Regulatory Radar

Quantum Core Institute · 37 references · reviewed quarterly · last reviewed October 2026

References that shape quantum risk obligations, grouped by legal force, strongest first. They do not all carry the same weight: some are statutes and final standards, some bind only federal agencies or national security systems, some are proposals, and some are analysis. Each entry's tag says which. Status labels mean what they say: Final means final, a proposal is not yet law, and a watch item should not be cited as settled.

Live version, with filters and source links: https://quantumcoreinstitute.com/regulatory-radar

Tier 1: Final standards

These are finished. Build to them, cite them, and write them into procurement language.

1. NIST FIPS 203, ML-KEM

Final standard · August 13, 2024 | US · Final

The key-encapsulation standard, specifying ML-KEM-512, ML-KEM-768, and ML-KEM-1024. This is the replacement for quantum-vulnerable key exchange and the workhorse of hybrid TLS and key-wrapping migration. NIST has issued post-publication planning notes, a useful reminder that even final standards keep evolving. Pin your version references.

Source: https://csrc.nist.gov/pubs/fips/203/final

2. NIST FIPS 204, ML-DSA

Final standard · August 13, 2024 | US · Final

The lattice-based digital signature standard, and the one with the widest identity blast radius. Digital signatures are what machine identity, code signing, certificate chains, and nonrepudiation run on, so ML-DSA is where the identity side of quantum migration becomes concrete.

Source: https://csrc.nist.gov/pubs/fips/204/final

3. NIST FIPS 205, SLH-DSA

Final standard · August 13, 2024 | US · Final

The stateless hash-based signature standard, built on SPHINCS+. Its security rests on different mathematics than ML-DSA, which makes it diversification: a second signature family in case lattice assumptions weaken. Treat it as an option in the portfolio, not the default everywhere. Signature sizes will tell you why.

Source: https://csrc.nist.gov/pubs/fips/205/final

Tier 2: Statutes and federal directives

Binding law and agency direction. This tier is also a preview of the procurement and examination language headed for everyone else.

4. Quantum Computing Cybersecurity Preparedness Act, Public Law 117-260

Statute · December 2022 | US · Final

Signed law directing federal agency preparation for post-quantum migration, including inventory and prioritization through OMB. It binds agencies, not the private sector, and it settles a question boards still ask: yes, Congress has already legislated on this.

Source: https://www.congress.gov/bill/117th-congress/house-bill/7535
Public Law 117-260 on GovInfo (approved December 21, 2022): https://www.govinfo.gov/app/details/PLAW-117publ260

5. NSM-10

Federal policy directive · May 2022 | US · Final

The White House memorandum directing federal agencies to begin the multi-year migration of vulnerable systems to

quantum-resistant cryptography, with 2035 as the mitigation horizon. A federal policy benchmark rather than a universal mandate. Benchmarks have a habit of becoming expectations.

Source: https://www.presidency.ucsb.edu/documents/memorandum-promoting-united-states-leadership-quantum-computing-while-mitigating-risks

6. OMB M-23-02

Federal agency directive · November 2022 | US · Final

The implementing memo behind the statute and NSM-10. It requires agencies to prepare for PQC and to conduct prioritized inventories of cryptographic systems. The inventory-first sequencing is the part worth noticing: when expectations reach the private sector, the first question will be the one OMB asked. Where is your inventory.

Source: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

7. Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks

Executive order · signed June 22, 2026 · 91 FR 38483 | US · Final

The order that turns federal PQC migration from planning into dates. Agencies must move high-value assets and high-impact systems to post-quantum key establishment by December 31, 2030, and to post-quantum signatures by December 31, 2031. It also directs the FAR Council to propose, within 180 days, a rule requiring federal contractors to meet FIPS, including the PQC standards, by December 31, 2030, and asks CISA for guidance on a cryptographic bill of materials. It binds agencies directly and reaches the private sector through procurement, which is how federal expectations usually arrive.

