RESEARCH

Post-Quantum Regulatory Clocks: Binding Law, Mandatory Policy, Advisory Roadmaps, and Proposed Measures for Financial Institutions

> There is no single global post-quantum deadline. Financial institutions need an applicability model that separates current law and mandatory government policy from guidance, milestones, and proposals.

ArcQubit Team · August 5, 2026 · 16 min read

VERSION 1.0

RESEARCH CURRENT THROUGH August 5, 2026

Abstract

Post-quantum cryptography migration is often presented as a race toward one deadline. The primary sources show a different picture. The United States has mandatory directives for specified federal and national security systems. The European Union has binding digital-operational-resilience duties but no post-quantum algorithm deadline in the Digital Operational Resilience Act. The EU and United Kingdom have also published transition milestones, while the G7 Cyber Expert Group has issued a deliberately non-prescriptive financial-sector roadmap. Proposed legislation adds another category that must be monitored but must not be reported as law.

This paper distinguishes those instruments by legal status, scope, audience, and date. It then sets out a practical method for financial institutions operating across jurisdictions: maintain an applicability register, connect each external instrument to internal cryptographic assets and evidence, and manage migration as a living risk program rather than as a countdown exercise. The analysis is current through August 5, 2026 and is informational, not legal advice.

Index Terms— post-quantum cryptography, PQC migration, cryptographic inventory, financial services, DORA, CNSA 2.0, regulatory compliance, crypto-agility.

I. Introduction

In August 2024, the National Institute of Standards and Technology approved its first three principal post-quantum cryptography standards: FIPS 203 for module-lattice-based key encapsulation, FIPS 204 for module-lattice-based digital signatures, and FIPS 205 for stateless hash-based digital signatures [1]. Standardization made implementation possible, but it did not create one universal migration date.

Different public bodies govern different systems and use different legal mechanisms. An executive order can direct United States agencies. National security policy can control products used in national security systems. An EU regulation can impose risk-management duties on financial entities. A national cyber authority can publish an indicative transition plan. An international working group can describe useful activities while expressly declining to set regulatory expectations.

Calling all of these instruments "deadlines" hides the distinctions a board, regulator, procurement team, and system owner need to understand. A useful regulatory map must answer four questions:

1. **What is the instrument's present legal status?**
2. **Who or what is directly in scope?**
3. **What action or outcome does it actually require or recommend?**
4. **Which date is stated in the primary source, and what does that date qualify?**

This paper applies those questions to the principal United States, European, United Kingdom, and G7 instruments currently relevant to a financial institution's post-quantum program.

II. Scope, Method, and Status Taxonomy

The analysis uses official publications from the issuing government, regulator, standards body, or intergovernmental group. Dates and scope statements are attributed to the primary source rather than to press coverage or vendor summaries. Where an instrument is silent, this paper does not convert an implementation assumption into a legal requirement.

Four status categories are used:

Category	Meaning in this paper	Examples
Binding law	An enacted legal instrument presently applicable to its stated subjects.	DORA and applicable delegated technical standards.
Mandatory government directive or policy	A compulsory direction within the government or national-security scope defined by its issuer, but not a generally applicable commercial statute.	Executive Order 14412 and CNSA 2.0.
Official guidance or roadmap	Governmental or intergovernmental guidance intended to coordinate or inform transition activity.	EU coordinated roadmap, UK NCSC milestones, and G7 Cyber Expert Group roadmap.
Legislative proposal	Text in the legislative process that creates no present obligation unless and until adopted and brought into force.	The European Commission's proposed targeted NIS2 amendments.

Legal force and operational significance are separate questions. A non-binding roadmap can influence supervisory conversations and vendor plans. Conversely, a binding instrument may impose governance and evidence duties without naming a post-quantum algorithm or migration date. Institutions should therefore record both status and operational relevance rather than sorting instruments into a single urgency score.

III. Timeline at a Glance

The dates below describe the outcome attached to each date; they are not interchangeable enterprise completion deadlines.

