on knowing when a quantum computer will actually exist, which is why every authority in this briefing sets dates without forecasting the hardware.

SOURCES BSI, study on the status of quantum computer development. German Federal Government, Bundestag Drucksache 20/8104. FINMA Guidance 05/2026. G7 Cybersecurity Working Group statement on preparing for a post-quantum cryptography migration. AIVD, CWI and TNO, The PQC Migration Handbook.

PANOP

03 · THE STANDARDS

The replacements exist, and the retirement date is set

NIST published the three principal standards on 13 August 2024. They are production-ready today, which removes the last technical argument for not planning.

THE THREE PUBLISHED STANDARDS

FIPS 203 — ML-KEM

Key encapsulation, derived from Kyber. The replacement for RSA key transport and elliptic-curve Diffie–Hellman.

NIST, 13 August 2024

FIPS 204 — ML-DSA

Digital signatures, derived from Dilithium. The general-purpose default for signing.

NIST, 13 August 2024

FIPS 205 — SLH-DSA

Hash-based signatures, derived from SPHINCS+. The conservative backup, resting on very different mathematics.

NIST, 13 August 2024

FIPS 206, standardising Falcon as FN-DSA, remains in development, and HQC was selected in March 2025 as a second key-encapsulation mechanism on a roughly two-year track. The backups are not redundancy for its own sake: a single algorithm family failing to cryptanalysis is precisely the scenario that hybrid deployment and crypto-agility exist to survive.

THE RETIREMENT SCHEDULE

STATUS	FROM	WHAT IT MEANS IN PRACTICE
Deprecated	**After 2030**	RSA, ECDSA, EdDSA and finite-field or elliptic-curve Diffie–Hellman should not be selected for new systems, and existing use needs a documented migration plan.
Disallowed	**After 2035**	No longer approved for the stated purpose. A disallowed signature scheme is treated as forgeable, and a disallowed key-establishment scheme as vulnerable to key recovery.

This schedule sits in **NIST IR 8547**. It is worth being precise when quoting it in a policy document: IR 8547 is still an initial public draft, published 12 November 2024, and its dates could change. They are nonetheless the de facto planning baseline that the EU roadmap, the UK NCSC timeline and US federal policy all anchor to.

WHERE THE REAL CONSTRAINTS SIT

Protocols — TLS 1.3 or nothing

Post-quantum key establishment exists only in TLS 1.3 and later. Anything still negotiating TLS 1.2 or below cannot be migrated at all until the protocol is upgraded, which makes protocol inventory a prerequisite rather than a parallel task.

Signing and updates

Code signing and firmware update chains have to be migrated before the devices that depend on them. Under the Cyber Resilience Act, a device that cannot receive a quantum-safe-signed update is a device that cannot be migrated later.

Public key infrastructure

Certificate hierarchies, key lengths and signature algorithms change together and take years to roll. Switzerland's FOITT is already migrating the Swiss Government PKI across certificate classes for this reason.

Suppliers and hardware

Hardware security modules, network appliances and embedded estates move on vendor timelines. This is the exposure FINMA singles out, because much of a bank's cryptography sits in infrastructure it does not operate.

> **The practical read.** Algorithm availability is no longer the constraint. Inventory, protocol support and supplier readiness are, and all three are discovery problems before they are cryptography problems.

SOURCES NIST, FIPS 203, FIPS 204 and FIPS 205, 13 August 2024. NIST IR 8547, Transition to Post-Quantum Cryptography Standards, initial public draft, 12 November 2024. NIST IR 8545, Status Report on the Fourth Round, March 2025. G7 Cybersecurity Working Group statement. FINMA Guidance 05/2026.

PANOP

04 · THE EUROPEAN PICTURE

A recommendation with dates, on top of law without them

Two distinct layers operate here, and conflating them is the most common mistake in this area. The post-quantum timetable is a recommendation. The duties it leans on are already binding.

THE COORDINATED ROADMAP: THREE MILESTONES

MILESTONE 1

31 Dec 2026

Every Member State has a national PQC roadmap, has implemented the First Steps, and has begun pilots and high-risk migration.

→

MILESTONE 2

31 Dec 2030

High-risk use cases fully transitioned, quantum-safe upgrades enabled by default, Next Steps implemented.

→

MILESTONE 3

31 Dec 2035

Transition complete for as many medium- and low-risk systems as is feasible.

The Commission adopted Recommendation (EU) 2024/1101 on 11 April 2024, and the resulting NIS Cooperation Group work stream — co-chaired by France, Germany and the Netherlands — published the roadmap on 23 June 2025. It is explicit that for high-risk use cases, quantum-vulnerable public-key mechanisms "shall not be used stand-alone" after the end of 2030, and after the end of 2035 for medium-risk ones. Where migration happens it recommends standardised, tested hybrid solutions. A Commission recommendation is not binding on private entities, and the roadmap describes its own measures as "no-regret" moves that support compliance with law that is.

