PUBLIC EDITION · SEPTEMBER 2026

Cryptographic Posture Management

The evidence standard for the quantum transition

The dates are set. The certificate clock is already running. What an organization can prove about its own cryptography now matters more than what it can list.

Contents

01. Executive summary

Between June 2025 and June 2026 the post-quantum transition stopped being a matter of guidance and became a matter of schedule. The European Union published a coordinated roadmap with 2030 and 2035 milestones. The G7 published a roadmap for the financial sector. The United States issued an executive order with 2030 and 2031 deadlines for the government's most important systems, and an OMB memorandum that turns those deadlines into agency plans due within months. In the same period the everyday clock sped up as well: a public TLS certificate can no longer be issued for more than 200 days, and the ceiling falls to 47 days in March 2029.

Both clocks run on one thing: an accurate, current, evidence-backed understanding of where cryptography is used, what depends on it and what it protects. Most organizations do not have that. They have a certificate expiry tool, a cloud key console, a code scanner and a CMDB, each describing one slice of the estate in its own vocabulary, and none able to say which business service breaks when an algorithm is retired.

Cryptographic posture management (CPM) is the discipline that closes that gap. This paper sets out what a credible practice looks like in 2026: the two clocks every enterprise is on, the dated schedule that now governs planning, five principles that separate a posture program from an inventory project, a readiness ladder for negotiated protocols that tells you whether a post-quantum control is real, and a way to measure progress that is built for audit, regulatory and board review. It closes with a short account of how Qinsight builds for this model and a ninety-day way to begin.

The organizations that meet the 2030 milestones without heroics will be the ones that stop asserting their cryptographic posture and start observing it.

02. The estate you cannot see

Cryptography used to live in a few places: a perimeter VPN, a handful of certificate authorities, a well-defined fleet of servers. Today it is in every layer. Cloud platforms mint keys on demand, development teams embed libraries and protocol defaults into applications, service meshes terminate and re-establish TLS between thousands of workloads, and secrets move through build pipelines and third-party SaaS. Certificates are issued by several teams and

several authorities, some of which nobody remembers approving.

It helps to think of the estate in three domains: data in motion, the protocols and handshakes between users, services and partners; data at rest, the keys that protect stored information in cloud key services, HSMs, vaults, databases and scattered keystores; and the software supply chain, the cryptography built into applications and their dependencies, where a supplier's choices become your exposure.

Ownership is fragmented across all three. The PKI team manages some certificates, the cloud team others, application teams the libraries, and the security team the policy. No one owns the relationships between them. A spreadsheet inventory is out of date the moment it is produced, and the objects that cause incidents are the ones no spreadsheet listed: the self-signed certificate a developer left in production, the key hard-coded three releases ago, the TLS terminated inside a vendor appliance that no team owns.

The questions that matter are relational. Which endpoint uses this key? Which applications depend on that protocol? Which assets are affected if this algorithm is retired, and who owns the change? A list of objects cannot answer relational questions, which is the first reason an inventory is necessary but not sufficient.

03. Two clocks

The operational clock

Every estate carries cryptographic debt: expired or expiring certificates, weak parameters, protocol versions that should have been retired years ago, keys nobody owns, secrets in source control. The cost is paid in outages, audit findings and incident hours, and it is paid today. In 2026 the operational clock accelerated. Under the CA/Browser Forum schedule, public TLS certificates have been capped at 200 days since March 2026, fall to 100 days in March 2027 and to 47 days in March 2029. Renewal stops being an annual event and becomes a continuous operation. Processes that worked at 398 days fail at 47, and the certificates that expire are always the ones nobody knew about.

The quantum clock

The public-key algorithms that secure the internet, RSA, elliptic-curve cryptography and finite-field Diffie-Hellman, would be broken by a cryptographically relevant quantum computer. Nobody can say when such a machine will exist, and that uncertainty is often used as a reason to wait. It is the wrong reasoning, twice over.

The first is harvest now, decrypt later. Encrypted traffic captured today can be stored and decrypted when the capability arrives, so any data whose confidentiality must outlast that arrival is exposed now. The second is that regulators have effectively fixed the window. NIST's draft transition guidance deprecates 112-bit classical security, which includes RSA-2048, after 2030 and disallows quantum-vulnerable public-key algorithms after 2035. Whether or not a quantum computer arrives on that schedule, the cryptography will be non-compliant on it.