Date or horizon	Instrument	Stated outcome or milestone	Direct audience	Status
January 17, 2025	DORA	DORA became applicable to in-scope EU financial entities; it does not establish a PQC cutoff date.	In-scope EU financial entities	Binding law [4], [5]
End of 2026	EU coordinated roadmap	Member States should have started transitioning to PQC under nationally coordinated roadmaps.	EU Member States	Official roadmap [6]
2028	UK NCSC	Define migration goals, complete discovery work, and produce an initial migration plan.	Primarily large organizations and relevant technology providers	Indicative guidance [7]
December 31, 2030	Executive Order 14412	Specified federal high-value assets and high-impact systems, excluding national security systems, are to use PQC for key establishment.	United States federal agencies in scope	Mandatory directive [2]
No later than end of 2030	EU coordinated roadmap	Critical infrastructure should transition as soon as possible and no later than the roadmap's stated horizon.	EU Member States and critical-infrastructure transition programs	Official roadmap [6]
2030 or 2033, by category	CNSA 2.0	Exclusive-use dates arrive on different schedules for product and service categories used in national security systems.	Owners, operators, and suppliers of national security systems	Mandatory NSS policy [3]
December 31, 2031	Executive Order 14412	The same specified federal systems are to use PQC for digital signatures.	United States federal agencies in scope	Mandatory directive [2]
2031	UK NCSC	Carry out the earliest, highest-priority migrations and refine the migration roadmap.	Organizations following NCSC guidance	Indicative guidance [7]
2035	UK NCSC	Complete migration of systems, services, and products.	Organizations following NCSC guidance	Indicative guidance [7]
No prescribed date	G7 Cyber Expert Group	Follow a risk-based sequence of preparation, discovery, planning, execution, testing, and monitoring.	Financial entities, authorities, and sector participants	Non-regulatory roadmap [8]

The table intentionally does not include a 2035 completion date for Executive Order 14412. The order contains no such date. It also does not turn a future Federal Acquisition Regulation proposal into a present contractor obligation.

IV. Binding Law and Mandatory Government Policy

A. DORA: binding governance without a PQC deadline

Regulation (EU) 2022/2554, the Digital Operational Resilience Act, applies from January 17, 2025 to the financial entities within its scope [4]. DORA is binding law. It does not, however, name ML-KEM, ML-DSA, or another post-quantum algorithm, and it does not set a date by which an institution must complete a PQC migration.

The relevant obligation is broader ICT risk governance. Commission Delegated Regulation (EU) 2024/1774 supplements DORA with technical standards addressing encryption and cryptographic controls, cryptographic-key lifecycle management, and certificate management. Its controls require decisions to be grounded in classification and ICT risk, informed by leading practices and standards, and responsive to developments in cryptanalysis, including quantum computing [5]. It also requires records that support the management of certificates used by ICT assets supporting critical or important functions.

For a financial institution, the defensible conclusion is not "DORA has a PQC deadline." It is that DORA requires a governed, documented, reviewable position on cryptographic risk. An institution should be able to show what cryptography supports critical functions, how algorithm risk is monitored, why a control remains acceptable, and how exceptions and remediation are managed. Annual review duties, exception documentation, and monitoring requirements should be mapped separately rather than compressed into a slogan about one annual deadline.

B. Executive Order 14412: two dates for specified federal systems

Executive Order 14412 was signed on June 22, 2026 and published in the *Federal Register* on June 25, 2026 [2]. Section 4 directs the Office of Management and Budget to issue guidance requiring agencies to review inventories and transition federal high-value assets and high-impact systems, excluding national security systems:

- to PQC for key establishment by December 31, 2030; and
- to PQC for digital signatures by December 31, 2031.

The scope matters. The order does not say that every federal information system must complete migration by those dates, and it contains no "remainder by 2035" requirement. National security systems follow a separate policy track.

The procurement provision must also be stated precisely. The order directs the Federal Acquisition Regulatory Council to publish a **proposed** rule within 180 days that would require covered contractors to comply by December 31, 2030 with applicable NIST FIPS, including FIPS incorporating PQC algorithms [2]. Until the rulemaking process produces an effective final rule, that direction is a procurement-policy signal and a proposed future requirement, not an existing contractor clause.

Financial institutions that supply covered federal services should monitor the rulemaking and identify potentially affected products and contracts. Institutions without that nexus should not report the executive order as a generally applicable financial-sector deadline.

