QTONIC QUANTUM
POST QUANTUM READY

RESEARCH EDITION
Q4 2026

STATE OF

Quantum Cybersecurity

Two original studies. Complete evidence inside.

Enterprise connectivity / generated editorial illustration

From exposure to a defensible transition.

Evidence through 8 September 2026

A practical outlook. A clear evidence boundary.

A Q4 planning report for the people who must approve the transition.

Edition	Q4 2026 planning edition. Latest news review: 8 September 2026, 19:12 UTC. October-December actions are proposed work.
Commission	Commissioned by Qtonic Quantum Corp. Research, writing and production used AI assistance.
Evidence	Two original studies and their embedded research ZIPs appear on pages 41-45. Method and limitations: page 91. Source register: pages 88-90. Company leadership: page 92.
Visuals	Five generated editorial illustrations, source-based diagrams and measured-data charts. The official logo is unchanged. No IQM imagery, survey results or interview quotations are reproduced.

Publication and legal notice

This publication provides general information and planning analysis. It is not legal, regulatory, investment or individualized security advice. Apply requirements with qualified advisers and the responsible authority for the jurisdiction, system and contract. The original instrument governs.

Sources and conditions may change after the stated cutoff. This is a selective review, not exhaustive news coverage. Forecasts and resource estimates depend on assumptions and do not guarantee an arrival date, product delivery, security, performance or compliance.

Qtonic Quantum has a commercial interest in its products and services. Third-party references do not imply endorsement. Examples and local measurements are not customer outcomes or product certifications. Index sponsorship and evidence differences are disclosed on page 80.

Testing requires written authorization and agreed scope. Services, fees, deliverables and responsibilities arise from signed engagement documents, not this report. The publication does not amend existing agreements. See the company terms [CO04]. The company leadership website is linked on page 92.

Find the decision you came for.

GO DIRECTLY

Original research
Studies & evidence / 41-45

CBOM acceptance
The buyer handover / 84

Company leadership
The team & expertise / 92

The quarter for defensible decisions

Quantum cybersecurity becomes useful when an organization can connect a cryptographic dependency to a business consequence and an accountable action.

This Q4 2026 planning edition is written for the people who must approve those actions: executives, security leaders, architects, procurement teams and mission owners. Its evidence cutoff is 8 September 2026. October-December activities are proposed plans or future milestones, never reported results.

Qtonic Quantum's thesis is practical: a cryptographic inventory earns its value when it changes a protection decision. Connect each important dependency to a consequence, an owner, an executable next step and evidence that can be renewed. That is how a quarter of discovery becomes a funded transition.

A new federal inventory milestone

EO 14412 section 5(d) directs CISA, coordinating with NIST, to release public CBOM minimum-elements guidance within 270 days of 22 June 2026. That calculates to 19 March 2027. It is a guidance deadline for government, not a blanket private-sector compliance date. [UP03]

Two original studies, one deployment question

The 18,000 local operation timings on pages 42-43 are now joined by 80 certificate-verified TLS handshakes on pages 41 and 44. The observed handshake grew by 2,322 bytes, while the selected key-exchange fields account for 2,272. Both complete evidence archives are embedded, with checksums on page 45. [OR01, TS01]

A useful Q4 decision

Choose one consequential service, accept a usable CBOM and settle the evidence for a pilot. Today's resource estimate is on page 9, the origin-connection decision on page 33 and Google's October plan on page 39. Page 81 shows how QScout Gold turns the inventory decision into an engagement.

Can the team show the evidence behind its next migration decision - and identify what would change that decision?

Five decisions deserve priority

A credible quarter plan begins with the organization's most consequential decisions, then assigns the information needed to resolve them.

Use one executive decision register shared by security, technology, operations and procurement. For each priority, name an executive sponsor, technical owner, evidence requirement and review date. Adjust the sequence for mission consequence, data lifetime, replacement cycles and applicable obligations. These are Qtonic Quantum recommendations, not survey findings.

01 **Set the protection objective**

Identify information and trust relationships whose compromise would cause lasting harm. Separate confidentiality from authenticity and current exposure from uncertainty about future capability.

02 **Establish the boundary**

Approve services, suppliers and environments for assessment. Record exclusions and outsourced dependencies. A business-service owner may lack authority over connected systems.

03 **Find the limiting dependency**

Identify the supplier, compatibility, equipment, budget or maintenance-window constraint that prevents change. Fund the dependency that unlocks the next defensible step.

04 **Require a deployment decision**

Give each pilot a written acceptance threshold and decision date. Preserve adverse results, recovery requirements and exceptions so the result supports an explicit choice.

05 **Make evidence renewable**

Agree when records expire and what triggers reassessment. Changes to software, suppliers, routes or trust anchors can invalidate an earlier conclusion.

An owned set of protection decisions, with enough evidence to approve action and enough transparency to revisit assumptions.

What changed before Q4

Policy, protocol and assurance developments now give buyers sharper questions for Q4 procurement and engineering decisions.

Selective primary-source review: 8 September 2026, 19:12 UTC. These developments change specific decisions. Publication, announced availability and customer deployment remain different evidence states.

8 September: read the resource estimate

IonQ released an architecture-specific ECC-256 estimate. It strengthens the case for planning signature and trust-anchor migration. It does not report a live break of deployed 256-bit cryptography. Page 9 separates the numbers from the forecast. [NW01, NW02]

8 September: inspect the origin connection

Cloudflare announced Automatic Key Exchange for origin connections. Page 33 links that change to the separate work of certificate authentication and shows what a customer still needs to verify. [NW03]

October: two concrete planning decisions

OMB M-26-15 sets a calculated 22 October deadline for non-NSS agency migration plans. Google documents default PQC enablement for eligible load balancers beginning in October. Their scopes are different. See pages 18 and 39. [TP17, OP01]

March 2027: prepare an adaptable inventory

EO 14412 section 5(d) directs CISA, with NIST, to publish CBOM minimum-elements guidance within 270 days. The calculated date is 19 March 2027. This is government guidance work, not a blanket private-sector compliance date. [UP03]

Finance and protocols supply the context

Treasury launched its Quantum-Readiness Task Force on 24 August. RFC 10024 became the August Proposed Standard for the named hybrid TLS mechanisms. Neither establishes readiness in a particular customer environment. [UP01, AR07]

Request the exact standard, product release, deployed configuration, test evidence and maintenance owner. A dated, specific answer is the useful unit of progress.

What the evidence establishes

A useful decision record distinguishes the source of a claim, the observation supporting it and the exact setting to which it applies.

This edition combines primary-source research, original local measurements, company-supplied product specifications and proposed management tools. Each has a different evidentiary role. A recorded software measurement answers a narrower question than a production acceptance test.

New evidence should change the conclusion when warranted. Preserve the previous finding, the new artifact and the reason for revision so that customers can follow the decision.

Published authority

Standards and policy documents establish algorithms, requirements or guidance within a defined scope. Follow the source IDs to the actual document and provision. [QQ05-QQ07, UP03]

Observed in this study

The studies record 18,000 primitive-operation timings and 80 local TLS 1.3 handshakes. Their code, observations, protocol messages and arithmetic are supplied. Each study names its setup and the questions it cannot answer. [OR01, TS01]

Reported by the company

Qtonic Quantum reports SAFE/29 with QShield v1.0 as built and operating. This is a company implementation statement. Its engineering specification defines the target and release gates. Page 83 preserves the distinction between implementation, demonstrated platform scope and external authorization. [PC07, QQ10]

Decided in the customer environment

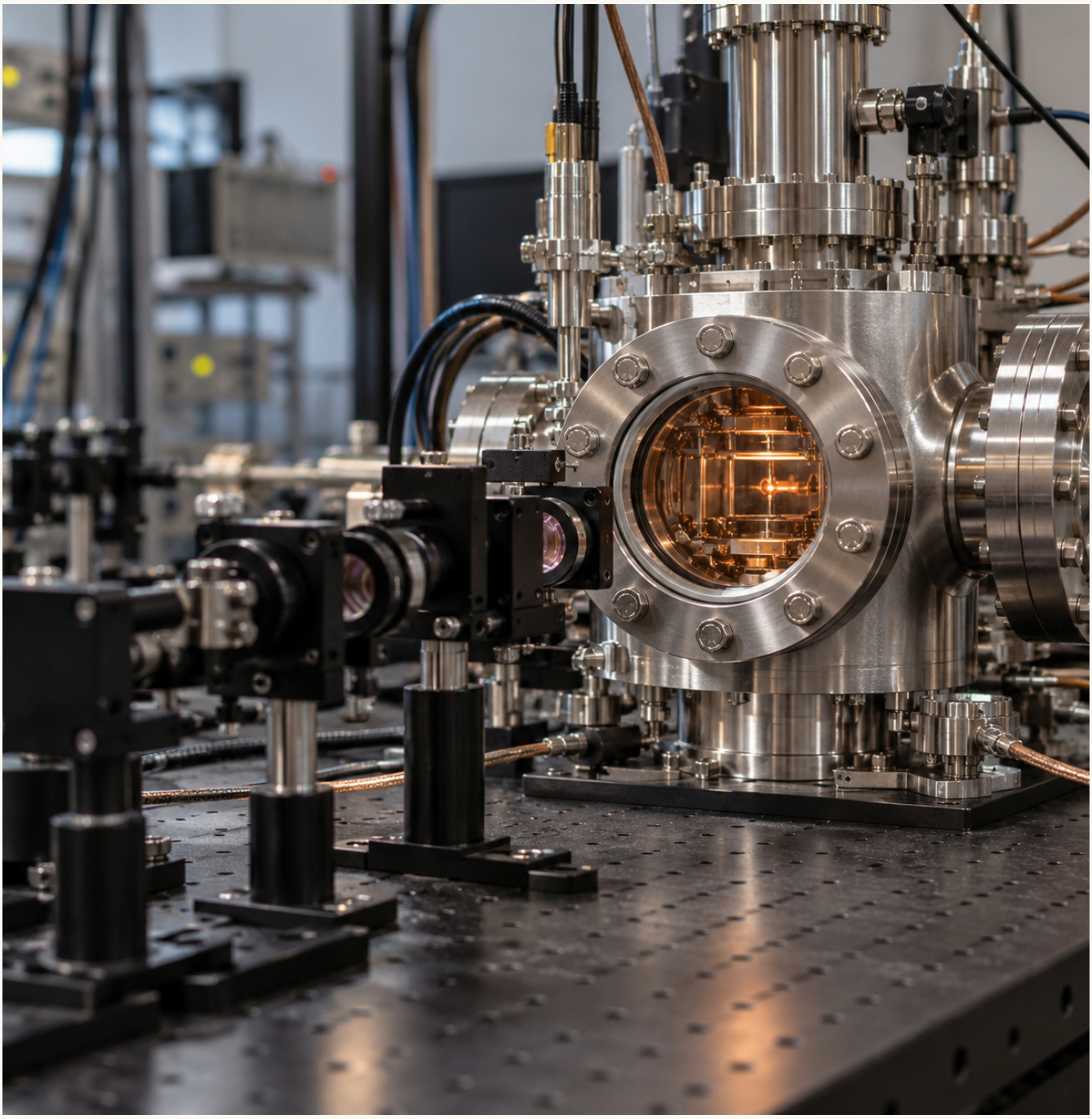
Inventory completeness, interoperability, operational acceptance and authorizations require evidence for the actual service. Name the owner, collection task and decision affected by each unresolved question.

Ask what was observed, in which version and environment, and what further decision the observation can support.

01

Threat, standards and policy

The evidence that should change a decision.



Quantum research apparatus / generated editorial illustration

Read the estimate. Own the decision.

A new resource estimate can change the migration conversation without establishing that a cryptographically relevant machine exists.

IONQ / AUTHOR ESTIMATE / ANNOUNCED 8 SEPTEMBER 2026

19,397
physical qubits

25.7 days
estimated runtime per attempt

Approximately 63% estimated success per run. Assumes the paper's proposed fault-tolerant architecture for secp256k1. These are conditional estimates.

IonQ's paper is dated 3 September and was announced on 8 September. It estimates the cost of solving the discrete logarithm problem on secp256k1 using a proposed fault-tolerant trapped-ion architecture. The figures above are author estimates, not Qtonic Quantum measurements or an observed key recovery. [NW01, NW02]

The same day, IonQ announced Superion 256 with customer deliveries planned for 2027. An announced system, a development roadmap and the larger fault-tolerant architecture assumed in the paper must remain separate claims. Raw physical-qubit counts are not interchangeable across architectures. [NW05]

The Qtonic Quantum decision. Review the signing and verification paths with the longest replacement times: firmware, software distribution, certificate hierarchies and device identity. Record the curve and cryptographic function actually used. A secp256k1 estimate is not a timing claim for every curve, RSA or AES.

Ask what would change the plan. Keep three records: demonstrated capability, conditional resource estimates and delivery forecasts. Require evidence for each. Prioritize replaceable trust anchors, verifier compatibility and tested recovery. These are useful delivery decisions even while the arrival date remains uncertain.

Disclose the commercial interest. IonQ sells quantum computing and security technologies. Qtonic Quantum publishes this report and offers cybersecurity services. Evaluate the evidence and scope of both companies' claims. [NW02]

Know what changes

Cryptographic functions face different quantum risks. Assess key establishment, signatures, payload encryption and hashes separately - and then examine their dependencies.

CRYPTOGRAPHIC FUNCTION	QUANTUM ISSUE	MIGRATION FOCUS
RSA / DH / ECDH	Public-key assumptions threatened	Approved PQC key establishment
RSA / ECDSA / EdDSA signatures	Authenticity threatened by a CRQC	PQC signing and verification paths
AES payload encryption	Generic search differs from public-key risk	Approved strength, modes and key management
Cryptographic hashes	Preimage and collision problems differ	Approved constructions and sizes

Shor-type algorithms threaten RSA and elliptic-curve assumptions. Larger public keys do not solve this problem. [TP01] Generic quantum search affects symmetric cryptography differently. NIST permits continued AES-128, AES-192 and AES-256 use under existing guidance, considering practical constraints. [TP02]

AES-protected data may still depend on vulnerable key exchange, wrapping or recovery. An RSA certificate alone does not establish how historical payloads were encrypted.

Record every role. Separate key establishment, authentication, payload protection, key wrapping, trust anchors and update signing. Preserve protocol versions and observed negotiated parameters.

Assess the complete construction. Apply required symmetric strengths. Evaluate protocol replacement, sizing and implementation assurance separately. Symmetric strength cannot repair vulnerable public-key exchange.

A quantum-resistant cipher cannot secure a system whose key protection or peer authentication remains vulnerable.

Confidentiality has a long tail

A future capability can create a present exposure when the information remains valuable after the protection around it becomes breakable.

