Qcomply

The State of Quantum-Safe Security Compliance

Regulators in the US, EU, UK and Switzerland have already set migration deadlines for post-quantum cryptography — years before any quantum computer capable of breaking today's encryption is expected to exist.

Banks and other regulated financial institutions face the densest overlap of quantum-safe obligations of any sector. No cryptographically relevant quantum computer (CRQC) — one able to break RSA or elliptic-curve encryption — exists today. But the encrypted data moving across networks now can be captured and stored by an adversary for later decryption, a practice regulators call "harvest now, decrypt later." That risk, not a firm date for Q-Day, is what is driving deadlines already on the books for 2027, 2030, 2033 and 2035.

NIST finalized its first post-quantum cryptography standards in August 2024. The NSA's CNSA 2.0 suite, the EU's coordinated PQC roadmap, the UK NCSC's migration timeline and Switzerland's FINMA guidance now all reference those standards and expect regulated entities — banks foremost among them — to inventory their cryptography, plan a migration and report progress to their boards.

2030

EU deadline for critical and high-risk systems, including core financial infrastructure, to complete PQC migration.

72%

of Swiss financial institutions surveyed by FINMA have no plan or project underway for quantum-safe migration (Nov 2025–Jan 2026 survey, n=60).

2033

CNSA 2.0 exclusive-use deadline for national security operating systems, browsers and cloud services in the US.

~2030s

expert consensus window for a cryptographically relevant quantum computer — with wide disagreement either side of it.

Harvest now, decrypt later — and an uncertain Q-Day

Quantum computers running Shor's algorithm could, in principle, break RSA and elliptic-curve cryptography, which secure most of today's TLS connections, VPNs, digital signatures and key exchange. No such machine exists yet: breaking RSA-2048 requires thousands of error-corrected logical qubits running deep circuits, and the best systems in 2026 field only dozens. Algorithmic improvements have cut the estimated physical-qubit cost of the attack from roughly 20 million to under a million, but hardware still needs to catch up.

Experts disagree sharply on timing. The Global Risk Institute's 2024 survey of 47 quantum computing experts put the probability of a CRQC by 2034 at 34%, roughly double its 2022 estimate of 17%. Other surveys and vendor statements range from "already exists in a classified lab" to "beyond 2045." Most public estimates cluster in the early-to-mid 2030s, which is why government migration deadlines converge on 2030–2035 — a deliberately conservative posture, since data encrypted today with a decade-plus secrecy requirement is exposed regardless of exactly when a CRQC arrives.

For financial services specifically, harvest-now-decrypt-later matters most where confidentiality or non-repudiation must hold for years: long-lived contracts, KYC and identity records, trade secrets, and archived communications. FINMA and the UK NCSC both single this out as the immediate risk, ahead of Q-Day itself.

NIST's post-quantum algorithms

NIST finalized three post-quantum standards in August 2024, replacing the RSA and elliptic-curve schemes quantum computers would break. A fourth, hash-based signature standard for firmware and constrained devices was finalized earlier as SP 800-208.

STANDARD	ALGORITHM	PURPOSE	PREDECESSOR DESIGN
FIPS 203	ML-KEM	Key establishment / encryption	CRYSTALS-Kyber
FIPS 204	ML-DSA	General-purpose digital signatures	CRYSTALS-Dilithium
FIPS 205	SLH-DSA	Conservative backup signatures	SPHINCS+
SP 800-208	XMSS / LMS	Firmware and code signing	Stateful hash-based signatures

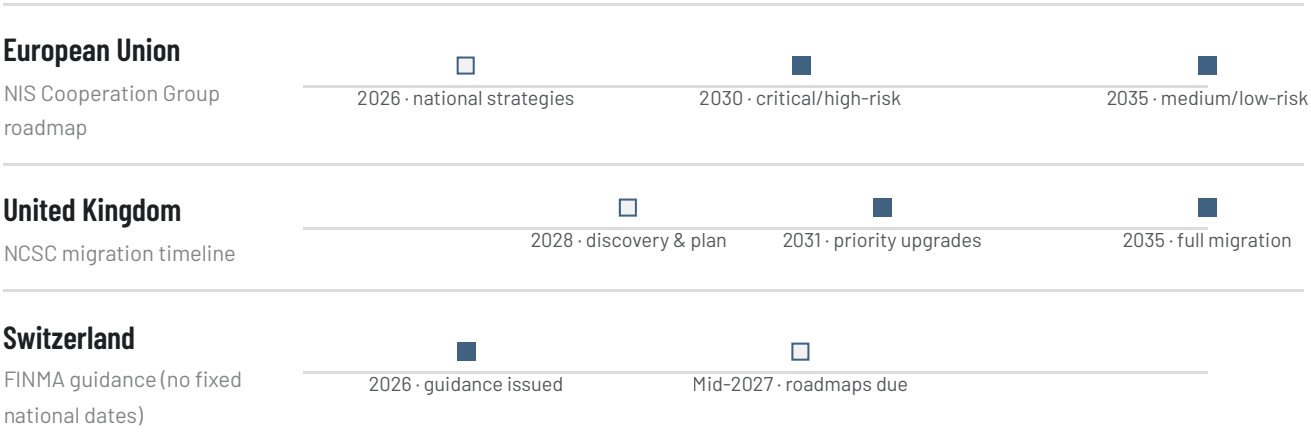
The NSA's CNSA 2.0 suite for US national security systems mandates the highest-strength parameter sets — ML-KEM-1024 and ML-DSA-87 — alongside AES-256 and SHA-384 or higher. Most other regulators, including the EU and UK, point to the same NIST standards without prescribing a specific parameter set, leaving that choice to the organization's risk assessment.