That makes the readiness question answerable without a prediction. If the confidentiality lifetime of your data plus your realistic migration lead time extends past the point where the algorithms protecting it are disallowed, the work is already justified. The only inputs are your retention obligations and your dependency map. Neither requires a forecast about hardware.

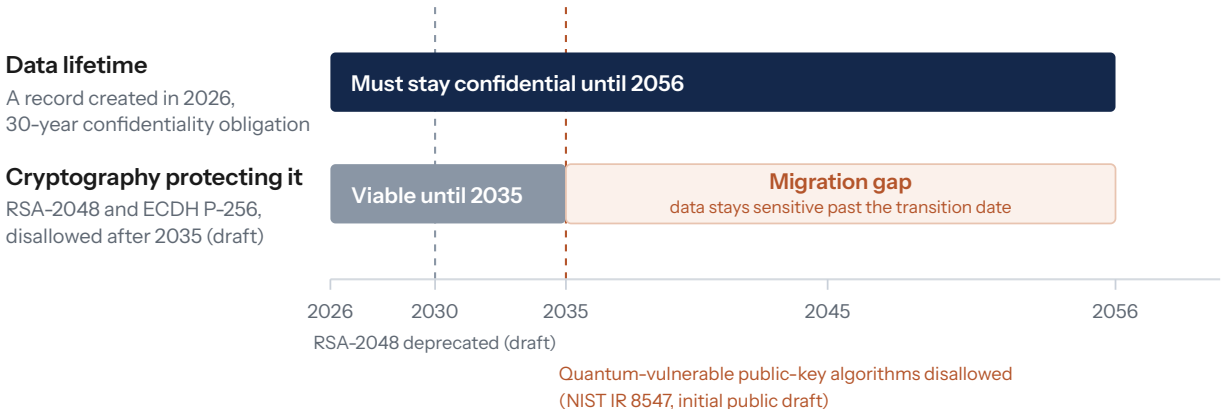

Figure 1. The risk clock. A record created in 2026 with a thirty-year retention obligation stays sensitive until 2056, well beyond the 2035 date after which NIST's draft transition guidance disallows the algorithms protecting it. The gap becomes an exposure if ciphertext captured in the meantime is still valuable when a capable quantum computer arrives.

The two clocks reward the same capability. The organization that can renew a 47-day certificate without an outage knows every place that certificate is used; the organization that can move a payment flow to post-quantum key establishment knows every hop in the flow. Starting with the operational clock is also the fastest route to the quantum one.

04. The schedule is now dated

Every instrument in the table is real, dated and public, and they are not equivalent. A mandate binds a defined population with a deadline. Guidance tells that population what good looks like. A roadmap sets a direction for a sector or a bloc without itself creating an obligation: the G7 roadmap states that it does not set guidance or regulatory expectations, and the EU roadmap is a recommendation that member states carry into national strategies. A plan that treats all three as the same is over-committing and under-committing at once.

Instrument	Primary audience or scope	Dates that matter	Type
CNSA 2.0 and CNSSP 15 (NSA, CNSS)	US National Security Systems and their suppliers	New NSS acquisitions CNSA 2.0 compliant from 1 January 2027; equipment that cannot support it phased out by end of 2030; CNSA 2.0 mandated by end of 2031; all NSS quantum-resistant by 2035	Mandate
Executive Order 14412 (June 2026)	Federal high-value assets and high-impact systems; covered contractors through a directed FAR rule	Post-quantum key establishment by end of 2030; post-quantum digital signatures by end of 2031	Mandate
OMB M-26-15	Federal civilian agencies (excludes NSS)	Migration plans within 120 days; TLS 1.3 by 2 January 2030; prioritized systems 2028 to 2031; remaining systems by 2035	Mandate