CISA, NSA and NIST describe the risk that adversaries collect encrypted information now and decrypt it later when sufficiently capable quantum computers become available. Their joint guidance recommends beginning migration preparation. [TP04]

The assessment unit should be a sensitive information flow and its key-protection chain. Ask who could obtain ciphertext, what additional material would be necessary, how long the information must remain confidential, and which systems control the protection. This produces a reasoned exposure assessment. It does not establish that collection has occurred.

Examples for assessment include durable intellectual property, sensitive health information, strategic plans and long-lived identity records. Their importance depends on the organization, the specific data and the harm from disclosure. A document retention period is an input, not a substitute for a business decision about confidentiality lifetime.

Migration stops additional exposure

Upgrading a live channel can protect future traffic when correctly implemented. It cannot retroactively change ciphertext already held by another party. Separate the legacy exposure question from the current migration program, and retain an explicit record of what can and cannot be remediated.

Do not overstate detection

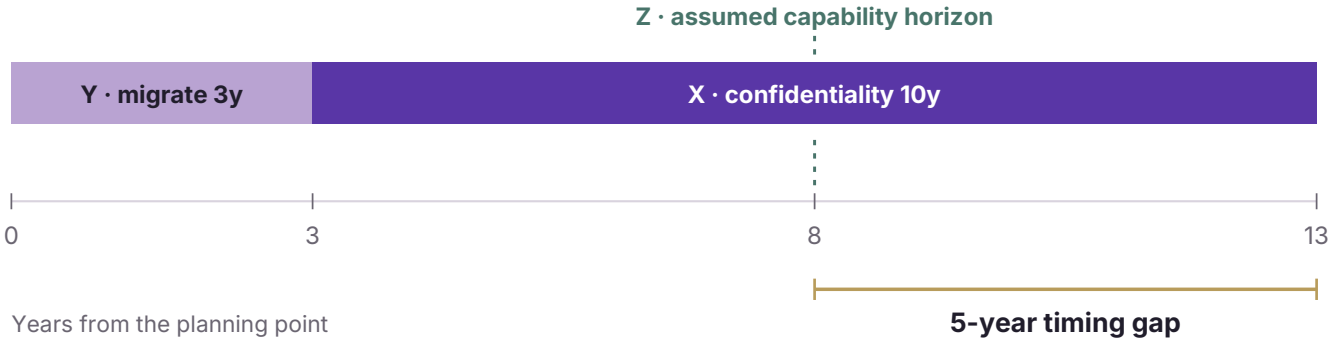
An inventory identifies vulnerable mechanisms. Traffic evidence can show observed negotiation. Neither alone proves hostile harvesting, its scale or an adversary's future decryption capacity. Describe a potential exposure as potential unless incident evidence supports a stronger statement.

Prioritize by the duration and consequence of disclosure, the plausible collection path and the time required to change the protection.

Three clocks. One decision.

Three clocks shape the decision: confidentiality lifetime, migration time and an uncertain horizon to relevant quantum capability.

ILLUSTRATIVE INPUTS X + Y = 13 years Z = 8 years



Scenario arithmetic only · no forecast or probability implied

SCENARIO SENSITIVITY / X = 10 YEARS

Migration time Y	Z = 8 years	Z = 12 years
1 year	3-year gap	No timing gap
3 years	5-year gap	1-year gap
5 years	7-year gap	3-year gap

Gap = max(X + Y - Z, 0). Illustrative assumptions, not a forecast.

Michele Mosca's model compares required secrecy lifetime X plus migration time Y with an assumed capability horizon Z. Qtonic Quantum uses the relationship to test whether the proposed schedule protects information for long enough. [TP05, TP28]

The table varies migration time and the scenario horizon while holding secrecy at ten years. Shortening migration reduces the gap. It does not establish when a relevant quantum computer will arrive.

This relationship supports planning and sensitivity analysis. It neither predicts a CRQC date nor estimates compromise probability.

Authentication needs its own plan

Replacing key establishment protects one part of the system. Identity, software authenticity and durable evidence require their own migration plan.

NIST's ML-DSA and SLH-DSA standards provide post-quantum digital signature mechanisms. These are distinct from ML-KEM, which establishes shared secrets. [TP06][TP07][TP08] Stateful hash-based signatures have separate operational requirements, including careful management of signing state. [TP09]

Map the verification ecosystem before changing a signing algorithm. A firmware signature depends on the device accepting its verification key and algorithm. A certificate depends on relying parties and trust distribution. An archived record depends on how later verification establishes what was valid at the relevant time.

Inventory the signer, verifier, trust anchor, key storage, signing frequency, lifetime of signed objects and replacement path. Pay particular attention to products whose boot or recovery verification is anchored in hardware. A modern transport protocol cannot compensate for an update mechanism that cannot safely introduce a new trust anchor.

Separate channel claims

A service that negotiates PQC key establishment may continue using classical certificate signatures. Describe that configuration precisely. A successful handshake is evidence about a particular connection, not proof that all device identity, administrative access or code-signing paths have migrated.

Preserve verifiable history

For long-lived records, work with records owners and counsel on evidence preservation, trusted time and signature renewal requirements. Do not assume that changing tomorrow's signer makes yesterday's signature independently trustworthy forever. Test verifier compatibility and recovery procedures before broad deployment.

Treat trust-anchor replacement and verifier adoption as first-class delivery work, with owners and acceptance criteria separate from encrypted transport.

Three technologies. Three purposes.

Post-quantum cryptography, quantum key distribution and quantum random number generation solve different problems. Their names are not interchangeable.

TECHNOLOGY	PRIMARY ROLE	WHAT IT DOES NOT ESTABLISH
PQC	Classical algorithms designed for quantum resistance	Secure integration or product validation
QKD	Distribution of keying material over a physical link	Complete end-to-end authentication and endpoint security
QRNG	Randomness derived from a quantum process	Quantum resistance of RSA, ECC or the whole system

PQC algorithms run on conventional computing platforms. [TP10] QKD uses specialized physical systems to distribute keying material and still requires source authentication. NSA identifies implementation and deployment limitations for NSS use. [TP11] Entropy-source assurance has its own requirements, including those in NIST SP 800-90B. [TP12]

On 8 September, IonQ and Congruity360 announced an $8.18 million agreement involving PQC and QKD appliances. This is a reported commercial agreement, not evidence that every customer system is protected. It is a concrete reason to make suppliers separate the functions in the table. [NW06]

Ask what becomes protected. Require the supplier to identify the security property delivered: key establishment, message authenticity, payload confidentiality or entropy quality. Then identify the components and threat assumptions outside that claim. A narrow, well-supported property is more useful than an unqualified "quantum-secure" label.

Keep enterprise migration coherent. A specialized QKD deployment does not remove the need to migrate vulnerable signatures and other public-key dependencies across an enterprise. Better randomness cannot change a vulnerable mathematical assumption. Evaluate complementary technology on its own merits while preserving a complete cryptographic transition plan.

Approve an architecture and evidence package for a defined use case. Do not approve a quantum label as a substitute for a security requirement.

The standards that matter

Use the final standard identifier, algorithm name and intended function in requirements. Selection for standardization is a different status from a published standard.

PUBLICATION / CANDIDATE	FUNCTION	STATUS
FIPS 203 / ML-KEM	Key establishment	Final
FIPS 204 / ML-DSA	Digital signatures	Final
FIPS 205 / SLH-DSA	Stateless hash-based signatures	Final
SP 800-208 / LMS, XMSS	Stateful hash-based signatures	Final, specialized constraints
SP 800-227	KEM implementation and use	Final guidance
FN-DSA / FIPS 206, HQC	Additional signature / KEM options	In development / selected

NIST finalized FIPS 203, 204 and 205 on August 13, 2024. [TP06][TP07][TP08] SP 800-227 became final on September 18, 2025. [TP13] FN-DSA/FIPS 206 remains in development. HQC is selected for standardization. Neither is a final FIPS here. [TP14]

Algorithm approval leaves parameter sets, protocol encoding, certificate profiles and product versions to applicable policy, security objectives and interoperability requirements.

Specify acceptance. Require the function, standard version, permitted parameters, protocol and validation evidence. Separate current support from roadmaps. Predecessor submission names require demonstrated conformity to final standards.

Track status. Maintain final standards, errata, drafts and selected candidates separately. Recheck at design approval and production acceptance. Drafts inform planning without establishing certification or mandatory deadlines.

A precise specification makes vendor claims comparable and exposes integration work that an algorithm checklist would miss.

Standards begin the proof

Algorithm approval, module validation and deployment acceptance answer different questions. Procurement needs the evidence connecting them.

NIST's CAVP validates algorithm implementations. This alone does not satisfy FIPS 140 module validation requirements. [TP15] CMVP evaluates modules with defined versions, operating conditions and security policies. NIST permits acceptance of FIPS 140-2 modules through 21 September 2026. Afterward they move to the Historical List for existing-system use only. [TP18]

Executive Order 14412, section 6(b), directs Commerce through NIST to revise CMVP processes within 180 days of 22 June 2026 to accelerate validations, to the extent appropriate and consistent with law. [UP02] The direction does not certify a product or guarantee a supplier's completion date.

Qtonic Quantum recommends two distinct procurement checks: verify the required PQC capability and verify the applicable module validation. A FIPS 140-3 certificate alone does not establish that the required PQC algorithm is included or that the application uses its approved mode.

Trace the deployed protection

Connect the protocol and application configuration to the exact module, security policy and operating environment. Then connect the module to the applicable algorithm evidence. Retain deployment records showing that this cryptographic path is active.

Test operational acceptance

Measure interoperability, failed negotiation, recovery, updates and performance in the intended configuration. Distinguish reproduced findings, supplier assertions and unresolved questions. Conformance and operational assurance each need their own evidence.

Can the buyer trace the exact deployed protection from negotiated protocol to module validation and algorithm evidence?

Policy, in context

Policy dates show how the landscape developed. Obligations depend on jurisdiction, system type, authority and the applicable instrument.

SEVEN INSTRUMENTS / PUBLICATION OR ISSUANCE DATES

18 NOV 2022	**OMB M-23-02**	Federal preparation
13 AUG 2024	**FIPS 203 / 204 / 205**	Final algorithms
12 NOV 2024	**NIST IR 8547 ipd**	Draft transition
20 MAR 2025	**UK NCSC timeline**	UK migration guidance
JUN 2025	**EU roadmap**	Member State coordination
22 JUN 2026	**Executive Order 14412**	Federal acceleration
24 JUN 2026	**OMB M-26-15**	Non-NSS agency execution

Chronological sequence. Intervals are not to scale.

The sequence connects federal preparation, draft transition guidance and the 2026 execution phase. These are publication or issuance dates. Obligations depend on the entity, system, authority and relevant provision.

For the next decision, use the actual deadline and the owner responsible for it. EO 14412 adds a CBOM guidance milestone on the calculated 19 March 2027 date. That direction is to CISA with NIST, not an automatic compliance deadline for every business. [UP03]

A roadmap date, an agency instruction and a binding contract clause do not establish the same obligation.

Federal migration moves to execution

June 2026 policy materially changes the planning baseline. A program built only around a distant 2035 endpoint is incomplete.

Executive Order 14412 directs accelerated migration of federal High Value Assets and high impact systems, excluding NSS: PQC key establishment by December 31, 2030 and digital signatures by December 31, 2031. It also directs further technical and procurement actions. [TP16]

OMB M-26-15 excludes NSS and requires agencies to submit migration plans within 120 days of June 24, 2026: October 22, 2026, calculated from the memorandum date. Its phases cover planning in 2026-2027, pilots in 2027-2028, prioritized key-establishment migration through 2030, signatures in 2031 and remaining systems by 2035. [TP17]

The next planning dependency is the CBOM minimum-elements guidance required by section 5(d) of EO 14412. The 270-day interval from 22 June 2026 calculates to 19 March 2027. CISA, coordinating with NIST, must address elements that enable automated assessment. Build schema and provenance flexibility into the Q4 baseline. [UP03]

Make shared responsibility explicit

For a hosted service, establish which party controls protocol configuration, certificates, application libraries, stored-data keys and recovery. Obtain product-specific commitments and evidence. A provider's general PQC announcement should not substitute for a responsibility matrix for the agency's deployment.

Distinguish rulemaking from obligations

EO 14412 directs a proposed FAR rule addressing covered contractors. The instruction to propose a rule is not itself a finalized universal contractor clause. [TP16] Contracting and legal teams should map actual current requirements while preparing for the stated policy direction.

The immediate deliverable is an executable migration plan with evidence and ownership. Technical pilots should retire uncertainties that would otherwise delay its critical path.

The NSS acceptance path

National Security Systems have a distinct policy and assurance framework. General enterprise PQC support does not establish NSS suitability.

NSA's CNSA 2.0 FAQ states that new NSS acquisitions must be compliant by January 1, 2027 unless otherwise noted. Equipment and services unable to support CNSA 2.0 are to be phased out by December 31, 2030, with CNSA 2.0 use mandated by December 31, 2031, subject to stated exceptions. Its general-purpose choices include ML-KEM-1024, ML-DSA-87, AES-256 and SHA-384/512. [TP01]

NSA's resource page points to CNSS Policy 15 released March 4, 2025. [TP23] Qtonic Quantum analysis: the applicable policy, implementation guidance, protection profile and authorization context must be checked together for the particular system. The January 2027 date should never be broadened into a claim that all US government purchases are prohibited if they use today's encryption.

Buy an approved integration path

Ask how the proposed architecture reaches the relevant NIAP, CSfC or other specified acceptance route, where applicable. Identify which cryptographic services are covered, which dependencies remain and who grants the system-level approval. An algorithm list is necessary technical information, not a substitute for that route.

Make the transition operational

Require a supported configuration, partner interoperability plan, update policy, migration dependencies and a means to verify actual use. If an exception or waiver is relevant, record its authority, scope and expiration. Do not describe a requested or anticipated waiver as approved.

Describe prototypes accurately

A demonstration can establish measured behavior within its test boundary. It does not establish accreditation, validation, deployment approval or operational suitability beyond the evidence supplied.

"CNSA 2.0 aligned" should name the exact property demonstrated and the remaining approval work. Precision strengthens a proposal's credibility.

Turn milestones into work

The UK timeline gives organizations a planning structure: establish the baseline, complete priorities, then finish the broader migration.

NCSC's March 20, 2025 guidance sets targets for discovery and initial planning by 2028, early highest-priority migration by 2031 and completion by 2035. It primarily addresses large organizations, critical national infrastructure operators and organizations with bespoke IT. These are migration guidance targets, not a prediction of a CRQC arrival date. [TP21]

Translate each target into an internal gate with measurable entry and exit criteria. An organization that waits until the first target year to begin discovery can lose the opportunity to align cryptographic upgrades with existing maintenance and procurement cycles.