Source: https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks

8. OMB M-26-15: Execution of the Migration to Post-Quantum Cryptography

Federal agency directive · June 24, 2026 · does not apply to national security systems | US · Final

OMB's implementing memo for EO 14412, which also fulfills OMB's duty under Public Law 117-260. Agencies owed OMB and the National Cyber Director a PQC migration plan within 120 days (October 2026) and must mitigate as much quantum risk as feasible by December 31, 2030, in five phases running from strategy and discovery in 2026–27 to full migration by 2035. National security systems are out of scope; they follow CNSA 2.0. The phase plan is a ready-made template for any organization asked to show its own.

Source: https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

9. NSA CNSA 2.0

Binding for National Security Systems · current edition, reissued May 30, 2025 | US · Final

The algorithm suite for National Security Systems, reissued May 30, 2025 as the current edition (superseding the original 2022 advisory), with new NSS acquisitions supporting CNSA 2.0 from January 1, 2027. If your organization sells into or operates alongside the defense-adjacent supply chain, this is not a future requirement. The procurement clock is already running.

Source: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

10. FD&C Act Section 524B and FDA's Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions

Statute (2023) and agency guidance · current edition February 3, 2026, superseding the June 27, 2025 version | US · Final, Published

Connected medical devices now require premarket cybersecurity documentation, including a software bill of materials. The current FDA guidance, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, dated February 3, 2026, supersedes the June 27, 2025 edition, which itself superseded the September 2023 guidance. Device cryptography is therefore already a regulatory artifact, and for fleets with fifteen-year field lives, the quantum question is baked into submissions being written today.

Source: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket

Tier 3: Proposed rules and supervisory expectations

Nothing here is final. Everything here is a direction of travel.

11. HIPAA Security Rule NPRM

Proposed rule · published January 6, 2025 · not final; Unified Agenda targets final action July 2027 | US · Proposal

HHS OCR has proposed changes to strengthen ePHI cybersecurity, including more specific risk analysis with technology asset inventories and threat identification. It is a proposed rule and must be described that way. But proposed inventory requirements in healthcare rhyme with the cryptographic inventory discipline this whole page keeps pointing at.

Source: https://www.federalregister.gov/d/2024-30983

12. NCUA 2026 Supervisory Priorities

Supervisory priority · 2026 | US · Published

NCUA's 2026 priorities emphasize risk-based compliance, payment systems, operational resilience, cybersecurity, and vendor oversight. The document does not say quantum. It says everything quantum readiness depends on. Indirect support, honestly labeled.

Source: https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ncuas-2026-supervisory-priorities

13. MAS Advisory on quantum readiness

Regulator advisory to financial institutions · Circular MAS/TCRS/2024/01 · February 20, 2024 | International · Published

The Monetary Authority of Singapore advised its financial institutions directly on quantum risk and cryptographic agility, among the first regulator-to-institution quantum communications anywhere. Not US law and not binding here. It is what supervisory expectation looks like once a regulator stops hinting.

Source: https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

14. G7 Cyber Expert Group statement and coordinated PQC transition roadmap

International supervisory signal · September 2024 statement and January 2026 financial-sector roadmap · non-binding | International · Published

Two G7 documents, read together. The September 2024 G7 Cyber Expert Group statement on quantum computing risks publicly urged financial institutions to build awareness, inventory cryptography, and develop migration plans. The January 2026 G7 CEG coordinated PQC transition roadmap for the financial sector extends that statement into operational direction: explicitly non-binding, aligned around a mid-2030s horizon, with critical systems targeted earlier. A statement and a roadmap, not a rule, but signed by the supervisory community of seven economies at once.

Source: https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

G7 CEG coordinated PQC transition roadmap for the financial sector (January 2026): https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

Tier 4: In the pipeline

Drafted or selected, not finished. Plan around these. Do not cite them as settled.

15. NIST IR 8547

Initial Public Draft · comment period closed January 2025 · still IPD as of October 2026 | US · Initial Public Draft

NIST's transition plan, still an Initial Public Draft as of October 2026: deprecate quantum-vulnerable public-key algorithms around 2030 and disallow them by 2035. The dates are draft and not yet binding, and we will update this entry the day that changes. One nuance worth knowing now: through the federal publication hierarchy, agencies and their contractors effectively treat this as operational direction, while everyone else reads it as the trajectory. Either way, it is the calendar your vendors are quietly planning against.