Instrument	Primary audience or scope	Dates that matter	Type
NIST IR 8547 (initial public draft)	Federal systems using NIST-approved cryptography; widely followed commercially	112-bit classical security, including RSA-2048, deprecated after 2030; quantum-vulnerable public-key algorithms disallowed after 2035	Guidance (draft)
EU coordinated PQC roadmap (June 2025)	EU member states; regulated sectors through national strategies	National strategies by end of 2026; high-risk use cases migrated by 2030; as much as feasible by 2035	Roadmap (non-binding)
UK NCSC migration guidance (March 2025)	UK organizations, public and private	Discovery and plan by 2028; priority migrations by 2031; completion by 2035	Guidance
G7 Cyber Expert Group roadmap (January 2026)	Financial sector institutions and their authorities	Points to 2035 as the overall target reflected in current guidance; suggests addressing the most critical systems in 2030 to 2032	Roadmap (non-binding)
CA/Browser Forum SC-081v3	Anyone using publicly trusted TLS certificates	Maximum validity 200 days from March 2026; 100 days from March 2027; 47 days from March 2029	Industry rule

Two things follow. First, the dates flow down. A contractor to a federal agency inherits the executive order through procurement; a supplier to a bank inherits the G7 and DORA expectations through due diligence; a device manufacturer inherits a hospital's retention obligations through the data its product touches. Regulated or not, every organization sells to someone who is. Second, the dates are close. Four years to 2030 is one budget cycle plus one migration program, and the discovery that has to precede both has not started in most estates.

The standards side is settled enough to build on. NIST's three post-quantum standards, ML-KEM for key establishment and ML-DSA and SLH-DSA for signatures, have been final since August 2024. Further algorithms are still moving through NIST's process; nothing about them changes the first step, which is knowing where the vulnerable algorithms are.

05. Five principles of cryptographic posture management

1. Observe, do not assert

A configuration file says a server supports ML-KEM. A handshake shows the server selected X25519. Both statements are true, and only one describes the protection your data received. For negotiated cryptography, TLS, SSH, IPsec and their kin, most reporting on post-quantum readiness is built from the bottom rungs of a ladder: an inventory says a library is present, a configuration audit says an option is enabled, a dashboard turns green. Readiness lives on the top rung, where the mechanism is observed in use. Controls that are not negotiated, such as code signing or encryption at rest, have no handshake to watch; for them the test is whether the configured mechanism is observed on the artifact or the data, not whether it is available.

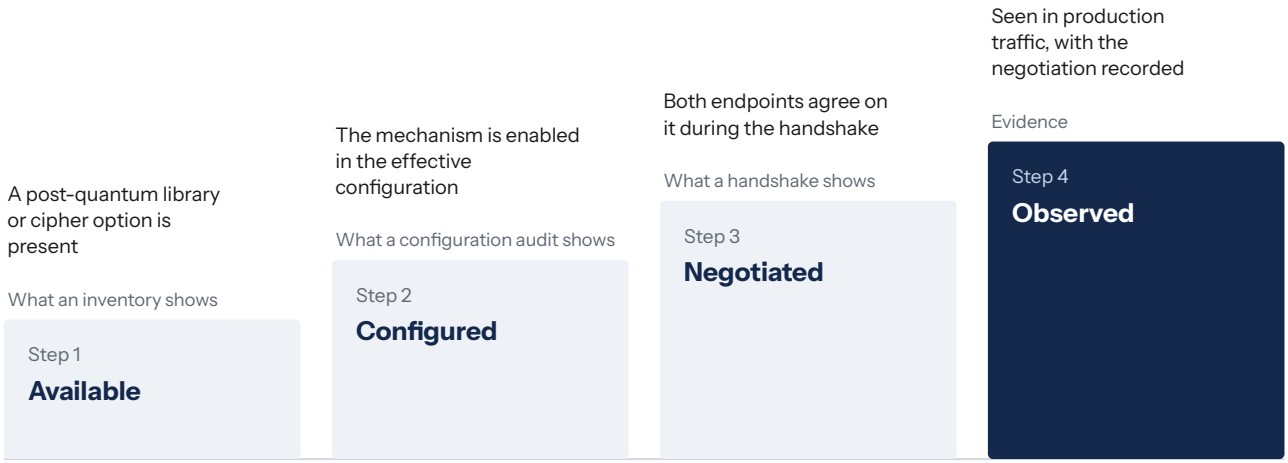

Figure 2. The readiness ladder for negotiated cryptography such as TLS, SSH and IPsec. A post-quantum control is available, then configured, then negotiated, then observed; evidence of readiness exists only on the top rung. Controls that are not negotiated, such as code signing or encryption at rest, go from configured to observed.