For the first gate, measure inventory coverage, ownership and dependency visibility. For the second, show that prioritized services meet approved acceptance criteria and that exceptions have owners. For the final gate, reconcile the full estate, including archived systems, subsidiary environments, recovery paths and managed services.

Prioritize difficult trust dependencies

Investigate products with long service lives, embedded trust anchors and limited update options early. The initial question is whether their upgrade path exists and can be exercised safely. That answer may affect an acquisition decision years before broad deployment of a new algorithm.

Map the actual obligation

A regulated entity should review applicable legislation, regulator communications, contracts and sector-specific requirements alongside NCSC guidance. Record where the organization voluntarily chooses an earlier milestone and where an external obligation determines the date. Preserve both the legal rationale and the technical evidence.

A date becomes a useful control only when the organization can define, demonstrate and independently review what completion means.

Coordinate the dependencies

Europe's coordinated roadmap connects national planning, risk-based migration and software upgrade capability. Multinational programs should preserve those distinctions.

The June 2025 EU roadmap calls for initial national roadmaps and high- and medium-risk planning and pilots by end-2026. It targets high-risk migration and quantum-safe software and firmware upgrades by default by end-2030, followed by medium-risk migration by end-2035. Low-risk migration proceeds as feasible. This coordinated roadmap addresses Member States. National implementation and sector obligations determine the enterprise application. [TP22]

Establish a European program baseline, then map each operating entity to its national implementation and sector obligations. Shared services may inherit requirements from several entities. Suppliers should identify where one deployment profile can satisfy them and where regional or sector differences require separate treatment.

Treat the supply chain as part of the migration boundary. The relevant dependency may be a cloud control plane, a certificate issuer, a software distribution mechanism or a device manufacturer. A local application cannot independently complete a transition if essential counterparties cannot accept its new cryptographic behavior.

Make the upgrade path a deliverable

For equipment expected to remain in service through the migration period, request evidence that software, firmware and trust anchors can be changed safely. Test the process and recovery behavior. A contractual promise to support PQC later should identify what will be delivered and how the buyer will assess it.

Preserve national nuance

Use the same evidence structure across countries while retaining the exact applicable authority and deadline for each entity. This supports consistent engineering without turning high-level coordination into an unsupported claim about legal duties everywhere.

The most useful European readiness measure is whether critical services and their external dependencies can complete an agreed transition together.

Finance moves together

The financial sector now has a U.S. coordination mechanism. Readiness still has to be demonstrated across each critical service.

Treasury launched its Quantum-Readiness Task Force on 24 August 2026. Its three workstreams cover sector alignment and PQC transition, third-party and vendor readiness, and digital assets and emerging technology risk. The public-private initiative builds on the G7 Cyber Expert Group roadmap. [UP01]

The January 2026 G7 roadmap promotes coordinated migration and cryptographic agility. It explicitly does not establish guidance or regulatory expectations, and its timelines are not prescriptive. [TP24] Treat the task force as a coordination signal. Establish any binding obligation through its actual authority.

Qtonic Quantum recommends assigning a migration owner to each critical business service. Payments, trading and custody cross counterparties, shared infrastructure and technology suppliers. Component owners need a common acceptance plan for the service they collectively support.

Make dependencies visible

Ask providers for the exact configuration, responsibility boundary, dependency map, delivery schedule and interoperability evidence. Record where a counterparty or shared service determines the pace of migration.

Preserve resilience during mixed adoption

Test communication between migrated and unmigrated components. Define acceptable compatibility behavior, exception authority and exit conditions. Include partial outages and rollback in the service acceptance plan.

Use a defensible readiness statement

Describe the practices adopted, the scope covered and the evidence produced. Do not advertise "G7 compliant" based solely on alignment with a voluntary roadmap.

Coordinate at sector level. Accept at service level. Preserve the evidence linking the two.

Keep safety in the decision

A carrier network or transportation data center must manage quantum exposure within its existing security, availability and safety constraints.

EO 14412 directs Sector Risk Management Agencies and CISA to assist critical infrastructure owners and operators with PQC migration plans. Its federal HVA/high-impact deadlines should not automatically be assigned to every private operator. [TP16] TSA maintains sector-specific security directives and emergency amendments. Applicability must be established for the operator and mode concerned. [TP26]

NCSC identifies OT migration challenges including resource constraints, limited upgradeability, embedded devices and proprietary protocols. [TP21] Qtonic Quantum analysis: use those constraints to define a controlled assessment boundary and modernization sequence. The correct priority may be a management or update dependency whose failure affects many operational assets.

Before selecting a vendor, establish the transport mode, jurisdiction, regulated entity, system owner, safety relevance and customer obligations. CISA coordination, TSA security direction and FAA requirements occupy different roles. A supplier should map an asserted requirement to the exact authority and covered system, rather than grouping agency names into a blanket compliance claim.

Test the operational envelope

Define accepted latency, availability, restart, failover, recovery and maintenance behavior for the intended service. Validate cryptographic changes in an appropriate representative environment before production introduction. Coordinate change control with operations and safety assurance where the system requires it.

Procure a maintainable lifecycle

Evaluate support duration, cryptographic update mechanisms, trust-anchor replacement, protocol dependencies and rollback constraints. Contract for the evidence needed to accept later upgrades. A product may support an algorithm today yet lack the lifecycle controls needed for a long-lived transportation asset.

Quantum readiness should strengthen the operational security program and preserve required safety and service performance through the transition.

What the board needs to know

The board does not need to choose algorithms. It needs assurance that management can identify exposure, fund a credible transition and verify progress.

NIST CSF 2.0 places cybersecurity governance within enterprise risk management and provides outcomes for communicating and prioritizing cybersecurity work. It does not prescribe one implementation. [TP27]

Place the quantum transition within existing risk governance, with a named executive owner and a cross-functional delivery team. The program should connect information protection needs, business-service dependencies, procurement decisions and operational change. A laboratory demonstration becomes meaningful when it resolves a documented business or engineering uncertainty.

Ask for a baseline with scope and limitations. Inventory coverage should identify the denominator: applications, services, devices or flows assessed. Migration progress should identify the acceptance standard. An unknown dependency should remain visibly unknown until verified, rather than disappearing into a green aggregate score.

Require three decision papers

First, exposure: what information or service is at risk, why it matters and which assumptions drive priority. Second, execution: accountable owners, resources, sequencing, dependencies and exception decisions. Third, assurance: the evidence required to declare a service migrated and the process for detecting regression.

Challenge the plan constructively

Ask which decisions remain sound under earlier or later threat scenarios. Identify the supplier commitment on the critical path, the asset that cannot be upgraded and the trigger for an accelerated response. Require a costed alternative when a dependency may not deliver.

Align claims with evidence

Public language, sales proposals and customer assurance responses should use the same verified status register as engineering. Distinguish planned, tested, deployed and independently validated capabilities. Consistency prevents unsupported confidence from outrunning the work.

A credible program gives leadership a decision it can approve, a result it can inspect and an exception it can explicitly own.

02 Migration architecture

Follow the trust dependency.

Inventory / 27 Trust paths / 33 Original research / 41

TLS 1.3 / RECORDED LOCAL STUDY

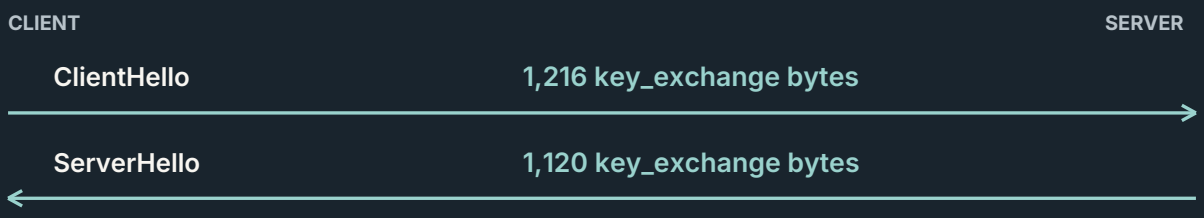
One session. Three separate controls.

In this study, server authentication remains classical.

01 / KEY ESTABLISHMENT

HYBRID

X25519 + ML-KEM-768



02 / SERVER AUTHENTICATION

CLASSICAL

ECDSA P-256 / RSA-PSS

Certificate + CertificateVerify in all four configurations

03 / APPLICATION PROTECTION

SYMMETRIC

TLS_AES_256_GCM_SHA384

AES-256 payload protection

Selected roles and messages, not a full handshake transcript. Assess key exchange and authentication separately. Study scope and bytes: pages 41 and 44.

Selected TLS messages / recorded study and cited protocol field sizes

Discover the dependency

A cryptographic inventory becomes useful when it connects a technical observation to a service, an accountable owner and a migration decision.

NIST's NCCoE separates cryptographic discovery from interoperability work and describes inventory as an input to risk and prioritization. Its project materials also distinguish preliminary practice-guide drafts from final publications. [AR01]

Qtonic Quantum recommends starting with a bounded business service: its entry points, processing components, identities, signing systems, storage and recovery paths. Identify the decisions the inventory must support before choosing collection tools. A certificate list can answer an expiry question. It cannot, by itself, establish the algorithms used inside every application or the protection of archived keys.

Reconcile several evidence channels. Compare approved configuration exports, software dependency records, certificate-management records and observed protocol metadata. Record the observation time and collection boundary. Treat vendor statements as a distinct evidence class until the relevant deployed configuration is verified. Discovery should collect the metadata needed for the decision, with access controls and retention limits appropriate to the environment.

Begin with a denominator

Define the assets, business services, environments and trust boundaries included in the assessment. Report the share covered against that declared population. If the population itself is incomplete, say so. A clean scan result cannot repair an undefined denominator.

Make findings actionable

Each material dependency needs an owner, the information it protects, its expected service life, a source reference, an uncertainty statement and a next action. The first deliverable is a queue of resolvable decisions, not a wall of algorithm names.

Can the service owner explain which cryptographic dependency blocks the next migration step, using dated evidence?

Build a CBOM that can evolve

Build the Q4 inventory so it can absorb the CBOM minimum-elements guidance due on the calculated 19 March 2027 date.

FIELD GROUP	MINIMUM USEFUL RECORD
Identity	Service, asset ID, environment, owner, criticality
Cryptographic role	Key establishment, signature, data encryption or hash
Implementation	Algorithm, parameters, protocol/profile, library or device version
Trust relationship	Issuer, verifier, key custodian and dependency links
Evidence	Source, observation date, coverage, confidence and reviewer
Decision	Retention need, target state, blocker, action and review date

EO 14412 section 5(d) directs CISA, coordinating with NIST, to release public CBOM guidance within 270 days. The elements must enable automated assessment of cryptographic assets. The table is Qtonic Quantum's working record, not a claim to know the future federal minimum. [UP03]

CycloneDX supplies a structured representation for cryptographic assets and relationships. Preserve stable IDs, schema versions, observation dates and provenance. Keep private keys, recovery secrets and production credentials out of the exported record. [AR02]

Add an acceptance receipt to the exported inventory. Record the schema check, file digest, signing-key identity and declared coverage. Page 28 defines the checks. Page 84 connects them to QScout's CycloneDX 1.7 deliverable.

Design for the guidance update. Assign a schema owner and retain a source-to-field mapping. When the guidance is published, compare every required element with the baseline, record gaps and update the acceptance test. An export format alone does not prove completeness or compliance.

An unknown value remains unknown until evidence resolves it. A blank field must never be converted into a passing security result.

Make the inventory acceptable

A structured CBOM becomes a usable handover when the customer can establish its origin, scope, meaning and freshness.

CycloneDX provides the interchange structure. A valid document can still describe an incomplete population, omit a material relationship or contain an old observation. Decide what constitutes acceptance before the export arrives. [AR02]

The acceptance record below is Qtonic Quantum's proposed buyer test. Use it with the inventory and source-to-field mapping. Keep the verification tool, schema version and signing-key provenance with the result.

Verify structure

Validate against the exact CycloneDX schema version, retain the validator output and resolve every error. A declared specVersion is an input to that check.

Verify origin

Recompute the digest and verify the detached signature using a trusted, separately authenticated public key. Record the signed byte representation and key identifier. A key downloaded beside a file still needs an identity check.

Reconcile coverage

Compare the exported population with the agreed scope. Identify inaccessible assets, inferred values and missing relationships. Keep the denominator and residual gaps in the receipt.

Assign the decision

Connect each material dependency to a service owner, protection objective, migration blocker and review date. Track exceptions and changes as part of the same record.

Ask for the inventory, the verification receipt and the unresolved decisions in the same handover.

Priority, with reasons

A transparent decision framework is more useful than an unexplained score that looks precise.

DIMENSION	QUESTION THE OWNER MUST ANSWER
Consequence	What becomes unacceptable if confidentiality or authenticity fails?
Protection lifetime	How long must data remain private or a signature remain trustworthy?
Exposure	Which relevant information or trust artifacts can leave the boundary?
Dependency	What supplier, verifier or replacement blocks change?
Readiness	Can an approved target be deployed and recovered safely?
Confidence	Which assumptions still lack evidence?

NIST key-management guidance connects protection, use and lifecycle responsibilities. It supplies no universal commercial quantum-exposure score. [AR03]

Assess each dimension using defined high, medium, low and unknown judgments, preserving reasons. Separate urgency from migration readiness: a blocked dependency can still demand immediate action.

Maintain three queues. Protect sensitive flows through supported, acceptable transitions. Resolve consequential unknowns and blockers, then schedule lower-urgency work into refresh cycles. Unsupported legacy systems may need procurement now while production changes remain deferred. Every exception needs a risk owner, review date and closure path.

Expose assumptions. This framework allocates resources under uncertainty. It does not forecast a CRQC arrival date. If adding numerical weights, publish them, test sensitivity and show how changed assumptions alter recommendations.

Move first where the consequence, protection lifetime and exposure justify action. Investigate early where uncertainty could change that decision.

Three services. Three decisions.

Illustrative scenario only. These assumptions and decisions describe no Qtonic Quantum customer and report no measured results.

SERVICE	ILLUSTRATIVE NEXT DECISION
Research transfer	Approve a bounded migration pilot
Public information site	Tie change to the platform refresh
Fleet update signing	Resolve verifier and trust-update path

Hypothetical inputs: one migration team, research confidentiality lasting 15 years, public website content and fleet devices verifying updates for 12 years. Assume supported PQ/T hybrid TLS for a research pilot, a near-term website refresh and no demonstrated supplier PQ verification path for devices. These assumptions are illustrative and assert no market availability.