C. CNSA 2.0: a separate national-security schedule

The National Security Agency's Commercial National Security Algorithm Suite 2.0 governs cryptographic transition for national security systems [3]. Its schedule is organized by product and service category rather than by one enterprise-wide date. Depending on the category, the NSA's schedule reaches exclusive use of CNSA 2.0 algorithms in 2030 or 2033.

That policy is mandatory within its national-security scope. It is not a statute governing all United States commercial systems. It can nevertheless matter commercially when a bank, cloud provider, software company, hardware manufacturer, or service provider supplies a product used in a national security system. Those suppliers should use the official CNSA 2.0 category table for product planning; a compressed "2030 to 2033" label is not sufficient for procurement or engineering decisions.

V. Official Advisory Roadmaps

A. European Union coordinated implementation roadmap

The NIS Cooperation Group published the *Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography* in June 2025 [6]. The roadmap addresses Member States and coordinates national transition activity. The European Commission's official summary states that Member States should start transitioning by the end of 2026, and that critical infrastructure should transition as soon as possible and no later than the end of 2030.

These dates do not come from DORA. The roadmap may inform national planning, sector policy, and future supervisory approaches, but it does not by itself impose a directly applicable 2026 or 2030 obligation on every financial institution. A firm should identify the relevant national implementation and sector-specific instructions before converting the roadmap into a compliance commitment.

B. United Kingdom NCSC milestones

The UK National Cyber Security Centre published indicative PQC migration timelines in March 2025 [7]. The milestones call for organizations to establish goals, complete discovery, and build an initial plan by 2028; perform early, highest-priority migrations and refine the roadmap by 2031; and complete migration of systems, services, and products by 2035.

The NCSC presents these as timelines that industry, government, and regulators can follow, not as a generally applicable statutory cutoff. Their operational value is substantial: they divide a long transition into discovery, priority execution, and completion. Their legal effect still depends on whether a competent authority, contract, or sector rule adopts them for a particular institution.

C. G7 Cyber Expert Group roadmap

The G7 Cyber Expert Group's January 2026 statement addresses the financial sector directly [8]. It describes a phased, risk-based progression through awareness and preparation, discovery and inventory, risk assessment and planning, migration execution, testing, and continuing validation and monitoring. Governance, third-party dependency, international coordination, and adaptation to changing risk run through those phases.

The statement is explicit that it does not set guidance or regulatory expectations, and its timelines are not intended to be prescriptive. It establishes no G7 completion deadline. Its importance comes from providing a shared planning vocabulary for financial authorities and institutions, not from creating a new rule.

VI. Proposed Measures

In January 2026, the European Commission proposed targeted amendments to the NIS2 Directive as part of a wider cybersecurity package [9]. At the research cutoff for this paper, the proposal had not been adopted and therefore created no present legal obligation.

Proposals should be tracked in a separate register from current law. The institution should record the proposal's legislative identifier, responsible owner, expected scope, and next review event. Any PQC-related national-strategy language, implementation period, or transposition date must be checked against the current legislative text and then rechecked in the final adopted act. Treating a proposal as settled law creates false assurance in one direction and false urgency in the other.

VII. Implications for Multi-Regulator Financial Institutions

The source material supports a program model rather than a countdown model.

A. Maintain an applicability register

For each instrument, record the issuer, status, direct audience, systems in scope, stated outcome, date, source URL, internal legal interpretation, and review owner. Keep law, mandatory government policy, guidance, and proposals visibly distinct. A status change should be reviewable without rebuilding the entire migration plan.

B. Connect external instruments to cryptographic assets

An external date is actionable only when it can be connected to systems, protocols, libraries, certificates, keys, data-retention periods, vendors, and owners. CISA's strategy for automated cryptographic discovery and inventory emphasizes the need for repeatable discovery rather than one-time manual spreadsheets [10]. The resulting inventory should preserve enough context to determine whether an asset performs key establishment, digital signing, identity, firmware validation, data-at-rest protection, or another function affected by a particular instrument.

C. Prioritize by exposure and dependency

Priority should reflect the lifetime of protected data, algorithm exposure, business criticality, system dependencies, implementation readiness, and the external instruments that actually apply. The earliest published date is not automatically the first engineering task. A lower-level shared library, hardware root of trust, or vendor dependency may need to move before the regulated service that depends on it.