Source: https://csrc.nist.gov/pubs/ir/8547/ipd

16. NIST HQC selection

Standardization selection · March 11, 2025 · final expected 2027 | US · Published

NIST selected HQC as a fifth algorithm and a backup to ML-KEM, with final standardization expected in 2027. A future option for algorithm diversity, not a deploy-now default. Its real lesson is architectural: the algorithm list will keep changing, which is the entire argument for crypto agility.

Source: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

17. FN-DSA, slated as FIPS 206

Emerging draft standard · no draft FIPS published as of October 2026 | US · Preliminary Draft

The FALCON-based signature standard in progress at NIST. Until NIST finalizes it, treat FN-DSA as emerging: track it, mention it in roadmap conversations, and do not write it into any requirement.

Source: https://csrc.nist.gov/projects/post-quantum-cryptography

Tier 5: Guidance and terminology

Not rules. These are the documents that make execution and audit language precise.

18. CISA, NSA, and NIST Quantum-Readiness factsheet

Joint agency guidance · August 2023 | US · Published

The tri-agency guidance telling organizations to establish a quantum-readiness roadmap, inventory their cryptography, and engage their vendors now. If the inventory-first, vendor-second sequencing sounds familiar, it should. It is the same order any credible readiness framework runs in.

Source: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

19. NIST SP 1800-38B

Preliminary Draft · current /iprd-(1) listing dated December 19, 2023 · volumes A, B, and C | US · Preliminary Draft

NIST's practical guidance for quantum readiness, centered on cryptographic discovery. The original /iprd listing was withdrawn; the current active listing is /iprd-(1), dated December 19, 2023, covering volumes A, B, and C. The closest thing to an official manual for building the inventory everything else assumes, and it points directly at CBOM readiness: knowing your algorithms, libraries, keys, and certificates as data rather than as folklore.

Source: https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)

20. NIST CSWP 39: Considerations for Achieving Crypto Agility

Final NIST cybersecurity white paper · December 19, 2025 · updated June 29, 2026 | US · Published

NIST's first document treating cryptographic agility as a discipline of its own: the ability to change algorithms without rebuilding the platform. After drafts circulated on March 5 and July 17, 2025, CSWP 39 was finalized on December 19, 2025 and updated on June 29, 2026 (CSWP 39 upd1), and already the public reference for why agility belongs in architecture standards and procurement language rather than in aspiration.

Source: https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final

21. FS-ISAC Post-Quantum Cryptography Working Group publications

Industry guidance | International · Published

Business guidance and use-case papers for financial institutions and the payment card industry, written by practitioners for practitioners. Not regulation, and the closest thing the sector has to shared field notes on the migration.

Source: https://www.fsisac.com/pqc-payment-card-industry

22. IETF RFC 9794

Informational RFC | International · Published

Standardized terminology for post-quantum and traditional hybrid schemes. It sounds like housekeeping until two vendors describe the same hybrid mode in different words inside your audit evidence. Language confusion creates audit confusion, and this document exists to prevent both.

Source: https://datatracker.ietf.org/doc/rfc9794/

23. NIST Multi-Party Threshold Cryptography project and NIST IR 8214C

NIST project and report · IR 8214C final January 20, 2026 | US · Published

NIST's work on distributing trust in cryptographic operations across multiple parties, so no single compromised key or holder breaks the system. Relevant to key management architectures planning the post-quantum transition, and to anyone whose HSM strategy is a single point of confidence.

Source: https://csrc.nist.gov/projects/threshold-cryptography
NIST IR 8214C, the threshold call (final, January 20, 2026): https://csrc.nist.gov/pubs/ir/8214/c/final

24. NSA, NCSC, and European agency guidance on quantum key distribution

Agency guidance · NSA (undated web guidance), UK NCSC (March 2020), ANSSI, BSI, NLNCSA and Swedish NCSA joint position paper (January 2024) | International · Published

Security agencies on both sides of the Atlantic agree that quantum key distribution is not a substitute for post-quantum cryptography. NSA does not recommend QKD for National Security Systems, the UK NCSC does not endorse it for government or military use, and the joint French, German, Dutch and Swedish paper limits it to niche use cases. When a vendor pitches QKD as your quantum-readiness plan, these are the documents to hand back.