Pilot research while starting fleet supplier work. Align the website transition with its refresh, subject to identity and contract requirements.

Changing device verifiers may be harder than changing signing.

Challenge the inputs. Six-month research retention could reduce urgency. Assess private website administration separately. A supported device trust update could accelerate fleet migration.

Separate functions. ML-KEM establishes shared keys. ML-DSA signs and verifies. Solving key establishment does not solve device signature verification. [AR05, AR10]

The same enterprise can rationally fund a deployment, a supplier dependency study and a scheduled refresh in the same quarter.

Agility is a tested capability

The meaningful test is whether an organization can replace a cryptographic dependency while preserving the service and its security requirements.

NIST's updated final CSWP 39 describes crypto agility across protocols, applications, software, hardware, firmware and infrastructure. The June 2026 update provides guidance on capabilities and tradeoffs, not certification of a vendor's agility. [AR04]

Qtonic Quantum recommends a controlled change exercise on one representative service. Measure the time to identify dependencies, obtain approval, change configuration, verify the negotiated result and recover the service. Preserve manual steps, unsupported combinations and supplier dependencies as findings.

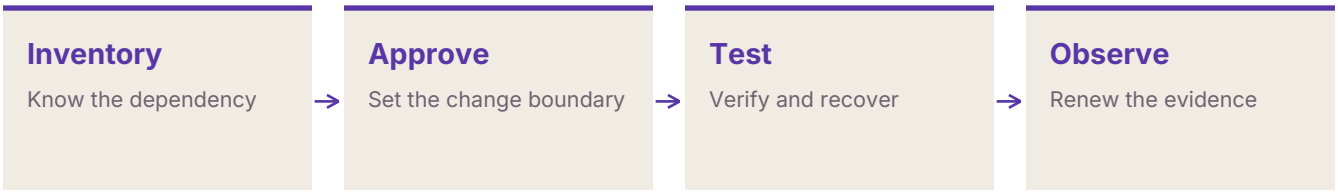
Three layers must work together

Engineering exposes supported choices. Policy defines permitted configurations and exceptions. Operations executes the change and recovery. A configurable algorithm field alone does not establish this capability.

Make the exercise repeatable

Keep the dependency map, release record, interoperability matrix and recovery procedure with the service. Ask a different authorized operator to repeat the transition after a material platform change.

CONTROLLED CHANGE / conceptual change sequence



A dated change record showing the before-and-after profile, observed behavior, service impact, recovery result and unresolved limitations.

Hybrid, precisely defined

Evaluate a hybrid proposal at the protocol and implementation level. Two algorithm names do not establish the security of their combination.

RFC 9954, published in July 2026 as Informational, describes a construction for hybrid key exchange within TLS 1.3. Its intended security goal depends on at least one component remaining secure and on the surrounding construction and assumptions. It does not approve arbitrary combinations in other protocols. [AR06]

ML-KEM is a key-encapsulation mechanism for establishing shared secret key material. It is not the bulk-data cipher and does not itself authenticate the peer. [AR05] Qtonic Quantum therefore recommends that every architecture review separate key establishment, peer authentication, traffic protection and key lifecycle before assessing a hybrid claim.

Ask the supplier to identify the exact protocol specification, algorithm parameters, implementation versions, negotiation behavior and security rationale. A final primitive can appear in a protocol profile that is still a draft. Conversely, an RFC may be Informational rather than an Internet Standards Track document. Record the status and date of each relevant layer.

Review the complete path

Examine how policy selects the profile, how mismatched peers are handled and what evidence confirms the resulting session. Include connection termination points and any onward connection. Test recovery behavior against the service's required protection boundary.

Do not export a claim across functions

Hybrid key agreement and hybrid authentication solve different problems. An architecture that strengthens future confidentiality while retaining traditional certificate signatures should describe that boundary clearly. Where a particular authority prescribes a profile, assess that requirement directly rather than assuming that "hybrid" automatically qualifies.

Accept a named, supported construction for a defined use case. Keep its security rationale separate from the operational evidence that the deployment works.

Follow both connections

A proxied application has distinct security boundaries. A client-facing handshake cannot prove what happens between the provider and the origin.

ONE APPLICATION / TWO CONNECTIONS / SEPARATE EVIDENCE

CONNECTION	KEY EXCHANGE	AUTHENTICATION
Visitor to edge	Inspect the negotiated hybrid group.	Inspect the certificate and trust path separately.
Edge to origin	Automatic Key Exchange prefers supported PQ groups.	ML-DSA requires the applicable origin trust configuration.

Cloudflare example. Availability and an enabled setting are inputs to validation, not an end-to-end security conclusion.

Cloudflare's 8 September announcement says Automatic Key Exchange learns origin capabilities and prefers X25519MLKEM768 where supported. It reports the feature active by default for existing and new domains. This is provider-reported behavior on the Cloudflare-to-origin leg, with deployment and origin conditions to verify. [NW03]

Its 29 July announcement separately added ML-DSA support to Custom Origin Trust Store and Authenticated Origin Pulls. These protect authentication on the origin leg under their product and configuration requirements. They do not establish universal browser-facing post-quantum authentication. [NW04]

TLS 1.3 separates key exchange, authentication and traffic encryption. RFC 10024 specifies the named hybrid groups, but a standard does not establish deployed support. Record the negotiated group and certificate-signature behavior at each termination. [AR07, AR08]

The Qtonic Quantum acceptance record. Name both endpoints, software versions, selected group, certificate chain and trust owner. Capture the origin-side evidence through the customer's approved monitoring. Test renewal, recovery, resumption and exception behavior before widening the claim.

Use the decision, not the headline. For an affected service, assign one owner to origin capability and another to trust configuration. Ask whether the evidence supports confidentiality, authentication or both. Keep service-to-service and administrative connections in the inventory.

Map the trust graph

A new signing algorithm must be usable by issuers, relying parties and the surrounding certificate lifecycle.

RFC 5280 defines the Internet X.509 certificate profile and certification-path validation. FIPS 204 standardizes ML-DSA signatures. Together, these publications do not establish compatibility across a particular certificate ecosystem. [AR09, AR10]

Qtonic Quantum recommends mapping roots, intermediates, enrollment services, certificate stores, applications and verification libraries. For every edge, record the issuer, relying party, accepted profile, owner and update route. Include embedded and recovery environments. Their upgrade paths may differ from the primary application.

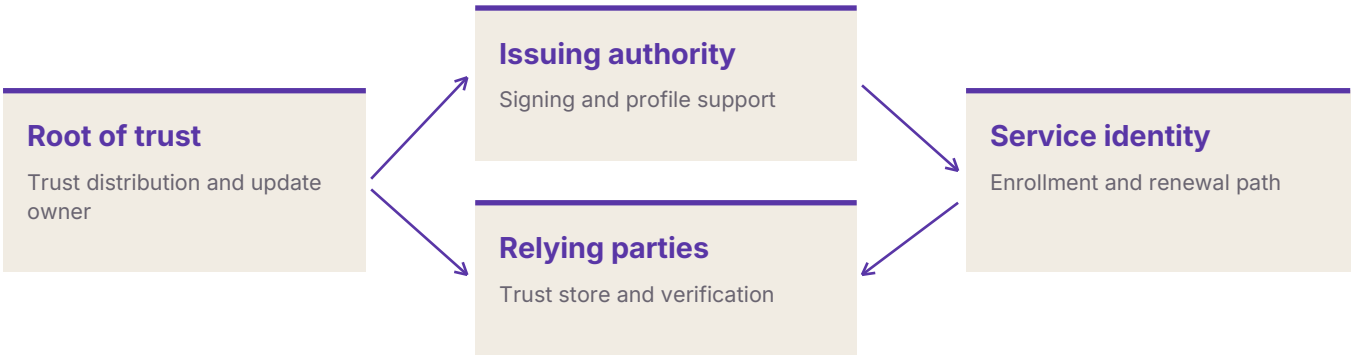
Sequence the trust change

Start within a coordinated trust domain. Separate algorithm choice from certificate profile and implementation support. Test issuance, renewal, revocation and partial deployment, preserving a recovery path for missed issuance or incompatible updates.

Preserve the authority boundary

A private-PKI test does not establish public-browser acceptance or government authorization. Confirm the intended ecosystem, applicable policy and supported verifier behavior.

TRUST DEPENDENCIES / illustrative topology



A certificate can be issued successfully while an intended verifier still cannot accept it.

A trust graph with owner, profile, verifier support, transition order, rollback conditions and unresolved dependencies for each critical certificate path.

Identity beyond certificates

Treat automated trust as a lifecycle of issuance, use, verification, rotation and recovery.

NIST SP 800-57 addresses protection and management of cryptographic keying material across its lifecycle. Qtonic Quantum's machine-identity approach applies that discipline to workloads, devices and automated services without assuming that all identities share one cryptographic design. [AR03]

For each service relationship, determine whether identity relies on certificates, signed tokens, shared secrets, hardware-bound keys or another mechanism. Record the issuer and verifier separately. A token-signing service may migrate before an older verification library. A device may keep a trust anchor longer than the workload it authenticates. Those dependencies need distinct acceptance decisions.

Group identities by verification path and operational owner rather than placing every certificate in a single undifferentiated backlog. Link issuance policy to the service inventory. Include non-production pipelines, disaster recovery and administrative automation, because the transition must remain manageable when the primary identity service is unavailable.

Recommended acceptance exercise

In an approved representative environment, issue the intended identity artifact, verify it with each required consumer, rotate the relevant key or certificate, and confirm the retired artifact is handled according to policy. Exercise the documented recovery procedure. Retain results tied to specific versions and configurations.

Keep authorization visible

A stronger signature does not determine what a workload is allowed to do. Review the identity-to-permission mapping separately, preserving least privilege and service ownership. Likewise, shorter credential lifetime can improve lifecycle control without, by itself, changing the quantum resistance of the underlying algorithm.

Can every required verifier accept the new identity artifact, and can the organization retire the old trust safely?

Protect the update path

The verification system's remaining life can matter as much as the date on which a signature is created.

FIPS 204 standardizes ML-DSA for generating and verifying digital signatures. NIST SP 800-193 separately addresses firmware protection, detection and recovery. Qtonic Quantum recommends considering those responsibilities together when planning changes to update trust. [AR10, AR11]

Inventory the complete release path: build outputs, approval controls, signing service, key custody, distribution, verifier implementation and recovery images. Identify the lifetime of devices that must continue to validate updates. The question is whether a supported verification and trust-update path exists for the fielded population, not simply whether the build system can emit a new signature.

Define how the verifier distinguishes approved artifacts and signing identities throughout a transition. If multiple signatures or certificate paths are proposed, document their acceptance semantics and applicable specification. Do not assume that accepting either signature provides the same security property as requiring both. Engineering convenience is not a substitute for a reviewed trust policy.

Sequence the change safely

Agree the verifier upgrade path before depending on a new production signing format. Include factory images, recovery media, offline devices and replacement components. Validate update continuity in a representative environment and document when old trust can be retired.

Demand recoverability

The acceptance plan should show how an incompatible update or unavailable signing service is handled without losing control of the release process. Preserve approval separation, artifact provenance and auditable key custody. These operating controls remain necessary regardless of the signature algorithm chosen.

For a device expected to remain in service for years, who is contractually responsible for its future verifier and trust-anchor update path?

Prove the protected boundary

A network encryption product should be evaluated by the flows and trust relationships it actually protects.

RFC 9370 is a Proposed Standard that extends IKEv2 to support multiple key exchanges. It provides a protocol framework. A specific post-quantum deployment still needs the applicable algorithm specification, implementation support and accepted configuration. [AR12]

Qtonic Quantum recommends drawing the encryption boundary before evaluating a VPN, tunnel or packet overlay. Identify the endpoints, where plaintext becomes available, who authenticates whom and what remains outside the protected path. Record data-plane encryption separately from control-plane key establishment, management access and certificate authentication.

Ask for evidence tied to the exact release and deployment mode. A product's use of a standardized KEM does not establish the security of its session protocol, replay handling, key lifecycle or peer identity binding. Where an overlay is proposed, compare the additional boundary it creates with the application and infrastructure dependencies it leaves in place.

Operational acceptance

Evaluate representative packet sizes, connection establishment, rekey, failover, restart and path changes in an authorized test environment. Record effective throughput, latency and failure behavior. Agree the service's required behavior when protection cannot be established, and verify that the implementation follows that policy.

Architecture trade-off

A narrowly scoped network layer can be a practical transition mechanism for a defined flow. It should not be described as upgrading stored-data encryption, software signatures or every application identity behind the tunnel. Compare operational burden and supplier dependence alongside protection benefits.

Name the two protected endpoints, the covered traffic, the authentication method and the explicitly excluded paths before making a quantum-security claim.

Follow the keys through recovery

Assess the full protection chain before deciding whether data must be re-encrypted, keys rewrapped or a surrounding service changed.

ML-KEM establishes shared secret key material. It is not a replacement for bulk symmetric encryption. NIST key-management guidance addresses key protection, backup, recovery and lifecycle considerations. [AR05, AR03]

Qtonic Quantum recommends separating the data-encryption layer from the mechanisms that distribute, wrap, recover or authorize access to its keys. Determine what an adversary could retain and which secret or trust relationship protects it. A storage platform's advertised algorithm says little about an export workflow that moves data and keys through another system.

Map primary storage, replicas, snapshots, offline media, legal-hold copies and restore services. Record the required confidentiality lifetime and the remaining life of each dependency. Preserve the distinction between key rotation, rewrapping and re-encryption: their effect depends on the storage design and on whether previous ciphertext or protected key material remains available.

Recommended decision process

Ask the platform and key-management owners to document the current wrapping and recovery path. Identify the supported target, any retained historical artifacts and the effect on restore operations. Choose the smallest change that demonstrably addresses the stated exposure without weakening recoverability.

Acceptance must include a restore

In a representative test environment, verify that an authorized restore works after the proposed transition and that access controls remain effective. Include an older retained backup and a recovery scenario involving unavailable primary services. Record dependencies that cannot yet be exercised and the owner of that residual uncertainty.

Changing a gateway or a current session cannot retroactively protect copies already acquired outside that boundary. Describe the protection achieved from the transition onward.

Cloud defaults can move your deadline

A provider rollout can change the customer's work this quarter. The protected connection and the remaining responsibility must stay visible.

AWS describes a shared-responsibility model whose customer obligations depend on the selected service. The practical question is which team controls each connection, key and deployment setting. [AR13]

Google Cloud's 26 August documentation scopes X25519MLKEM768 support to frontend TLS. Default enablement begins in October 2026 for load balancers without a policy or explicit PQC setting. An explicit DEFERRED setting postpones enablement to October 2027. These are provider plans with defined product and client conditions. [OP01]

The 11 August Google Cloud roadmap reports hybrid support in application and proxy load balancing and separates confidentiality work from its later authentication program. A key-exchange rollout does not complete certificate or identity migration. [OP02]

Own the October decision

Identify the target proxy, attached policy, current feature setting and supported client population. Test representative application paths before the provider changes the default. If compatibility requires a deferral, record the reason, owner and remediation date.