D. Preserve evidence as the program changes

Boards and supervisors need evidence that explains current posture and forecast completion. Useful evidence includes source-linked applicability decisions, cryptographic inventories, risk acceptances, vendor commitments, migration waves, test results, exceptions, and changes in regulatory status. Each report should state its effective date; a roadmap without a research cutoff can silently mix superseded guidance with current requirements.

E. Separate vendor signals from effective obligations

Proposed procurement rules, public cloud commitments, and product-support announcements can materially affect sequencing without yet being law. Track them as dependencies and planning assumptions. Do not label them as binding until the relevant final instrument, contract term, or policy applies.

VIII. DORA Case Study: An Obligation Without a PQC Date

DORA illustrates why legal status and migration date must be separate fields. A DORA-scoped institution already has binding ICT risk-management duties [4]. The supporting technical standards make cryptographic governance, key management, certificate management, and monitoring of cryptanalytic developments relevant now [5]. Neither instrument says that all in-scope firms must deploy a named PQC algorithm by a particular year.

A defensible DORA-oriented PQC evidence package would therefore show:

1. which ICT assets supporting critical or important functions rely on quantum-vulnerable cryptography;

2. how those assets, keys, and certificates are recorded and owned;
3. what leading standards and cryptanalytic developments were considered;
4. how risk, exceptions, compensating controls, and monitoring are documented;
5. how vendor and system dependencies affect the migration sequence; and
6. when the analysis, policy, and roadmap will next be reviewed.

This approach avoids two errors. The first is claiming that DORA mandates an algorithm or PQC completion date it does not contain. The second is treating the absence of that date as permission to defer cryptographic governance. The applicable duty is to manage and evidence ICT risk under the regulation's actual terms.

IX. Conclusions and Update Policy

There is no single post-quantum regulatory clock. There are binding laws, mandatory government directives, national-security policies, official roadmaps, non-regulatory coordination documents, and legislative proposals. They differ in scope and effect even when they point toward similar technical work.

For financial institutions, the durable response is one source-linked migration program with multiple applicability views. Each external instrument should map to the assets, owners, dependencies, decisions, and evidence it affects. Dates should retain their qualifiers, proposals should remain separate from current obligations, and every regulatory interpretation should carry a research cutoff.

This paper is version 1.0 and reflects sources reviewed through August 5, 2026. It should be reviewed when an underlying source is amended, a proposed measure advances, a procurement rule is published, a national authority adopts a roadmap, or a new cryptographic standard changes the expected transition path.

References

[1] National Institute of Standards and Technology, “Post-Quantum Cryptography FIPS Approved: FIPS 203, FIPS 204, and FIPS 205,” Aug. 13, 2024. [Online]. Available: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved. [Accessed: Aug. 5, 2026].

[2] The President of the United States, “Securing the Nation Against Advanced Cryptographic Attacks,” Executive Order 14412, *Federal Register*, vol. 91, pp. 38483–38486, Jun. 25, 2026. [Online]. Available: https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks. [Accessed: Aug. 5, 2026].

[3] National Security Agency, “Commercial National Security Algorithm Suite 2.0,” Cybersecurity Information Sheet, Sep. 2022. [Online]. Available: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSI_CNSA_2.0_ALGORITHMS_.PDF. [Accessed: Aug. 5, 2026].

[4] European Parliament and Council of the European Union, “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector,” Dec. 14, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj. [Accessed: Aug. 5, 2026].

[5] European Commission, "Commission Delegated Regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework," Mar. 13, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj. [Accessed: Aug. 5, 2026].

[6] NIS Cooperation Group, "Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," Jun. 23, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography. [Accessed: Aug. 5, 2026].

[7] UK National Cyber Security Centre, "Timelines for migration to post-quantum cryptography," Mar. 20, 2025. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines. [Accessed: Aug. 5, 2026].

[8] G7 Cyber Expert Group, "Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector," Jan. 2026. [Online]. Available: https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector. [Accessed: Aug. 5, 2026].

[9] European Commission, "Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act," Jan. 20, 2026. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act. [Accessed: Aug. 5, 2026].

[10] Cybersecurity and Infrastructure Security Agency, "Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools," Sep. 2024. [Online]. Available: https://www.cisa.gov/resources-tools/resources/strategy-migrating-automated-post-quantum-cryptography-discovery-and-inventory-tools. [Accessed: Aug. 5, 2026].