2. Keep the evidence

Every fact in an inventory should trace back to an observation: which method produced it, from which source, at what time, with what confidence. Provenance makes the record auditable, replayable when a standard changes its classifications, and defensible when a finding is contested by the team that owns the system. It also keeps the record honest about its limits. What a method could not see should be reported as unseen, never as absent. An inventory that hides what it could not observe is an inventory nobody can sign.

3. Relationships over lists

The unit of migration is not the algorithm. It is the dependency: the certificate, the key behind it, the service that terminates it, the applications that call that service, the data flowing through and the owner who can change any of it. A relationship graph turns thirty-seven findings into one payment flow with one weak hop, which is a decision a team can act on. Blast radius and migration cohorts fall out of the graph; they cannot be computed from a list, however long.

4. Context sets priority

A weak key on an isolated test server is a hygiene item. The same key on a payment gateway is an incident.

Priority is a function of the observed condition, the exposure path, the lifetime of the data protected, the criticality of the service and how hard the dependency is to change. The last factor is the one most programs forget: a key that can be rotated in an afternoon and a key baked into a firmware image carry different urgency at the same severity. And when context is missing, do not infer sensitivity or criticality; report the gap. A missing owner is itself a finding, and it belongs to whoever runs the CMDB.

5. Keep the evidence portable

A posture record is most useful when it belongs to the organization rather than to any one tool. PKI platforms, hardware security modules, key management services and remediation tools each hold part of the picture. A good record draws on all of them through supported integrations, then holds the result in open exchange formats such as CycloneDX, so that it can be handed to an auditor, a regulator, a remediation partner or a successor tool without translation. Crypto-agility is partly an architecture property and partly a commercial one: the ability to change your cryptography, and the tools around it, without losing your evidence.

06. Measuring readiness

Readiness is not a percentage of algorithms replaced. It is the ability to answer progressively harder questions about your own estate, with evidence.

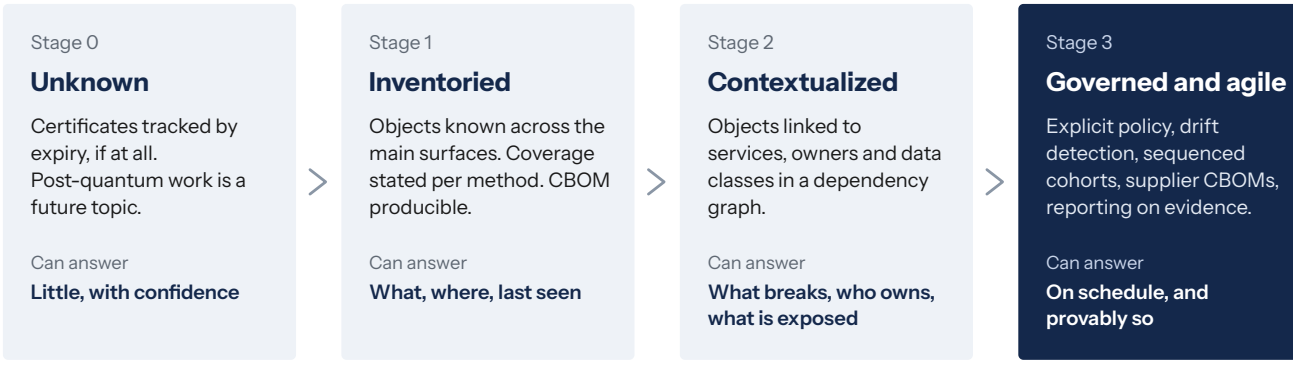

Figure 3. Four stages of cryptographic posture, each defined by the questions it can answer with evidence.

Stage 0, unknown. No authoritative inventory. Certificates are tracked by expiry date, if at all. Post-quantum work is a discussion about the future.

Stage 1, inventoried. Objects are known across the main surfaces, coverage is stated per method with confidence, and a CBOM can be produced. The estate can answer: what do we have, where, and when was it last seen.