Trace the next connection

Assess the load-balancer-to-backend leg separately. Preserve the negotiated profile and certificate behavior at each termination. A protected frontend cannot establish protection for a downstream service, stored copy or signing workflow.

Make the output usable

The Q4 pilot should deliver a configuration record, compatibility results, observed negotiation, recovery steps and a decision. Link them to the service CBOM so a later default or release change triggers a focused review.

A published rollout date becomes useful when it has a service owner, a compatibility test and an explicit decision.

A lifecycle strategy for OT

Protecting the mission requires a transition that respects safety, reliability and the equipment's supported operating envelope.

NIST SP 800-82 Rev. 3 addresses OT security while recognizing performance, reliability and safety requirements. It provides an OT security framework. It does not certify a post-quantum retrofit or prescribe one migration architecture for every plant. [AR14]

Qtonic Quantum recommends starting with the asset owner and engineering authority. Identify control functions, field devices, remote access, maintenance workflows, signed updates and long-lived trust anchors. Separate equipment that can receive a supported software change from equipment requiring a gateway, supplier intervention or planned replacement.

Where direct endpoint change is constrained, evaluate compensating architecture for the specific exposed flow. A gateway can alter a communication boundary without changing the cryptography inside a controller or the signature verifier in its firmware. Document that distinction and the consequence of the remaining dependency. Retain a funded replacement or remediation route for exceptions.

Use the right test environment

Agree the test scope with operations and safety personnel. Use representative equipment or an approved staging environment to assess timing, failure recovery and maintenance compatibility. Collection and change methods must fit the operating constraints. An IT procedure should not be imported into OT without review.

Procure the future update path

For new equipment, request the supported method for changing trust anchors, cryptographic libraries and signature verification. Specify responsibility for updates, the support horizon and evidence of compatibility with required management systems. Resolve lifecycle commitments before a long-lived platform becomes difficult to replace.

A migration plan is incomplete when it names a stronger algorithm but cannot explain how the equipment remains safe, maintainable and recoverable.

ORIGINAL RESEARCH / QQ-TLS-LOCAL-2026-09

A hybrid handshake has more than one proof

Original TLS study: eighty complete, certificate-verified handshakes connect protocol choice to observed bytes and authentication.

80 CERTIFICATE-VERIFIED TLS 1.3 HANDSHAKES / FOUR CONFIGURATIONS

SERVER IDENTITY	KEY EXCHANGE	RECORD BYTES	COMPLETED
ECDSA P-256	X25519	1,029-1,031	20 / 20
ECDSA P-256	Hybrid ML-KEM	3,351-3,353	20 / 20
RSA-2048	X25519	1,613	20 / 20
RSA-2048	Hybrid ML-KEM	3,935	20 / 20

Hybrid = X25519MLKEM768. Record bytes are the complete local TLS handshake records, before application data. Both identity types use classical authentication. No TCP or internet path was measured.

We completed 20 fresh handshakes for each of four configurations using Python 3.12.13 and OpenSSL 3.5.7. The client verified the server certificate and the test hostname "report.invalid", then both sides exchanged synthetic application data. The transport was in-memory SSL, with no network sockets. [TS01]

The default configurations selected X25519MLKEM768. Their authentication remained ECDSA P-256 or RSA-PSS, exactly as configured. Every case reported the same TLS_AES_256_GCM_SHA384 cipher suite. A cipher-suite name therefore did not distinguish the key-exchange group or server signature.

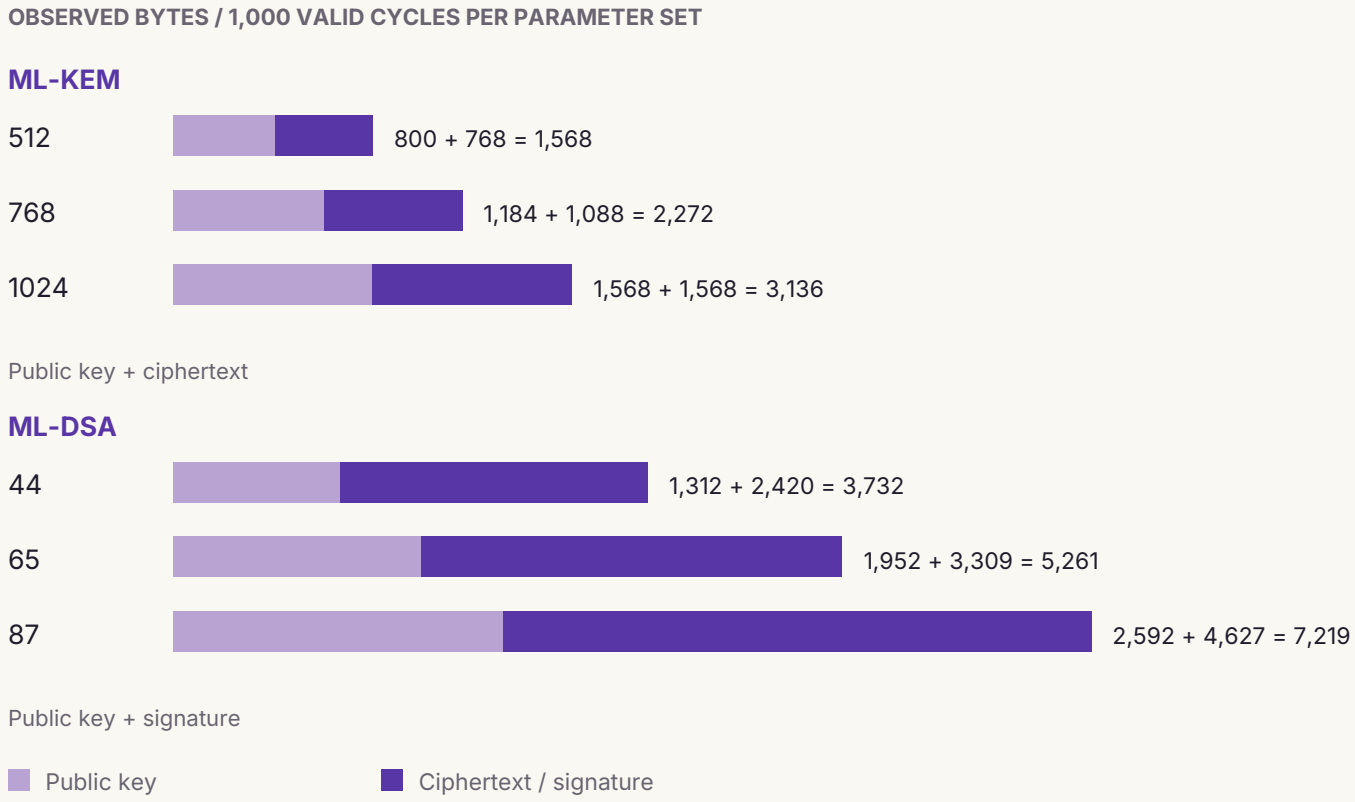
One lesson for acceptance. Record all three: protocol and cipher suite, negotiated key-exchange group, and certificate/signature behavior. An observed hybrid exchange supports its stated confidentiality claim. Authentication needs its own migration evidence.

What this study establishes. The four configurations worked in this disclosed runtime. It does not establish internet interoperability, production certificate-chain behavior, ML-DSA authentication, fleet compatibility or latency. The complete evidence is attached, with access on page 45. [TS01, TS02]

ORIGINAL RESEARCH / QQ-PQC-LOCAL-2026-09

The bytes are part of the architecture

Original Qtonic Quantum publication experiment: observed key, ciphertext and signature lengths across six standardized parameter sets.



We generated fresh keys and completed 1,000 valid cycles per parameter set. Every observed length matched FIPS 203 Table 3 or FIPS 204 Table 2. This verifies the observed encoding lengths, not the security of the implementation. [OR01, OR02, OR03]

ML-KEM-1024 used a 1,568-byte public key and a 1,568-byte ciphertext. Their combined 3,136 bytes exclude authentication, framing and any traditional hybrid component. They are exchanged at different steps and are not one measured network packet.

ML-DSA-87 produced 4,627-byte signatures on the 1,024-byte test message. The corresponding public key was 2,592 bytes. The 7,219-byte key-plus-signature sum is a sizing aid, not a certificate-chain or protocol-handshake measurement.

The engineering consequence. Budget for the complete exchange and the actual credential lifecycle. Key reuse, caching, protocol framing and certificate chains change what travels over a link. Higher parameter sets should follow the required security profile, not a performance ranking.

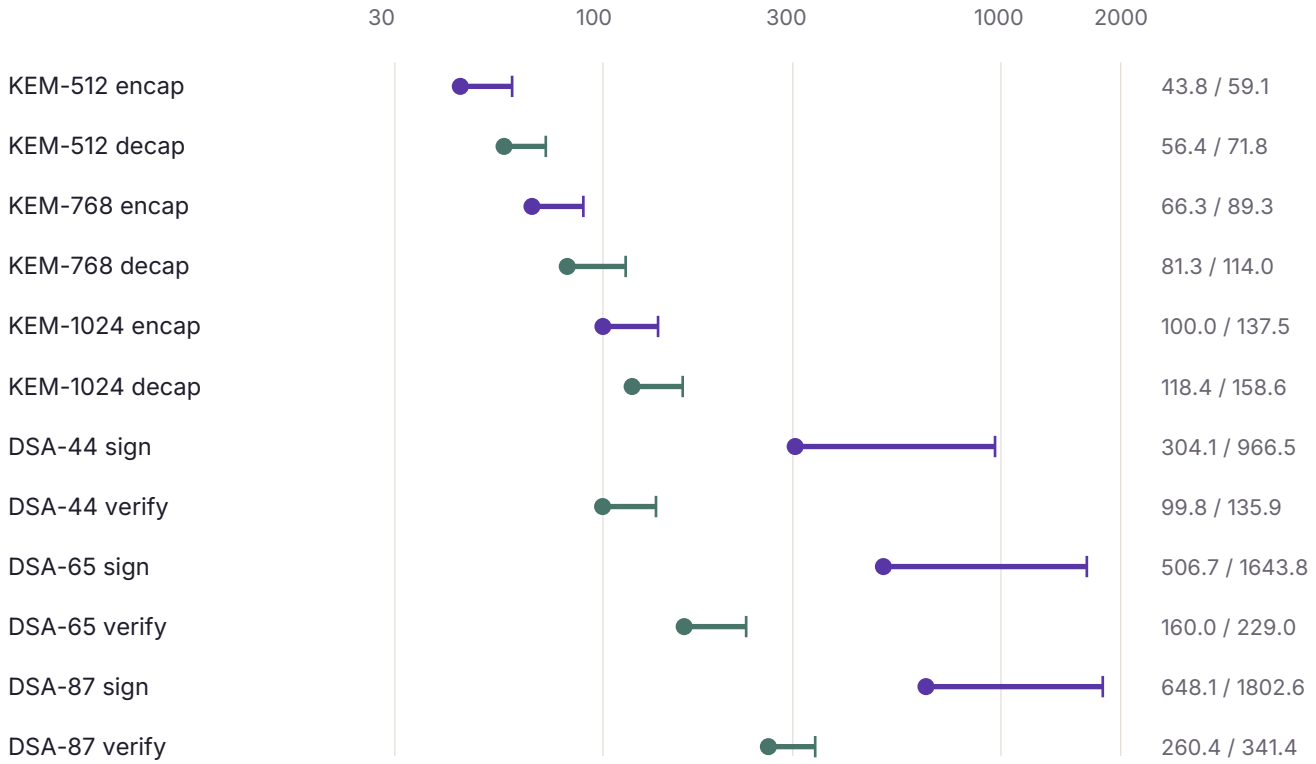
ORIGINAL RESEARCH / QQ-PQC-LOCAL-2026-09

Latency has a distribution

18,000 recorded operation timings. Medians show the typical call. The 95th percentile shows why a single average is insufficient.

LOCAL CALL LATENCY / MICROSECONDS / MEDIAN TO P95

Key generation and full observations are in the companion dataset.



Logarithmic axis. Dot = median. End tick = nearest-rank p95.

Each plotted operation has 1,000 observations in five blocks. The pqcrypto 0.3.4 run used one CPU-pinned Linux container and includes Python/CFFI overhead. Signing p95 was about 2.8-3.2 times the median. [OR01, OR04]

FIPS 204 defines a Fiat-Shamir-with-Aborts rejection-sampling loop: signing repeats candidate generation until its checks pass. Variable repetitions are an algorithmic source of variable work. This is sourced background. Our run did not count iterations or isolate their contribution to latency. [OR03]

What the buyer should test. Preserve tail latency when evaluating a signing service. Measure it under the actual workload and concurrency. Neither the distribution nor this algorithm explanation establishes side-channel security or QShield performance.

ORIGINAL RESEARCH / QQ-TLS-LOCAL-2026-09

The 50 bytes a field-only budget misses

The specified algorithm fields are correct. An observed handshake adds configuration choices that the narrow formula excludes.

FROM SPECIFIED FIELDS TO OBSERVED HELLO GROWTH / BYTES

01 / SELECTED KEY-EXCHANGE FIELDS

ROLE	HYBRID	X25519	INCREASE
Client	1,216	32	+1,184
Server	1,120	32	+1,088
Net field increase			2,272

02 / LOCAL CONFIGURATION

+36 Extra client share + entry header

+14 Additional supported-group IDs

2,272 field increase

+ 50 configuration extras

= 2,322 observed hello growth

Field sizes: RFC 10024. The extra bytes reflect this OpenSSL 3.5.7 setup. These are hello-message bytes, before network framing.

RFC 10024 specifies 1,216 client and 1,120 server key_exchange bytes for X25519MLKEM768. Against two 32-byte X25519 shares, the increase is 2,272 bytes. Our hybrid handshakes reproduced those exact field lengths. [AR07, TS01]

The complete hello messages grew by 2,322 bytes. The default client also offered an X25519 share and seven additional supported-group identifiers. Those choices add 36 and 14 bytes respectively. The retained hello messages let readers reproduce the reconciliation. [TS01]

With RSA authentication, total TLS handshake-record bytes rose from 1,613 to 3,935. ECDSA runs varied slightly with the encoded CertificateVerify signature. These are observations in one configured runtime, with one lab leaf certificate per identity type, no resumption and tickets disabled.