THE LAYER THAT ALREADY BINDS

NIS2 — Directive (EU) 2022/2555

Requires in-scope entities to adopt risk-management measures including policies on the use of cryptography, and makes management bodies liable for failures. It does not say "post-quantum". It does say state-of-the-art cryptography and top-level risk management, which is the hook a supervisor will use.

DORA

Imposes equivalent ICT risk-management duties on EU financial entities, with the same board-level accountability for cryptographic risk. For a group operating on both sides of the Swiss border, DORA and FINMA expectations point the same way.

Cyber Resilience Act — from 11 Dec 2027

Applies to products with digital elements placed on the EU market, covering confidentiality protection and the authenticity and upgradeability of software and firmware updates. This is the provision that turns update-chain cryptography into a product requirement.

eIDAS and the Cybersecurity Act

Trust services and certification schemes both need post-quantum-aware parameters. Version 2 of the European Cybersecurity Certification Group's Agreed Cryptographic Mechanisms, May 2025, already carries PQC algorithm recommendations for EUCC.

The honest summary for an EU entity. No law currently names a post-quantum deadline for you. The combination of NIS2 cryptography duties, the Cyber Resilience Act's 2027 product requirements and a 2030 political target for high-risk systems makes waiting for one an expensive strategy.

SOURCES European Commission, Recommendation (EU) 2024/1101, 11 April 2024. NIS Cooperation Group, A Coordinated Implementation Roadmap, 23 June 2025. Directive (EU) 2022/2555. ECCG, Agreed Cryptographic Mechanisms version 2, May 2025.

PANOP

05 · SWITZERLAND

Outside NIS2, and holding the firmest sectoral date

Switzerland sits outside NIS2 and is not among the 21 European states that signed *Securing Tomorrow, Today*. It has nonetheless produced the most concrete sectoral deadline in this briefing.

FINMA'S BENCHMARK SURVEY OF 60 INSTITUTIONS

FINDING	FIGURE
Institutions with a specific roadmap for quantum-safe encryption	**8%**
Planning to draw one up within one to three years	**around half**
No decision taken yet	**43%**
Rate crypto-agility as important or very important	**73%**
Expect to be directly affected within seven years	**around two-thirds**
Expect RSA-2048 to be breakable within 24 hours within ten years	**around two-thirds**

FINMA's central recommendation is that supervised institutions have a PQC strategy **adopted by the board of directors, with an implementation plan, milestones and target dates, by mid-2027 at the latest**. It expects a cryptographic inventory, prioritisation of data needing long-term confidentiality or non-repudiation, explicit treatment of HNDL risk, crypto-agility as a design requirement for new systems and procurements, and early engagement with external service providers.

It is guidance, not new law

FINMA's position is that Switzerland's technology-neutral, principles-based operational-risk and resilience requirements already cover quantum risk. The guidance states how those existing duties apply, and says the topic will feature more prominently in ongoing supervision.

Mid-2027 is the roadmap, not the migration

FINMA deliberately sets no final migration date. It requires instead that institutions set their own target dates — for full migration, and separately for critical business processes — and state them.

THE REST OF THE FEDERAL PICTURE

01 **NCSC / BACS technology brief, 8 December 2025**

Quantum computers and post-quantum cryptography, published alongside an assessment that action is required. Guidance, not obligation.

02 **Three parliamentary items, June 2026**

Motion 26.3628 (Juillard) for a national transition roadmap, motion 26.3830 (Blunschy) to prepare federal IT for quantum-safe cryptography, and postulate 26.3831 seeking a situation report and migration plan. The Federal Council came out in favour of a national roadmap at the start of September 2026, but the motions had not completed parliamentary passage at the edition date — so Switzerland still has no binding national roadmap, only a government on record supporting one.

03 **Swiss Government PKI**

The FOITT is already migrating it, with certificate key lengths and signature algorithms changing across classes.

04 **Cyber-Defence Campus**

armasuisse has run dedicated quantum-computing technology monitoring since 2023.

Where Switzerland sits. Neither leading nor lagging. The mid-2027 roadmap milestone lands ahead of the UK's 2028 planning deadline and roughly six months behind the EU's, and FINMA aligned with the BSI and ANSSI position on hybrid rather than the NSA's.