A global timeline, converging on 2030–2035

Every major jurisdiction covered here has now published dated milestones. They differ in mechanism — the US timeline is a binding mandate for national security systems, the EU and UK timelines are supervisory expectations, Switzerland's is a set of recommendations — but they land in the same decade.

United States

NSA CNSA 2.0 / NSM-10



Open dots mark planning milestones; filled dots mark migration or exclusive-use deadlines.

What each regime actually requires

UNITED STATES

CNSA 2.0 / NSM-10

Binding for national security systems only, via CNSSP 11 and the Risk Management Framework. New acquisitions must support CNSA 2.0 from January 2027; software and firmware signing move to exclusive use first. The NSA recommends the same suite as best practice for financial services, healthcare and critical infrastructure, though it is not mandatory outside NSS.

EUROPEAN UNION

DORA, NIS2 & the PQC roadmap

DORA (effective January 2025) requires financial entities to manage ICT risk, including cryptographic threats, and supports crypto-agility under its resilience-testing articles. NIS2 requires "state of the art" cryptography without naming algorithms; ENISA's June 2025 guideline and a 2026 legislative proposal explicitly recommend quantum-resistant algorithms and name harvest-now-decrypt-later as a present risk.

UNITED KINGDOM

NCSC timelines

Published March 2025, not legally binding for most commercial organizations, but operators of essential services under the UK NIS Regulations should expect sector regulators to use the 2028/2031/2035 milestones as the technical baseline when assessing security measures.

SWITZERLAND

FINMA guidance

No dedicated Swiss law mandates PQC migration. FINMA instead relies on its existing operational-risk mandate: institutions must identify, manage and report technological risk continuously, and FINMA's July 2026 guidance names quantum computing explicitly within that duty, recommending a board-approved strategy, an implementation plan with milestones, and crypto-agility clauses in outsourcing contracts.

Banks are furthest along on paper, furthest behind in practice

Financial services carries the most overlapping obligations of any sector covered here: DORA and NIS2 in the EU, PCI DSS 4.0 globally, and sector-specific expectations from FINMA in Switzerland.

PCI DSS 4.0 Requirement 12.3.3, mandatory since March 31, 2025, requires a documented cryptographic inventory and ongoing monitoring of threats to current algorithms — a crypto-agility requirement in substance, though it stops short of naming PQC algorithms or a migration deadline.

FINMA's own survey of 60 Swiss banks, insurers and financial market infrastructures (Nov 2025–Jan 2026) found awareness is high but execution has not followed: only 8% have a concrete roadmap with milestones and target dates. 72% have taken no formal step.

That gap is the practical starting point: the regulatory expectation already exists under existing risk-management duties, whether or not a jurisdiction has published a PQC-specific deadline.

Why crypto-agility matters more than any one deadline

Every regulator in this report treats crypto-agility as the underlying requirement, whether or not it names PQC directly. NIS2 requires cryptography to reflect the "state of the art" without specifying an algorithm — a standard that only an organization able to change algorithms quickly can actually satisfy over time. DORA frames it as evidence of operational resilience. FINMA calls it out as a named priority alongside the migration itself, including as a condition financial institutions should place on new outsourcing and software contracts.

Crypto-agility means an organization can swap a cryptographic algorithm, key length or protocol without re-architecting the systems around it — through abstracted cryptographic libraries, centralized key and certificate management, and inventories that are queried rather than rebuilt from scratch each time a standard changes. NIST's algorithms will not be the last word: parameter sets, implementations and even entire

algorithms have been revised before under far less scrutiny than PQC is receiving now. Migrating once to ML-KEM and ML-DSA without building the capability to migrate again is a narrower fix than the deadlines imply.