Stage 2, contextualized. Objects are linked to services, owners and data classes in a dependency graph, and priorities are defensible. The estate can answer: what breaks if this changes, who owns it, which data is exposed.

Stage 3, governed and agile. Policies are explicit, drift is detected between observations, migration cohorts are sequenced by shared dependency, supplier evidence arrives as CBOMs, and the board is briefed on observations. The estate can answer: are we on schedule, and can we prove it.

The measures worth tracking follow from the stages. Coverage: the share of approved scope observed, by method, with a confidence level. Freshness: the age of the newest observation per object. Ownership: the share of objects attached to a service and an accountable owner. Exposure: quantum-vulnerable mechanisms grouped by the lifetime of the data they protect. The negotiation gap: mechanisms configured but not observed in use. Time to answer: how long it takes to say what depends on a given certificate, key or algorithm. The number of findings is not on the list; it rises as coverage improves and falls as coverage collapses, and rewards the wrong behavior both ways.

07. Sector notes

The instruments and the constraints differ by sector; the first question does not. Four sectors, in brief.

Sector	The clock	The constraint	Start here
Financial services	G7 roadmap, DORA, PCI DSS 4.0; counterparties on their own schedules	A payment crosses five owners; the flow is only as ready as its weakest hop	One payment or identity flow, mapped end to end
Healthcare and life sciences	Records and formulation IP stay valuable for thirty years, decades past 2035	Validated systems resist change; device fleets carry cryptography you did not write	The data class with the longest retention obligation
Government and defense	CNSA 2.0 gates NSS acquisitions from January 2027; EO 14412 and OMB M-26-15 date civilian systems; the FAR rule reaches suppliers	Accredited boundaries: collection inside, evidence out through an approved path	One boundary or one delivered system, with evidence assembled for the accreditation reviewer
Critical infrastructure	Assets outlive the standards that permit their cryptography; the replacement cycle sets the timeline	Availability first; active scanning of a live process network is often prohibited	The IT and OT boundary, with passive-safe methods

08. Governance: from audit snapshots to evidence

Traditional cryptographic assurance is a point-in-time exercise: a sample, an interview, a screenshot, a report that is stale by the time it is filed. Posture management replaces the sample with the record. Policy states what should be true in explicit, testable terms: which algorithms and parameters are acceptable for which data classes, which protocol versions may be negotiated where, how long a certificate may live. Posture is what is observed to be true. Governance measures the distance between them and closes it in order of consequence.

Frameworks give the policy its vocabulary. NIST's draft mapping of post-quantum migration capabilities to CSF 2.0 and SP 800-53 connects discovery and inventory to control outcomes; PCI DSS, DORA and HIPAA ask their own versions of the same questions. None of them is satisfied by a tool. A tool produces the evidence; the organization owns the conclusion.

Suppliers belong inside the perimeter of the record. The CycloneDX cryptographic bill of materials, now in its 1.7 release, gives buyers and suppliers a common format for declaring the cryptography inside a product. Ask suppliers for a CBOM, ingest it, and compare what was declared with what is observed where the product runs. Declared and observed rarely match on the first pass, and the difference is the most useful conversation a supplier review produces.

Five questions to ask anyone who says they are quantum ready

- Which of your claims are observed in production, and which are inferred from configuration or documentation?
- Can you show the provenance of any single finding: method, source, time and confidence?
- What could your methods not see, and where is that stated?
- Which business services depend on the mechanisms you have flagged, and who owns the change?

- Who else can use your record: can it be exported in an open format and handed to an auditor or to another tool?

09. How Qinsight approaches it

Qinsight Atlas is a cryptographic posture management platform designed around evidence. It discovers cryptography across networks, cloud key services, databases, code repositories, vaults, hardware security modules and supported security platforms through scheduled or on-demand scanning and credentialed read-only integrations with supported third-party systems. It imports CycloneDX CBOMs, and in scoped or controlled evaluations it can import customer-supplied packet captures, so that supplier declarations and observed behavior can be compared in one place. Every observation is retained with its provenance, then normalized into a relationship graph that connects certificates, keys, algorithms and protocols to the endpoints, applications and assets that depend on them, with business context from the customer's CMDB where a supported integration is enabled.