SOURCES FINMA Guidance 05/2026, 9 July 2026. NCSC / BACS, Technology brief: Quantum computers and post-quantum cryptography, 8 December 2025. BACS, parliamentary items 26.3628, 26.3830 and 26.3831, June 2026; inside-it.ch on the Federal Council's support for a national roadmap, 1 September 2026.

PANOP

06 · THE NATIONAL AUTHORITIES

Agreed on inventory first, divided on hybrid

They agree on inventory-first and disagree on hybrid. If you operate across borders, the strictest applicable position is the one to build to — and the gap between ANSSI and the NSA is a genuine architectural decision rather than a nuance.

POSITIONS AND DATES

ANSSI — France

The strictest in Europe. Hybridisation is **mandatory**, not advisory, for products seeking French security visas, on a three-phase roadmap: defence-in-depth, then post-quantum assurance with mandatory hybridisation from around 2025, then optional standalone PQC no earlier than 2030. ANSSI intends to require post-quantum support for product qualification from 2027, and states it will not be reasonable to buy products without it after 2030.

ANSSI position papers 2022 and 2023; PQC FAQ

BSI — Germany

Recommends hybrid, publishes the reference study on quantum computer development, co-chairs the EU work stream with France and the Netherlands, and anchors the "early 2030s" planning hypothesis used for high-security government work.

BSI, status of quantum computer development

NCSC — United Kingdom

The clearest published three-phase timeline. By 2028, complete discovery and assessment and produce an initial migration plan. By 2031, complete the highest-priority migrations. By 2035, finish. Aimed at large organisations and critical national infrastructure.

NCSC, Timelines for migration to PQC

NIST and CISA — United States

FIPS 203, 204 and 205 plus the IR 8547 deprecate-2030 and disallow-2035 schedule. A June 2026 executive order, *Securing the Nation Against Advanced Cryptographic Attacks*, tightened federal expectations, with reporting that internal migration targets moved from 2035 toward 2030. NSA's CNSA 2.0 gates national-security-system acquisitions separately.

NIST IR 8547; executive order, June 2026

ACN, CSE and NCO — Italy, Canada, Japan

Co-signatories of the G7 Cybersecurity Working Group statement on preparing for a PQC migration. ACN also publishes its own quantum-safe cryptography guidance.

G7 Cybersecurity Working Group statement

ENISA and the ECCG — EU

Support the Commission's roadmap and maintain the Agreed Cryptographic Mechanisms document, whose version 2 adds post-quantum recommendations for EU certification under EUCC.

ECCG, Agreed Cryptographic Mechanisms v2

THE ONE QUESTION THEY ANSWER DIFFERENTLY

AUTHORITY	STANCE ON HYBRID	WHAT IT MEANS FOR YOU
ANSSI	**Mandatory**	Standalone post-quantum cryptography is not acceptable for certified products before 2030. If you sell into France under a security visa, hybrid is the design.
BSI and EU	**Recommended**	Standardised, tested hybrid solutions are the recommended migration route, and the EU roadmap says high-risk mechanisms shall not be used stand-alone after 2030.
US NSA	**Not required**	Standalone post-quantum cryptography is treated as sufficient, with hybrid permitted as an interim measure. Building hybrid satisfies both camps; building standalone does not.

The most useful cross-border document. The G7 Cybersecurity Working Group statement, jointly published by CSE, BSI, ACN, ANSSI, CISA, the NCSC with DSIT and Japan's NCO in collaboration with the European Commission, because it is practical rather than declaratory. The G7 Cyber Expert Group published a companion roadmap for the financial sector in January 2026, the natural pairing with the FINMA guidance.

SOURCES ANSSI, views on the PQC transition (2022), follow-up position paper (2023) and PQC FAQ. BSI quantum computer study. NCSC, Timelines for migration to post-quantum cryptography. NIST IR 8547. G7 Cybersecurity Working Group statement. NIS Cooperation Group roadmap, 23 June 2025.

PANOP

07 · WHERE THE DEADLINES LAND

Planning due now. Sensitive systems by 2030.

DATE	WHAT LANDS
31 Dec 2026	EU Member States: national PQC roadmaps and First Steps complete
Mid-2027	Swiss financial institutions: board-approved PQC roadmap (FINMA Guidance 05/2026)
2027	ANSSI intends to require post-quantum support for product qualification
11 Dec 2027	Cyber Resilience Act applies to products placed on the EU market
2028	UK: discovery and assessment complete, initial migration plan in place
2030	EU high-risk use cases migrated, no stand-alone quantum-vulnerable public key; NIST deprecation; ANSSI procurement expectation
2031	UK: highest-priority migrations complete
2035	EU, UK and NIST converge on full transition and disallowance

08 · THE NEXT NINETY DAYS

Every roadmap starts in the same place, and it is not cryptography

Days 0–30 — See

Establish what you actually expose. Enumerate internet-facing services and the TLS versions and certificate algorithms they present, because the G7 statement singles these out as the highest HNDL exposure and post-quantum key establishment exists only in TLS 1.3 and later. Identify data with a confidentiality or non-repudiation requirement extending past 2030 and record the required lifetime explicitly. Name an accountable owner for the transition.