The planning consequence. Budget from the deployed handshake configuration and full-handshake volume. Add network framing, retries, real certificate chains and path constraints when testing the service. These local totals exclude network transport and do not measure throughput or latency. [TS01, TS02]

RESEARCH AND PROCUREMENT / THREE ATTACHED ARTIFACTS

Two studies. Evidence you can carry.

Two research archives and the CBOM acceptance sheet are attached. Save the originals, verify their hashes and inspect the method.

PRIMITIVE STUDY

18,000 timings

6 parameter sets
6,000 valid cycles

TLS STUDY

80 handshakes

4 configurations
40 hybrid handshakes

Primitive study QQ-PQC-LOCAL-2026-09: 18,000 timings, six parameter sets and 6,000 valid cycles. Collected 7 September on one CPU-pinned shared Linux host through pqcrypto 0.3.4. Each set has five blocks of 200 cycles, following 20 excluded warm-ups. [OR01]

TLS study QQ-TLS-LOCAL-2026-09: 80 handshakes across four configurations. Collected 8 September using Python 3.12.13 and OpenSSL 3.5.7, with certificate and hostname checks. Retained records and messages support the byte ledger. [TS01]

Recheck and reproduce. Run recompute.py for the primitive study or recompute_tls.py for the TLS study. Each README also explains how to collect new observations.

Keep the conclusion in scope. AI-assisted publication experiments. These are not product tests, field studies or FIPS validation. Neither archive includes production credentials or test private keys.

SAVE. VERIFY. REUSE.

Save files using the paperclips or a PDF reader's Attachments panel. Browser viewers may hide attachments. Verify the hashes below. ZIPs contain study READMEs.

01 / PRIMITIVE STUDY Qtonic_Quantum_Original_Research_Q4_2026.zip

SHA-256 ebb8cb716dc568dfb70cca04f5f89ebcb2cf74b9b3a75451b7ffeeec62eef6f4

02 / TLS STUDY Qtonic_Quantum_TLS_Proof_Study_Q4_2026.zip

SHA-256 d5728e297dab86ad884baf1815876545dad976f41f3274d14c9282a989df8a20

03 / CBOM SHEET Qtonic_Quantum_CBOM_Acceptance_Requirements.pdf

SHA-256 e62f5978dd72a4b3d48882fbe4f4440761ac913146e8d3f3ac9862ffbe41f13c

Research desk & separate copies **qtonicquantum.com/contact**

03

Industry and buyer decisions

Protection has a business context.

Industrial control systems / generated editorial illustration

01 / INDUSTRY LENS

Finance

A payment service is ready only when its counterparties, signing infrastructure, operational controls and recovery arrangements can move together.

Treasury's August 2026 task force puts financial-sector migration, supplier dependencies and emerging-technology risks on a shared agenda. [UP01] Qtonic Quantum recommends converting that signal into one funded business-service decision with named counterparties and explicit acceptance evidence.

The BIS Innovation Hub's Project Leap Phase 2 tested post-quantum signatures in an operational payment system while sending liquidity transfers. Its December 2025 report identifies component compatibility work and significant performance differences between traditional and post-quantum algorithms. The experiment supports feasibility, not universal production readiness. [SC01]

Organize the program around payment authorization, interbank messaging, onboarding, market connectivity and long-lived records. Separate retained-information confidentiality from instruction authenticity. A transport upgrade does not replace application signatures, hardware security module dependencies or counterparty trust agreements.

Map the trust dependency

Identify who signs, who verifies, where keys reside, who accepts the signatures and which technology version controls the dependency. Assign the service owner to obtain evidence from processors, exchanges, custodians and suppliers.

Measure the operating envelope

Test transaction completion, tail latency, queue growth and recovery under representative workloads. Include peak periods, certificate replacement and failover. Assess capacity, message size and integration changes before selecting an implementation.

Agree on acceptance

Have the business owner, technology owner and risk function agree on allowable disruption and residual exposure. Preserve the tested configurations and counterparties. Internal success does not establish external acceptance.

For Q4, fund one complete business-service migration decision with named counterparties and acceptance evidence, then use the results to size the next wave.

02 / INDUSTRY LENS

Healthcare

Quantum readiness in healthcare has two clocks: the useful life of sensitive information and the safe replacement cycle of clinical technology.

The HIPAA Security Rule applies to electronic protected health information held by covered entities and business associates and requires administrative, physical and technical safeguards. HHS's reviewed source identifies the January 2025 Security Rule changes as proposed. This report does not turn that proposal into a current post-quantum mandate. [SC02]

FDA's February 2026 final medical-device cybersecurity guidance addresses device design, labeling and premarket documentation, including recommendations concerning statutory cyber-device requirements. Its device scope differs from a hospital's enterprise HIPAA obligations. Neither an enterprise encryption purchase nor a cryptographic inventory automatically resolves both. [SC17]

Prioritize information with lasting sensitivity

Qtonic Quantum recommends classifying genomic data, longitudinal records, research datasets and retained patient communications by their actual confidentiality requirements. Include backups, research exchanges and outsourced hosting. Confirm whether deletion is possible and permitted before treating retention reduction as a risk treatment.

Treat clinical changes as clinical changes

Map device software signing, remote support, gateways and manufacturer update paths. Involve clinical engineering and the device manufacturer before changing a production connection. Define how a failed upgrade affects treatment availability, and preserve approved emergency access and recovery arrangements.

Ask suppliers for a supported path

Request model and version-specific cryptographic dependencies, support horizons and upgrade evidence. Separate changes the provider can make from changes requiring manufacturer action. A network overlay can protect a defined link while leaving device authentication and stored records outside its boundary.

The Q4 deliverable should connect high-sensitivity data flows to clinical owners, supported supplier actions and patient-safe change windows.

03 / INDUSTRY LENS

Transportation

For fleets, airports, rail and logistics networks, the best migration sequence follows service continuity, supplier responsibility and engineering constraints.

EASA's Part-IS materials address management of information-security risks with potential effects on aviation safety. They are European aviation instruments with defined organizational scope, not a blanket post-quantum requirement for every transportation business. Determine the relevant authority, operation and system boundary before mapping obligations. [SC03]

NIST's operational-technology guidance explicitly recognizes performance, reliability and safety requirements, including transportation systems. Qtonic Quantum's recommendation is to bring cryptographic change into the existing safety and engineering process wherever a change can affect an operational service. Corporate IT and safety-relevant infrastructure should share a risk model without sharing an indiscriminate deployment schedule. [SC07]

Map the full service path

Identify fleet-to-ground communications, maintenance data, software distribution, remote access and carrier interconnections. Record which trust anchors are embedded, which can be replaced remotely, and who controls the relevant component. The owner of a network segment may not own its endpoint.

Separate refresh opportunities from hard constraints

Use planned infrastructure renewal to require supported algorithm transitions and exportable inventory evidence. For installed equipment, assess memory, message-size, timing and maintenance constraints. Obtain the responsible engineering judgment on certification or approval consequences instead of assuming every cryptographic change is administratively minor.

Build acceptance around operational behavior

Test representative loss, delay, restart and failover conditions in an approved environment. Demonstrate that expected services recover within agreed bounds. Record explicitly whether the evaluation covers passenger systems, enterprise connectivity, operational communications or safety-relevant functions. Those scopes are not interchangeable.

For Q4, add cryptographic lifecycle requirements to the next major transport procurement and name the engineering owner for every proposed operational change.

04 / INDUSTRY LENS

Defense

An algorithm choice is one part of a defense acquisition. Mission assurance depends on the implementation, authorization path and evidence for the actual system.

NSA's December 2024 CNSA 2.0 FAQ addresses National Security System owners, operators and vendors. It also offers guidance relevant to defense organizations and the industrial base. It explicitly does not dictate algorithm choices to every entity outside NSS. Establish system applicability before claiming a CNSA requirement. [SC04]

The FAQ distinguishes standardized algorithms, validated implementations and product-specific implementation guidance. It also highlights firmware roots of trust that can be difficult to replace over a system's lifetime. These distinctions prevent a common procurement error: equating use of an approved mathematical algorithm with approval of a complete mission system. [SC04]

Start from the mission thread

Qtonic Quantum recommends mapping the information exchange from origin to authorized consumer, including platform identity, distribution services, deployed endpoints and key management. Document confidentiality duration and the consequences of unauthorized commands or software separately. Different mission effects can justify different migration priorities.

Specify the operating environment

Require evidence for bandwidth, intermittent connectivity, recovery, credential provisioning and key replacement under representative conditions. Include platform resource limits and the support chain for deployed systems. Benchmarks from a commercial data center cannot be treated as proof for a constrained operational environment.

Keep research claims inside their boundary

A prototype can demonstrate a narrowly defined function and produce engineering evidence. It does not by itself establish an authorization to operate, NSA approval, NIAP validation or suitability for classified use. Acquisition documents should distinguish demonstrated behavior, planned capability and the remaining approval work.

For Q4, produce a mission-specific evidence plan that identifies the customer's authoritative requirements and the officials responsible for acceptance.

05 / INDUSTRY LENS

Space

For space systems, a component's useful life can outlast several generations of terrestrial security products. The trust architecture needs its own replacement plan.

NIST IR 8441 describes hybrid satellite networks as combinations of independently owned and operated components with differing assurance levels. Its cybersecurity profile emphasizes the interfaces between participants. Published in 2023, it references CSF 1.1. It should not be presented as a new CSF 2.0 or post-quantum certification. [SC05]

Qtonic Quantum's analysis applies that interface discipline to cryptography. Separate the space segment, ground segment, user terminals, hosted payloads and operational partners. A protected ground-network link may reduce a specific exposure while leaving onboard software verification, command authentication or terminal enrollment unchanged. Make each boundary visible in the assurance claim.

Identify what can still change

Record trust anchors, verification logic, available memory, update mechanisms and recovery options before design freeze. Determine whether a future algorithm transition is remotely supportable or depends on hardware replacement. Document the authority allowed to initiate changes and the consequences of losing that authority.

Evaluate mission conditions

Use representative contact windows, link budgets and interruption patterns to evaluate proposed cryptographic changes. Consider the size of identity material and update packages as well as processing performance. A successful laboratory handshake is insufficient evidence of successful operation across the mission's actual communication constraints.

Contract for the shared boundary

Assign responsibilities for credential issuance, revocation, key recovery, telemetry and incident coordination across operators and suppliers. Require interface-level evidence and supported upgrade commitments. Do not assume a satellite operator, ground provider and terminal manufacturer share a single cryptographic roadmap or acceptance process.

The Q4 question is practical: can the mission replace its critical trust dependencies during its planned life, and who has demonstrated that path?

06 / INDUSTRY LENS

Legal services

The end of a transaction or dispute does not automatically end the sensitivity of the information a law firm holds.

ABA Model Rule 1.6(c) calls for reasonable efforts to prevent unauthorized disclosure of, or access to, information relating to client representation. It is a model rule, not a universal standalone law. The applicable jurisdiction's adopted rules and the engagement's obligations govern. It does not prescribe a particular post-quantum product. [SC06]

Qtonic Quantum recommends that legal organizations classify cryptographic exposure by matter and information lifecycle. Trade secrets, sensitive investigations, deal materials and litigation records can retain value after a file closes. The right inquiry is what must remain confidential, for how long, where copies travel and which party controls the protection.

Follow the matter beyond email

Include document management, client portals, virtual data rooms, e-discovery, translation providers, expert witnesses and archived exports. Record identity providers and certificate dependencies as well as encryption settings. Secure transport to one platform does not establish protection across every service used on a matter.

Make retention decisions with counsel

Separate business convenience from preservation duties and client instructions. Do not delete retained information merely to reduce quantum exposure. Record where a legal hold, contract or other requirement constrains migration, re-encryption or disposal, and identify who can approve the appropriate treatment.

Turn supplier assurances into evidence

Ask providers which service boundaries use post-quantum mechanisms, which cryptographic functions remain conventional and which versions support change. Request precise scope, dates and limitations. Preserve the firm's decision record and supporting evidence so that a future reviewer can understand the basis for reasonable action.

For Q4, select one sensitive matter workflow and document the complete chain of custody, retention and cryptographic ownership across its providers.

07 / INDUSTRY LENS

Manufacturing

Industrial migration should protect the process, the product and the engineering knowledge without assuming that every controller can be changed like a laptop.

NIST SP 800-82 Revision 3 treats operational technology as systems that interact with the physical environment and addresses their particular reliability, performance and safety needs. Those constraints are essential context for quantum planning in manufacturing. The publication is general OT security guidance, not a plant-level post-quantum approval. [SC07]

Qtonic Quantum recommends separating three exposures: confidential engineering information, authenticated access to production systems, and the integrity of software or firmware installed in equipment. A single label such as "encrypted factory" hides these differences. Each requires an accountable owner, a supported treatment and evidence that the treatment preserves production requirements.

Use passive and supplier evidence first

Begin with engineering inventories, architecture records, approved configuration exports and manufacturer documentation. Establish the permitted assessment method with plant operators. Discovery should respect production constraints and should not assume that active interaction with every device is acceptable or technically reliable.

Prioritize durable dependencies

Map boot verification, signed updates, industrial gateways, remote maintenance and product-connected services. Record components that cannot change their verification algorithm. Use scheduled maintenance, equipment replacement and new product design to introduce supported transition paths before those dependencies become expensive to alter.

Evaluate the whole change cost

Include validation time, engineering review, spare equipment, support contracts and downtime exposure in procurement comparisons. A lower license price can be outweighed by repeated qualification work. Where direct migration is unavailable, document the protection and remaining limitations of segmentation or a gateway-based treatment.

The Q4 deliverable is a plant-approved migration map that connects cryptographic dependencies to maintenance windows, manufacturer support and production acceptance criteria.

08 / INDUSTRY LENS

Software & SaaS

For software providers, quantum readiness becomes credible when customers can see exactly which service boundary changed and verify its operating behavior.

NIST's Secure Software Development Framework provides a common vocabulary for secure development and communication between purchasers and suppliers. It supports lifecycle discipline. It is not a certificate that a particular service is quantum resistant. Cryptographic migration should be managed as a supported product change with explicit scope. [SC08]

Qtonic Quantum recommends mapping public interfaces, service-to-service connections, tenant identity, software signing, stored data and key management separately. Browser-to-edge protection does not describe the edge-to-origin connection or an application's signature scheme. A release should communicate those boundaries in terms a customer can use in its own architecture and risk record.

Make dependency ownership visible

Identify cryptographic libraries, runtime providers, certificates, signing services and third-party integrations. Record which team owns each upgrade and which release contains it. Track where a platform update changes behavior automatically and where customer configuration or an endpoint upgrade is still required.