The record is portable by design. Atlas works alongside PKI, HSM and remediation platforms rather than in place of them: it integrates with supported third-party systems, exports in open formats, and the evidence goes to whichever auditor, regulator or remediation partner the customer chooses. Prioritization is explainable at the level of the individual finding: the observed condition, its classical and post-quantum relevance, the context available, and the context that is missing.

Atlas is also clear about what it does not do. Discovery is scheduled or on demand, not continuous passive monitoring. It never extracts private keys or decrypts application traffic. It does not rotate keys, replace certificates or change infrastructure, and it does not certify compliance. Configurable policy evaluation and workflow handoff are being expanded and are described to customers as such. In the language of this paper, Atlas helps organizations progress from stage 0 toward stages 1 and 2, and supplies the evidence that stage 3 governance depends on.

10. Where to start: the first ninety days

The programs that stall begin by scanning everything. The programs that finish begin with one question, answered with evidence, and expand from there.

Weeks 1 to 2: define the question. Choose one business service with a long data lifetime or an external exposure path: a payment flow, a records system, a delivered platform. Agree the scope, the data-handling rules and the decision the work supports. Write down what good looks like before anything is collected.

Weeks 3 to 6: collect from three to five sources. Network observation of the service's endpoints, one cloud key service, one database environment, one source repository, and one CBOM requested from a supplier in the flow. Read-only credentials; confirm impact before running anything.

Weeks 7 to 10: correlate and compare. Attach owners and criticality from the CMDB. Map the flow end to end. Find the gap between what is configured and what is observed. Hand the list of ownerless objects to whoever runs the CMDB.

Weeks 11 to 13: report on evidence. Coverage with confidence per method, exposure grouped by data lifetime, the first migration cohort with its dependencies, and the gaps that limit confidence. Then set the cadence and repeat, one surface or one service at a time.

Ninety days is enough to learn the shape of the estate, the quality of its ownership data and the real distance between policy and posture, and to produce a first artifact designed to support regulatory, audit and board review. Know what you have. Prove it. Then migrate in the order the dependencies dictate.

Appendix. Glossary and references

Glossary

CBOM. Cryptographic bill of materials: a structured, machine-readable record of the cryptographic components in a system and the dependencies between them, expressed in CycloneDX.

CRQC. Cryptographically relevant quantum computer: a quantum computer capable of breaking deployed public-key cryptography at useful scale.

Harvest now, decrypt later. Collecting encrypted data today in order to decrypt it once a capable quantum computer exists; the reason long-lived data is at risk before that capability arrives.

Provenance. The method, source, time and confidence attached to an observation, which make a fact in the inventory traceable and auditable.

Readiness ladder. Available, configured, negotiated, observed: the four states a post-quantum control in a negotiated protocol such as TLS passes through, of which only the last is evidence of protection. Controls that are not negotiated skip the third state.

References

- The White House, Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, 22 June 2026.
- Office of Management and Budget, Memorandum M-26-15, Execution of the Migration to Post-Quantum Cryptography, June 2026.
- National Security Agency, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, version 2.1, December 2024; Committee on National Security Systems, CNSSP 15.
- NIST, IR 8547, Transition to Post-Quantum Cryptography Standards, initial public draft, November 2024.
- NIST, FIPS 203, FIPS 204 and FIPS 205, Module-Lattice-Based Key-Encapsulation Mechanism, Module-Lattice-Based Digital Signature and Stateless Hash-Based Digital Signature Standards, final, August 2024.
- NIST, CSWP 48, Mappings of Migration to PQC Project Capabilities to NIST Cybersecurity Framework 2.0 and to Security and Privacy Controls for Information Systems and Organizations, initial public draft, September 2025.
- EU member states and the European Commission, NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23 June 2025.
- UK National Cyber Security Centre, Timelines for migration to post-quantum cryptography, 20 March 2025.
- G7 Cyber Expert Group, Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector, January 2026.
- CA/Browser Forum, Ballot SC-081v3, Introduce Schedule of Reducing Validity and Data Reuse Periods, April 2025.
- OWASP CycloneDX, specification version 1.7, 21 October 2025, and Authoritative Guide to CBOM, second edition.