Days 31–60 — Inventory

Build the cryptographic inventory outward from the asset inventory you already maintain, which is the starting point the G7 statement recommends over a greenfield exercise, and consider CBOM as the format. Run a quantum risk assessment weighting potential damage, data lifespan and network accessibility; a three-level scheme is enough to sequence work. Open the supplier conversation.

Days 61–90 — Commit

Write the roadmap with milestones and target dates, approved at board level if FINMA applies to you. Put crypto-agility and post-quantum support into procurement criteria and contract language now, because procurement is the cheapest lever available. Pilot hybrid key establishment on something real. Map the result to NIS2, DORA or FINMA expectations and set a reassessment cycle, because the standards and the dates are both still moving.

FIVE QUESTIONS FOR THE NEXT BOARD MEETING

01 Which of our data, if captured in transit today, would still be sensitive in 2035?

02 Do we have a cryptographic inventory, and if not, when will we?

03 Which internet-facing services still negotiate TLS 1.2 or below, and who owns them?

04 Which of our suppliers have a published post-quantum roadmap, and which have gone quiet when asked?

05 If FINMA, a NIS2 supervisor or a large customer asked for our roadmap next quarter, what would we send them?

> **If question two has no answer**, that is the ninety-day programme. The cryptographic inventory is a discipline of its own. The layer underneath it is knowing what you actually expose to the internet, which of it is reachable, and which supplier and cloud infrastructure sits in the path — which is the asset inventory the G7 statement tells you to start from.

PANOP

09 · REFERENCES AND METHOD

Every claim traces back to a public source

Use this page to check anything in the briefing, and to hand colleagues the primary material rather than the summary.

STANDARDS AND ALGORITHMS

NIST, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), 13 August 2024.

NIST IR 8547, Transition to Post-Quantum Cryptography Standards, initial public draft, 12 November 2024.

NIST IR 8545, Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, March 2025.

ECCG, Agreed Cryptographic Mechanisms, version 2, May 2025.

EU LAW AND POLICY

European Commission, Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, 11 April 2024.

NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23 June 2025.

European Parliament and Council, Directive (EU) 2022/2555 (NIS2).

SWITZERLAND

FINMA, Guidance 05/2026, quantum computing, 9 July 2026.

NCSC / BACS, Technology brief: Quantum computers and post-quantum cryptography, 8 December 2025.

BACS, parliamentary items 26.3628, 26.3830 and 26.3831, June 2026.

inside-it.ch, Federal Council supports a roadmap for post-quantum cryptography, 1 September 2026.

NATIONAL AUTHORITIES AND JOINT STATEMENTS

G7 Cyber Security Working Group and CISA, Preparing for the Post-Quantum Era: A Call to Action, 3 September 2026.

G7 Cybersecurity Working Group, Statement on preparing for a post-quantum cryptography migration, with CSE, BSI, ACN, ANSSI, CISA, NCSC and DSIT, and Japan's NCO, in collaboration with the European Commission.

ANSSI, PQC FAQ; ANSSI views on the post-quantum cryptography transition (2022); follow-up position paper (2023).

BSI and 20 further European authorities, Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, second version, 27 June 2025.

BSI, study on the status of quantum computer development.

UK NCSC, Timelines for migration to post-quantum cryptography.

BACKGROUND

AIVD, CWI and TNO, The PQC Migration Handbook.

German Federal Government, reply on quantum threat planning assumptions, Bundestag Drucksache 20/8104.

METHOD AND LIMITATIONS

This is an awareness briefing, not legal advice, a compliance opinion or a cryptographic assessment.

Figures are reproduced as published by the cited source and were current at the edition date.

Regulatory dates in this area have already moved and may move again. Verify against the primary source before relying on any date here.

NIST IR 8547 remains an initial public draft. The Swiss parliamentary motions had not completed passage at the edition date.

USING THIS BRIEFING

Circulate section 01 to risk, legal and board readers; sections 02 to 06 to security and architecture owners.

The ninety-day sequence in section 08 is written to be lifted directly into a workplan.

A web version with every source hyperlinked is published at panop.io/blog/post-quantum-cryptography-swiss-eu-deadlines.

Prepared by Panop Research, edition september 2026. This document is intended for awareness and briefing use. It is not legal advice and does not constitute an assurance opinion.