Test negotiated behavior and recovery

In approved environments, confirm the protocol and algorithm actually in use across supported clients. Measure latency, resource use and failure behavior. Test credential renewal, recovery and mixed-version deployments. Preserve evidence of unsupported clients and remaining conventional paths rather than silently counting them as migrated.

Publish a usable customer statement

State supported versions, required settings, service boundaries, validation status and limitations. Offer evidence that is specific enough for procurement and assurance reviews without exposing sensitive operational details. Maintain the statement as deployments change so that a successful release does not become a stale enterprise-wide claim.

The Q4 release gate should require a customer-readable scope statement backed by reproducible tests for the advertised functionality.

09 / INDUSTRY LENS

Telecom

A carrier's migration depends on peers, equipment suppliers, enterprise customers and long-lived endpoints that do not all move on the same schedule.

GSMA's PQ.03 Guidelines for Telecom Use Cases provides industry guidance for the transition to quantum-safe cryptography. Its existence supports a coordinated sector approach. It does not establish that every network function, roaming relationship or deployed device already supports a final interoperable implementation. [SC09]

Qtonic Quantum recommends dividing the carrier estate by trust relationship: customer access, network management, core services, interconnect, supplier access and software distribution. Identify where cryptographic functions terminate and which party controls the next connection. An enterprise transport service can offer a defined protection boundary without resolving a customer's application-layer cryptography.

Build the supplier and peer map

Require product-family and software-release detail for cryptographic capabilities and upgrade paths. Include management interfaces, certificate authorities and signing dependencies. For shared services, identify the party that can approve changes and the counterparties whose acceptance is necessary for continuity.

Evaluate scale and heterogeneity

Test representative endpoint diversity, connection establishment rates, certificate operations and failover. Record resource and message-size effects at expected scale. A small test with two compatible devices provides useful evidence but cannot justify a statement covering a heterogeneous national network.

Separate service offers from internal readiness

Describe a quantum-resistant customer service by its actual endpoints, algorithms, key management and supported configuration. Maintain a separate internal transition record for carrier infrastructure. Protecting one commercial service does not demonstrate complete migration of signaling, operations systems, firmware or the customer's stored information.

For Q4, agree on one interconnection or enterprise-service pilot with both endpoint owners and a published acceptance boundary before expanding deployment.

10 / INDUSTRY LENS

Quantum & HPC

Buying access to a quantum processor establishes a computing capability. It does not establish that the surrounding organization is ready for quantum-era security risk.

DOE's description of quantum information science distinguishes computing, simulation, networking and sensing. It also describes supporting facilities, testbeds and other infrastructure. These are related research and capability domains, not interchangeable security controls. A quantum computer is not a general substitute for classical computing infrastructure. [SC10]

Qtonic Quantum recommends two separate decisions for high-performance computing and quantum facilities. First, determine the scientific or computational value of the system. Second, assess the security of access, control software, data movement, updates, identities and suppliers. A favorable answer to the first question cannot be used as evidence for the second.

Protect the conventional control environment

Map operator workstations, management services, scheduling, remote access and software distribution. Establish who can submit jobs, change configurations, approve updates and retrieve outputs. Include the supplier's access arrangements and the facility's ability to investigate an operational event.

Classify research and customer information

Determine which input datasets, algorithms, experimental results and retained logs have confidentiality or integrity requirements. Record tenancy boundaries and external collaboration paths. Apply the same lifecycle reasoning used elsewhere in the enterprise, including backups and identities that authorize access to them.

Write two acceptance packages

Evaluate computing performance with workload-relevant scientific metrics and clearly bounded assumptions. Evaluate cybersecurity with evidence of isolation, access control, supported cryptographic transitions and recovery. Do not accept physical qubit count, an equipment photograph or a computing benchmark as a measure of post-quantum protection.

For Q4, ensure every quantum or HPC acquisition has a separate cybersecurity owner, risk boundary and acceptance record alongside its technical computing evaluation.

Buy a supported transition

A durable purchase gives the buyer an enforceable path from today's supported configuration to tomorrow's requirements, with evidence at each decision point.

NIST SP 800-161 Revision 1 integrates cybersecurity supply-chain risk management into organizational risk activities and addresses assessment of products and services. Qtonic Quantum applies that lifecycle approach to cryptographic procurement: inspect the supplier's delivery obligations, dependency visibility and maintenance capability alongside the advertised algorithms. [SC11]

A request for information should establish what is available now, what is under development and what depends on another supplier. A request for proposal should convert the selected requirements into deliverables. Contract award should not collapse these different maturity states into a single claim of readiness.

Before selection

Define the assets, trust boundaries, data lifetimes and operating conditions to be protected. Require a product-specific cryptographic inventory and identify external dependencies. Ask for versioned documentation, supported configurations, published security maintenance commitments and the evidence available for each material claim.

Before acceptance

Agree on test cases, performance bounds, failure handling and upgrade conditions before demonstration. Require the deployed version to match the evaluated version or document the differences. Record which systems and counterparties participated so that acceptance remains tied to the tested environment.

After deployment

Require notice of material cryptographic changes, unsupported components and revised transition commitments. Set review triggers for product replacement, contract renewal and supplier ownership changes. Preserve the ability to export configuration and inventory evidence so that changing providers does not destroy the buyer's understanding of its dependencies.

For Q4, add a cryptographic lifecycle annex to one live procurement and make evidence delivery part of acceptance, maintenance and exit.

Write the acceptance contract

"Quantum ready" becomes a useful procurement statement only when the parties agree on its exact scope, configuration, evidence and continuing obligations.

NIST's CMVP maintains records for validated cryptographic modules, including validation status and the evaluated version and environment. [SC18] The program cautions that appearance on its Modules In Process list does not guarantee final validation. Buyers should distinguish an algorithm claim, a module certificate and a supplier's overall product statement. [SC12]

Qtonic Quantum recommends using counsel-reviewed technical schedules rather than an undefined marketing term as the acceptance standard. The schedule should identify protected functions, supported algorithms and parameters, covered product versions, operational environments and excluded dependencies. Contract language should reflect the buyer's specific requirements and the supplier's demonstrable commitments.

Require precise evidence

Where validation is required, identify the relevant certificate and verify its scope, status, module version and approved operating conditions. Ask the supplier to explain how the delivered configuration uses that module. A pending submission should remain a pending submission in the contract and the acceptance record. [SC18]

Specify change and support duties

Set notification duties for security defects, algorithm changes, dependency changes and missed migration milestones. Define support horizons and the process for qualifying an upgrade. Identify the evidence the supplier must preserve and provide when an incident or material change affects the buyer's assessment.

Agree on practical remedies

Match remedies to the business need: correction, retest, replacement, termination or assisted transition, as negotiated. Allocate testing costs and define the decision authority. Do not promise immunity from future cryptanalysis. Require transparent capability statements and a workable response when a dependency must change.

The Q4 contract test is simple: could an independent reviewer determine whether the supplier delivered the exact protection the buyer purchased?

Give the pilot a decision

A useful pilot resolves a bounded uncertainty. It is strongest when failure is measurable, limitations are recorded and the next decision is already defined.

NIST's NCCoE migration project separates cryptographic discovery from interoperability testing and describes resolving compatibility issues in controlled, non-production environments. It lists SP 1800-38A, B and C as preliminary drafts. These materials support structured experimentation. Their draft status should remain visible when they are cited. [SC13]

Qtonic Quantum recommends writing the pilot hypothesis before choosing a demonstration. For example: can the selected application path meet its agreed service requirements after a supported cryptographic change, across the clients and counterparties in scope? That question creates a testable decision without claiming the entire enterprise is protected.

Define the entry conditions

Name the owners, approved environment, representative data, software versions and baseline measurements. Establish the allowed changes and the recovery plan. Identify dependencies excluded from the pilot and any differences from production that could materially affect interpretation.

Measure the behavior that matters

Capture successful operations, rejected operations, resource use, relevant latency measures and recovery outcomes. Include supported mixed-version conditions and planned credential changes. Preserve both successful and unsuccessful results. A headline average without the workload, distribution and configuration is weak evidence for a deployment decision.

Make the exit criteria consequential

Use predetermined acceptance bounds and have the responsible service owner review exceptions. End with a deploy, revise, defer or reject decision for the defined scope. List the additional evidence required for the next environment. A successful pilot should narrow uncertainty rather than become a permanent substitute for operational acceptance.

For Q4, commission a pilot only when its acceptance criteria connect directly to an identified procurement or deployment decision.

Make evidence reproducible

An evidence package should let a qualified reviewer trace a claim to a system boundary, configuration, test result and accountable decision.

NIST's supply-chain guidance emphasizes understanding how acquired technology is developed, integrated and deployed. Its SSDF also gives purchasers and suppliers a shared vocabulary for secure software practices. Qtonic Quantum's evidence model turns those principles into a compact record suitable for a cryptographic migration decision. [SC11][SC08]

The package should distinguish supplier assertions from observations and customer decisions. Preserve enough detail to explain what was tested without distributing secrets or unnecessary personal information. Evidence must remain intelligible when the original project team changes, the software version advances or an assurance reviewer asks a narrower question.

Record the boundary and provenance

Include the approved scope, architecture, asset identifiers, software and module versions, configuration references, dates and responsible people. Identify the origin of each artifact. Record untested components and differences from production alongside the headline result, so exclusions cannot disappear in a summary.

Preserve the observations

Retain the test procedure, baseline, workload description, relevant outputs, failures and retest history. Use controlled storage, access restrictions and integrity records appropriate to the information. A signature or hash can help detect a changed artifact. It does not prove that the original test was correctly designed.

Attach the acceptance decision

Map each requirement to evidence, a result and any exception. Identify the person accepting residual risk, the rationale and the next review trigger. Keep customer-facing summaries consistent with the detailed record. Store supplier commitments and support limitations with the technical results rather than in a disconnected sales folder.

The Q4 standard is traceability: every material readiness claim should have a bounded statement, a supporting artifact and an owner who can explain it.

Prepare for cryptographic disruption

A cryptographic incident can be an implementation defect, exposed key, invalid trust relationship or disruptive migration. Response plans should cover those plausible events now.

NIST SP 800-61 Revision 3, finalized in April 2025, incorporates incident response across the cybersecurity risk-management activities described by CSF 2.0. Qtonic Quantum recommends applying that discipline to cryptographic dependencies instead of waiting for a hypothetical quantum-computing milestone to trigger preparation. [SC14]

A suspicious event is not evidence of quantum cryptanalysis. Investigators should evaluate ordinary explanations such as credential theft, endpoint compromise, configuration error or software vulnerability. Claims about the cause of a compromise require evidence. Communication should separate confirmed facts, working hypotheses and information that remains unavailable.

Prepare the decision paths

Name who can suspend a trust relationship, replace credentials, coordinate with suppliers and authorize a service change. Maintain current dependency records and tested recovery procedures. Ensure that the people needed for an emergency transition can access the relevant documentation during an outage.

Preserve evidence before it disappears

Capture the affected configurations, versions, credential references, relevant logs and incident timeline through approved procedures. Protect sensitive evidence and coordinate preservation needs with counsel. Rotating a current key does not by itself establish that previously copied information is safe or explain what an adversary already obtained.

Rehearse recovery and communication

Exercise a supplier defect or compromised signing service as a tabletop scenario. Test whether the organization can identify affected systems, notify the right parties and restore accepted trust. Define what evidence is needed before returning to service, and update the migration backlog with the lessons identified.

For Q4, run one cryptographic-dependency exercise and close the ownership or recovery gaps it exposes before expanding the migration program.

Give each dependency an owner

Cryptographic risk becomes manageable when business impact, technical responsibility, funding and acceptance authority meet in the same decision record.

NIST CSF 2.0 provides a taxonomy of cybersecurity outcomes for organizations of different sizes and sectors. It does not prescribe a single implementation method. Qtonic Quantum uses that distinction to frame quantum readiness as an accountable risk program, with metrics and decisions adapted to the organization's actual services. [SC15]

A board does not need to choose cryptographic parameter sets. It needs visibility into material exposure, unresolved dependencies, delivery risk and decisions requiring investment or accepted exceptions. Technical teams need clear boundaries and time to validate changes. Procurement needs enforceable obligations. Governance connects those responsibilities without pretending one function can do all of them.

Create a decision register

For each material service, record the owner, data or mission consequence, current protection, planned treatment and decision date. Separate evidence gaps from known gaps in protection. A missing supplier answer is uncertainty requiring follow-up, not automatic proof of either safety or failure.

Measure progress with honest denominators

Report the proportion of the defined estate inventoried, dependencies with named owners, validated transition paths and overdue exceptions. State what the denominator excludes and when the inventory was refreshed. Avoid a single enterprise percentage that combines discovery, planned upgrades and accepted deployments.

Review changes, not just calendars

Trigger review when a supplier commitment slips, a major system is purchased, a trust anchor changes or a relevant standard is revised. Keep exceptions time-bound and approved by the appropriate business authority. Link budget requests to the dependencies and service outcomes they will resolve.

For Q4, ask leadership to approve the first migration wave, its evidence requirements and the specific residual risks that remain after completion.

Build the team around the work

A sustainable quantum cybersecurity program needs coordinated engineering, operations, procurement and risk skills more than it needs a new title for every existing role.

The NICE Framework describes cybersecurity work through tasks, knowledge and skills. NIST distinguishes the framework publication from its separately maintained components. Qtonic Quantum recommends using that task-oriented approach to identify what the migration program must accomplish and then assigning people who can demonstrate the required capabilities. [SC16]

Few organizations need every employee to become a cryptographer. They do need architects who understand trust dependencies, engineers who can integrate supported implementations, operators who can diagnose failures, buyers who can challenge supplier claims and leaders who can accept risk knowingly. Deep cryptographic review should be available for decisions that require it.

Train for role-specific decisions

Give procurement teams examples of precise and imprecise claims. Give developers guidance on approved libraries, protocol behavior and supported upgrades. Give operations teams practice with credential renewal and recovery. Give executives short decision records that connect exposure, cost and uncertainty.

Assess capability with practical evidence

Use a bounded exercise: interpret an inventory, identify missing ownership, explain a certificate's scope or review a pilot result. Evaluate whether the person can perform the actual task safely and communicate its limits. Attendance at a briefing is useful context but weak evidence of operational capability.

Transfer knowledge before handover

Require suppliers and specialist advisers to deliver usable documentation, paired working sessions and named handover owners. Maintain coverage for critical tasks when an individual leaves. Preserve the reasoning behind exceptions and design choices so the organization can revisit them as technology and requirements change.

The Q4 workforce deliverable is a task-to-owner map, with targeted training and demonstrated backup coverage for the migration's critical decisions.

04

The Q4 execution plan

A quarter with owners and gates.