A checklist by function

Every published roadmap — US, EU, UK — starts with the same first move: know what cryptography you have before deciding what to change. The steps below sequence roughly in that order, but ownership sits with different functions.

BOARD & EXECUTIVE

- Approve a quantum-risk strategy and named executive owner
- Set a migration budget spanning multiple years, not one cycle
- Request annual progress reporting against milestones
- Treat crypto-agility as a resilience metric, not a one-off project

CISO & SECURITY

- Commission a full cryptographic inventory (algorithms, key lengths, certificates, protocols)
- Classify data by required secrecy duration to prioritize harvest-now-decrypt-later exposure
- Pilot hybrid classical/PQC key exchange on external-facing TLS
- Track NIST, NSA, ENISA and NCSC guidance updates as a standing agenda item

ARCHITECTURE & ENGINEERING

- Abstract cryptography behind libraries and APIs so algorithms can change without application rewrites
- Centralize key and certificate management ahead of larger PQC key and signature sizes
- Prioritize code-signing and firmware first — it establishes the root of trust for everything else
- Test PQC-larger payloads against protocol and hardware constraints (constrained devices, legacy PKI)

PROCUREMENT & VENDORS

- Add crypto-agility and PQC-support clauses to new software and outsourcing contracts
- Request PQC migration roadmaps from HSM, PKI, VPN and cloud providers
- Flag long-lived contracts and legacy systems without a vendor PQC commitment

RISK, COMPLIANCE & AUDIT

- Map DORA, NIS2, PCI DSS 4.0 and local regulator expectations to internal control evidence
- Document the cryptographic inventory and migration plan as auditable artifacts, not slideware
- Monitor draft rules (EU Quantum Act, evolving NIS2 amendments) for tightening obligations

COMMUNICATIONS & TRAINING

- Brief the board and senior leadership on why deadlines exist without a working quantum computer yet
- Build internal engineering fluency in PQC algorithms and hybrid deployment patterns
- Coordinate messaging with customers and counterparties on migration timing

A roadmap aligned to the published deadlines

NOW → 2027

Discover and decide

Complete a cryptographic inventory. Classify data by secrecy duration. Get board sign-off on a strategy and owner. Start with code and firmware signing — the highest-urgency, most tractable first migration.

2027 → 2031

Migrate priority systems

Deploy hybrid classical/PQC cryptography on external-facing TLS, VPNs and networking equipment. Update vendor contracts. Rebuild PKI and certificate infrastructure to handle larger PQC keys and signatures.

2031 → 2035

Complete and sustain

Retire classical-only cryptography from production. Extend migration to legacy and constrained systems. Treat crypto-agility as a permanent operating capability, not a program with an end date.

CNSA 2.0 transition milestones by system category

CATEGORY	SUPPORT & PREFER BY	EXCLUSIVE USE BY
Software & firmware signing	2025	2030
Web browsers, servers & cloud services	2025	2033
Traditional networking equipment (VPNs, routers)	2026	2030
Operating systems	2027	2033
Niche/constrained equipment & large PKI systems	2030	2033
Custom applications & legacy systems	Update or replace by 2033 — no grandfather clause	

CNSA 2.0's required parameter sets: ML-KEM-1024 for key establishment, ML-DSA-87 for signatures, XMSS or LMS for firmware, AES-256 for symmetric encryption, SHA-384 or higher for hashing. These are the highest NIST security levels and go beyond what most non-NSS organizations need to adopt immediately — but they indicate the direction regulators expect the market to move.

NIST — FIPS 203, 204, 205 post-quantum cryptography standards (Aug 2024) — csrc.nist.gov

NSA — Commercial National Security Algorithm Suite 2.0 and transition timeline — postquantum.com/cnsa-2-0

NIS Cooperation Group — Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (June 2025) — digital-strategy.ec.europa.eu

European Commission — DORA (Regulation (EU) 2022/2554) and NIS2 (Directive (EU) 2022/2555)

UK NCSC — "Timelines for migration to post-quantum cryptography" (March 2025) — ncsc.gov.uk

FINMA — Guidance on quantum computing and financial institution survey results (July 2026) — finma.ch

Swiss Financial Innovation Desk (FIND) — Action Plan to a Quantum-Safe Financial Future

PCI Security Standards Council — PCI DSS v4.0 Requirement 12.3.3

Global Risk Institute — 2024 quantum threat timeline expert survey

Palo Alto Networks; Quantum Zeitgeist; The Quantum Insider — Q-Day and CRQC progress reporting (2026)

Prepared August 2026. Regulatory guidance in this area is evolving quickly — the EU proposal to write PQC directly into NIS2 and the anticipated EU Quantum Act were both still in draft at time of writing. Verify current requirements against primary sources before acting on specific deadlines.

Qcomply

Prepared by QComply AG — qcomply.tech