Source: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
UK NCSC, Quantum security technologies (March 24, 2020): https://www.ncsc.gov.uk/paper/quantum-security-technologies
ANSSI, BSI, NLNCSA and Swedish NCSA, Position Paper on Quantum Key Distribution (January 2024): https://cyber.gouv.fr/en/publications/jointly-led-international-publications/position-paper-on-quantum-key-distribution/
Same position paper on the BSI site: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

Tier 6: Research and market signals

No legal force. Read them anyway. These are the documents boards quote back to you.

25. Federal Reserve FEDS 2025-093

Federal Reserve working paper · September 2025 | US · Published

The Fed's research on harvest-now-decrypt-later, concluding that previously recorded distributed-ledger data can remain vulnerable even after future PQC upgrades. A working paper, not regulation, and a serious institutional signal: the central bank's researchers have put the irreversibility of HNDL exposure on the record.

Source: https://www.federalreserve.gov/econres/feds/harvest-now-decrypt-later-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm

26. Citi Institute quantum threat analysis

Market-risk analysis · January 2026 | US · Published

Citi's systemic-risk report putting probability ranges on a cryptographically relevant quantum computer (19 to 34 percent by 2034, 60 to 82 percent by 2044) and modeling a one-day Fedwire disruption at $2.0 to $3.3 trillion in GDP-at-risk. Private-sector analysis, not regulation, and the number that turned quantum risk into a financial stability conversation.

Source: https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf
Landing page: https://www.citigroup.com/global/insights/post-quantum-migration-and-the-path-to-resilient-blockchains

27. BIS Project Leap

Central bank experiment, completed · Phase 2 report December 11, 2025 | International · Published

The BIS Innovation Hub project on quantum-proofing payment systems, now completed. Phase 2, reported December 11, 2025 with the Bank of Italy, Bank of France, Deutsche Bundesbank, Nexi-Colt, and Swift, tested post-quantum signatures on liquidity transfers in an operational payment system. Proof, not prototype: the institutions operating the world's settlement plumbing have now run PQC through live rails.

Source: https://www.bis.org/project/leap
Project Leap Phase 2 report (December 11, 2025): https://www.bis.org/publications/project-leap-phase-2-quantum-proofing-payment-systems

28. Europol Quantum Safe Financial Forum call to action

Sector call to action · February 7, 2025 | International · Published

Europol's financial-sector forum called on institutions and policymakers to prioritize the quantum transition, coordinate on standards, and start now. Law enforcement convening banks about future decryption risk is the kind of sentence that did

not exist five years ago.

Source: https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

29. PQFIF written input to the SEC

Written input submitted to the SEC Crypto Assets Task Force · not SEC policy | US · Published

A post-quantum financial infrastructure framework submitted to the SEC Crypto Assets Task Force, referencing FIPS 203, 204, and 205 and proposing migration concepts. It is written input, not an SEC proposal and not adopted policy. It earns its place as evidence that migration frameworks are now arriving at regulators from the outside in.

Source: https://www.sec.gov/files/cft-written-input-daniel-bruno-corvelo-costa-090325.pdf

30. GAO-27-108740: Quantum Computing: Federal Actions Needed to Prepare for Emerging Cyber Threat

GAO audit report · publicly released October 6, 2026 · reissued with revisions October 14, 2026 | US · Published

The public version of a sensitive GAO report from September 2025. None of the 24 CFO Act agencies GAO reviewed had fully addressed three preparatory practices: inventorying cryptography, assessing funding needs, and testing post-quantum algorithms. GAO traced the gaps to missing cryptographic expertise, no processes for inventories or funding, and no testing plans, and the sensitive version made 89 recommendations to 23 agencies. If agencies working under a statute since 2022 have not finished their inventories, assume your suppliers have not either.

Source: https://www.gao.gov/products/gao-27-108740

EU and UK

EU and UK: For institutions in scope of European and UK regimes, this section outranks most of the page. Two of these are binding law in force today.

31. DORA, the Digital Operational Resilience Act

EU regulation, in force · applying since January 2025 | EU · Final

Binding on EU financial entities and their critical ICT providers: ICT risk management, incident reporting, resilience testing, and third-party oversight. DORA does not say quantum the way headlines want, and it does not need to. Cryptographic risk management and vendor accountability are already inside its perimeter.

Source: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

32. NIS2 Directive

EU directive, transposed into member-state law | EU · Final

Cybersecurity obligations across essential and important entities in eighteen sectors, including governance accountability and supply-chain security. The hook for quantum readiness is the same as DORA: risk management obligations that do not expire when an algorithm does.

Source: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

33. EU coordinated PQC implementation roadmap

Commission Recommendation (EU) 2024/1101 and NIS Cooperation Group roadmap (June 2025) · three-date milestone ladder | EU · Published

The Commission recommended a coordinated member-state transition to post-quantum cryptography, and the NIS Cooperation Group roadmap set a three-date milestone ladder: by end of 2026, member states begin transitioning; by end of 2030, critical infrastructures migrated; by 2035, full transition for as many systems as practically feasible. That first date is closer than most European planning assumes, and it is the deadline this page exists to keep visible.

Source: https://eur-lex.europa.eu/eli/reco/2024/1101/oj

NIS Cooperation Group coordinated implementation roadmap (June 2025):
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

34. UK NCSC PQC migration timelines

National cyber authority guidance · March 20, 2025 | UK · Published

The NCSC put dates on the migration for UK organizations: discovery and planning by 2028, highest-priority migration by

2031, completion by 2035. Guidance rather than law, and the clearest national timeline published anywhere. UK boards no longer get to ask what the schedule is.

Source: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

35. COM(2026) 13

Proposed NIS2 amendment · published January 20, 2026 · in Parliament committee (ITRE) as of October 2026 · watch item | EU · Proposal, Watch Item

A proposed amendment to NIS2, published January 20, 2026 and anchored explicitly to the June 2025 EU PQC roadmap. It reaffirms the 2030 and 2035 migration targets, would make PQC migration planning a named component of national cybersecurity strategies, and brings European Digital Identity Wallet providers into NIS2 scope. Still a proposal, which is why the badge stays dashed, but watch items are where next year's obligations rehearse, and this one is rehearsing loudly.

Source: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52026PC0013

Legislative procedure 2026/0012(COD) on EUR-Lex: https://eur-lex.europa.eu/procedure/EN/2026_12

European Parliament Legislative Observatory: https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026/0012(COD)

36. MiCA: Markets in Crypto-Assets Regulation

EU regulation, in force · fully applicable December 30, 2024 | EU · Final

Binding on crypto-asset service providers (CASPs), stablecoin issuers, and crypto-asset issuers across the EU. MiCA is not quantum-specific, and that is the point: every entity in scope relies on elliptic-curve cryptography for wallet key management, transaction signing, and custody, exactly the primitives Shor's algorithm breaks. Article 70's operational resilience and ICT security obligations and Article 73's crypto-asset custody requirements are the hooks where quantum risk lands today, and the DORA overlap means the same controls get examined twice. An intersecting regime worth treating as in-scope now.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114

37. EuroQCI and IRIS²

EU infrastructure programme · IRIS² Regulation (EU) 2023/588 in force · EuroQCI deployment ongoing | EU · Final, Watch Item

The EU's sovereign secure-communications build-out. IRIS², established by Regulation (EU) 2023/588, is the Union's secure satellite constellation, and the Regulation provides for gradually integrating the European Quantum Communication Infrastructure (EuroQCI) into it. EuroQCI's first satellite, ESA's Eagle-1, is due to launch in late 2026 or early 2027. This is infrastructure policy, not an obligation on firms: it shows where EU governments plan to use QKD, on government links, and it does not change the PQC migration every organization still has to run.

Source: https://eur-lex.europa.eu/eli/reg/2023/588/oj

European Commission, IRIS² secure connectivity: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

ESA, Eagle-1 (EuroQCI's first quantum key distribution satellite): https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1