Migration work / generated editorial illustration

A purposeful quarter

A proposed Q4 mobilization: agree the scope, examine a priority pilot, and make the next funding decision with evidence.

PROPOSED Q4 2026 DECISION GATES

	OCTOBER	NOVEMBER	DECEMBER
Scope Program owner	◆ Baseline accepted		
Pilot Service owner		◆ Evidence reviewed	
Decision Executive sponsor			◆ Fund or defer

ALL QUARTER Logs, registers and weekly review continue throughout

October-December 2026 dates are proposed planning targets, not completed work or a promise of enterprise-wide migration. Adjust for change freezes, safety requirements and existing evidence.

CISA, NSA and NIST recommend roadmaps, inventories, risk assessment and vendor engagement. Qtonic Quantum translates this direction into three decisions: accept the scope, review a controlled pilot, and fund or defer the next wave. [EX01]

Assign authority before kickoff. Name a program owner, service owner and cost owner. Select the initial service and dependencies. Record supplier contacts, access constraints, acceptance criteria and authority to stop the pilot.

Use a dated program horizon. Qtonic Quantum's "ready before 2029" frame uses 1 January 2029 as a planning control date. From 8 September 2026, that is 846 days. Set service-specific evidence gates within the horizon. This is a company planning objective, not a prediction of Q-Day or a universal deadline. [PC06]

Deliver an accepted baseline, pilot evidence or a documented blocker, and an owned next step. This does not establish enterprise quantum safety.

Q4 / PROPOSED WORK PROGRAM

October

Establish the baseline

Start with a business service the organization can describe, observe and change. Make uncertainty visible before assigning a readiness label.

The initial service should matter to the business and have an available owner. It could be a sensitive document exchange, an internal application or a managed connection. These are examples for scoping, not claims about any Qtonic Quantum customer. Record the selection rationale and the services deliberately left outside the first assessment.

NIST's migration project treats understanding cryptographic use and prioritizing a roadmap as foundational activities. The proposed October deliverable is a versioned service record linking business purpose to observed cryptography, operational dependencies and unresolved questions. One external connection test cannot establish the cryptographic state of an entire service. [EX09]

01

Week 1: agree the boundary

The service owner identifies users, data flows, counterparties and operating constraints. The data owner records confidentiality duration and integrity requirements. Security approves collection methods and evidence handling. The program owner fixes the initial denominator: named services and components in scope.

02

Weeks 2-3: reconcile evidence

Compare authorized observations with configuration records, software dependencies, certificate inventories and supplier responses. Label each finding observed, documented, inferred or unknown. Record the collection date and component version. Ask owners to resolve material conflicts instead of averaging contradictory findings.

03

Week 4: accept the baseline

The CISO and service owner review the records together. Every material dependency must have an owner or an escalated ownership gap. Each high-priority unknown receives a resolution task, a due date and a named decision maker.

Q4 / PROPOSED WORK PROGRAM

November

Validate the path

A pilot should answer a specific deployment question and preserve the evidence needed to repeat the decision.

Select a pilot only after the baseline identifies a supported implementation path and a manageable failure domain. Write the question before selecting the product: can this service use the proposed cryptographic profile while meeting its security, compatibility and operating requirements? Define the exact release, configuration and counterparties under evaluation.

NIST describes crypto agility as adapting cryptographic mechanisms while preserving security and operations. Qtonic Quantum's proposed pilot gate therefore combines cryptographic evidence with service behavior. A successful connection alone does not prove the intended confidentiality and authentication properties. [EX03]

01

Approve the experiment

The service owner sets latency, availability and recovery criteria appropriate to the workload. Security specifies the required algorithms, protocol profile and permitted fallback behavior. Operations approves the test environment, monitoring and restoration plan. Use representative data with an approved handling classification.

02

Run and retain

Record the baseline and candidate under the same workload conditions. Capture release identifiers, relevant configuration, negotiated properties, resource use and errors. Exercise normal operation, restart, certificate or key lifecycle events, dependency failure and restoration. Retain failures and environmental differences with the successful results.

03

Decide without grade inflation

The review can approve progression, request remediation or reject the candidate for this service. Each outcome is useful. A limited laboratory result must retain its boundary. It cannot become a production performance claim or a statement about untested operating systems, network paths or partners.

Q4 / PROPOSED WORK PROGRAM

December

Decide and hand over

Close Q4 with an executable next wave, explicit risk ownership and a service team prepared to operate the result.

The December review should connect the original business concern to the evidence collected and the next investment required. Separate the pilot's conclusions from unresolved questions about wider deployment. Where holiday freezes limit safe change, complete the decision and operating preparation while scheduling production work for an approved window.

NIST's Organizational Profiles support comparison between current and target cybersecurity outcomes. Use that discipline to show which outcomes moved, which did not, and why. The proposed quarter-end package is a management decision record. It is not certification of quantum readiness. [EX04]

01

Approve the next wave

The sponsor selects the services to proceed, the funds released, the prerequisites and the accountable delivery owner. For each deferred service, record the reason, decision deadline and trigger for reconsideration. Escalate dependencies whose delivery dates conflict with required service or procurement milestones.

02

Transfer operational ownership

Operations receives supported configurations, monitoring rules, lifecycle procedures, escalation contacts and a tested restoration process. The receiving team confirms access to the evidence and can explain the response to a failed update or unexpected fallback. Schedule a review after the first production change.

03

Carry uncertainty forward

Publish the remaining unknowns alongside accepted results. Refresh the scope denominator when services are added or retired. Identify which supplier statements expire or need reconfirmation before purchase. Keep legal applicability and technical feasibility as separate decisions with their respective owners.

Sequence the dependencies

The highest-risk service may need immediate planning and a later cutover. Priority and deployment order are related, but they are not identical.

WAVE	PURPOSE	ENTRY CONDITION
Enable	Establish ownership, policy and test capability	Sponsor and service scope agreed
Prove	Validate a representative service path	Supported candidate and approved pilot
Expand	Migrate services sharing the proven pattern	Dependencies and operating capacity ready
Resolve	Address specialized or legacy constraints	Replacement, retirement or exception approved

Qtonic Quantum recommends organizing the backlog around business services and shared dependencies. Give every service both an urgency decision and an earliest credible deployment window. A critical service blocked by an unsupported trust component should remain highly visible while the enabling work proceeds.

NCSC's guidance distinguishes discovery, priority migration and completion across a multiyear program. Its UK target dates are planning guidance for their stated audience, not a universal commercial deadline. The proposed waves below are an original delivery pattern and should be adapted to the organization's applicable obligations. [EX02]

Use shared changes carefully. A common library, identity service or gateway can affect many applications. Group dependent services for planning, but retain a service-level acceptance decision. Validate the rollout order, coexistence period and recovery path before a shared component changes.

Keep the backlog honest. A service leaves a wave only after its agreed gate passes. Buying a license, installing a capability or receiving a supplier roadmap does not close the migration item. If retirement is the chosen treatment, verify the actual retirement and remaining data or trust dependencies.

Begin difficult, long-lead work early. Do not let easy deployments make the program appear complete while the most consequential dependencies remain unresolved.

Map what can block change

A service depends on more than its visible connection. Trace who establishes trust, where cryptography terminates and who controls the next change.

RECORD FIELD	DECISION IT SUPPORTS
Business service and data owner	Who accepts impact and protection needs?
Connection and termination points	Where does each protection actually apply?
Trust roots and signing dependencies	What must change for authentication?
Libraries, devices and managed services	Who can deliver a supported update?
Partner, contract and release constraints	What controls the migration sequence?
Evidence date and unresolved question	What must be verified before approval?

Map each selected business transaction to the systems and organizations protecting confidentiality, identity, software authenticity and recovery. Improving one connection does not improve every dependency.

NCSC recommends understanding system and service dependencies. Qtonic Quantum's proposed record supports review by technical owners, procurement and the risk sponsor. Link configurations and evidence rather than duplicating them. [EX02]

Review both directions. Ask service owners what could stop the transaction. Ask platform owners which services an update would affect. Reconcile answers with evidence to expose missing dependencies and overbroad rollout assumptions.

Name the boundary. Stop the initial map at a documented boundary with a named external owner. Opaque supplier services remain dependencies requiring verification, even when internal tools cannot inspect them.

Can each consequential dependency be linked to an owner, a supported change path and an evidence-backed acceptance decision?

Budget from the work

Use explicit quantities, internal labor assumptions and supplier quotations. This report does not invent a universal migration price.

COST LINE	PLANNING FORMULA
Internal effort	Role hours × loaded internal hourly cost
Specialist services	Accepted scope × quoted milestone price
Software and support	Quoted entitlement + support + renewal terms
Test environment	Reserved capacity × duration + setup
Replacement and deployment	Units × installed cost + change effort
Operation	Annual support + monitoring + lifecycle labor
Contingency	Named uncertainty × approved allowance

Separate discovery, engineering, procurement and operation. Budget the bounded Q4 scope, then revise using pilot evidence. NCSC advises funding preparation and migration without prescribing universal prices. [EX02]

Assign each line a quantity, cost basis, owner, uncertainty and decision date. Reconcile internal labor against existing budgets. Avoid double counting. Date supplier quotations and distinguish commitments from unapproved options.

Show an estimate range. Build lower, central and upper cases around discovery gaps, integration, supplier availability and replacements. Explain each difference. These are organization-specific scenarios, not market benchmarks or probability forecasts.

Fund successive gates. Approve baseline work, then a defined pilot, then expansion against demonstrated requirements and a credible operating model. Separate actual effort from forecasts. Revise remaining estimates when material assumptions change.

Show the next decision's cost, the wider estimate range and the assumptions that could move it. Precision depends on a defined architecture and scope.

Measure what matters

Every percentage needs a denominator, collection period and evidence rule. Report unknowns as a visible category.

MEASURE	NUMERATOR / DENOMINATOR	REQUIRED EVIDENCE
Owner coverage	Scoped services with accepted owner / all scoped services	Owner acceptance and scope version
Assessment coverage	Scoped services meeting baseline criteria / all scoped services	Complete baseline record
Dependency closure	Due critical dependency actions closed / all due critical dependency actions	Accepted resolution record
Pilot acceptance	Passed agreed requirements / all agreed pilot requirements	Test case and result, blocked cases stay visible
Observed adoption	Eligible observed sessions using required profile / all eligible observed sessions	Time window, profile and observation boundary
Exception overdue rate	Open exceptions past review date / all open exceptions	Exception register snapshot

HYPOTHETICAL COVERAGE EXAMPLE / THE ASSESSED COUNT STAYS 18

NIST guides measure selection and evaluation. Set targets after defining scope and establishing reliable collection. These are proposed management measures, not validated readiness benchmarks. [EX05]

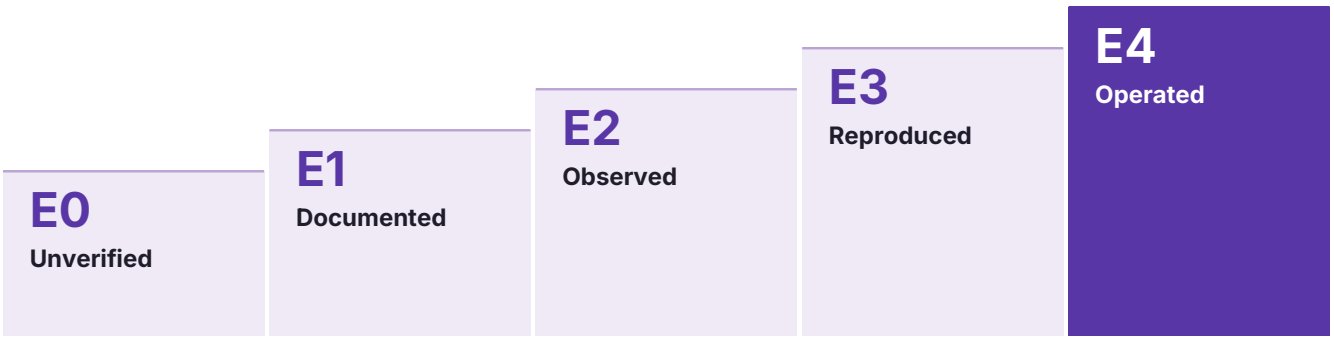
Assign owners. The program owner maintains scope. Service owners supply evidence. Security interprets findings. The risk owner manages exceptions. Report collection failures and unresolved ownership.

Respect boundaries. Adoption describes observed sessions. Pilot passes describe agreed tests. Neither establishes overall security. Show critical failures and scope changes alongside the percentages.

Grade the evidence first

An original Qtonic Quantum rubric for the strength of evidence behind a specific claim. It is not a validated readiness benchmark.

PROPOSED EVIDENCE MATURITY RUBRIC Qtonic Quantum



Ordered categories · no numeric distance or probability implied

E0-E4 are ordinal evidence levels, not a universal readiness scale. Apply them to a named claim, service or capability with version, scope, date and reviewer. They measure neither compromise probability nor quantum safety and are unrelated to IQM's Quantum Readiness Index.

NIST supports deliberate measure selection. Calibrate this proposed rubric internally. Compare suppliers only where scope and evidence are equivalent. [EX05]

Require complete support. Every condition must be supported. Record gaps separately. Evidence for one platform cannot raise an untested platform's level. Never average levels into an enterprise safety score.

Reassess material changes. Release, configuration or dependency changes can invalidate evidence. Retain prior records. A downgrade reflects changed evidence, not proof of an incident.

State the demonstrated level and its boundary. Production operation requires continuing review. No level constitutes certification.

Keep assurance independent

The team that implements a change should provide evidence. A reviewer with appropriate independence should challenge whether that evidence supports acceptance.

Independence is a defined relationship, not an adjective on a proposal. Record who designed, implemented, tested and approved the change, and disclose commercial interests. When one firm performs several roles, the client should require a separate acceptance authority and a clear statement of the assurance boundary.

Cryptographic assurance also has distinct objects. NIST defines FIPS-validated cryptography through module validation and identifies algorithm implementation testing as a prerequisite. An algorithm test record, a module certificate and a service acceptance decision answer different questions. Require the exact evidence relevant to the purchase and deployed configuration. [EX08]

Proposed reviewer checks

The reviewer traces material claims to dated artifacts, confirms the tested versions and examines unresolved failures. Sampling is permitted only with a stated selection method and limitation. The service owner decides operational acceptance. The authorized risk owner decides whether residual exposure is tolerable.

Make exceptions actionable

Each exception identifies the affected service, unmet requirement, business reason, accountable owner, compensating measures, approval and review date. Describe what evidence would close it. An exception is an explicit decision to carry a defined risk. It is not technical proof that the requirement was met.

Escalate conditions that change

Review exceptions after a supplier release, architecture change, missed milestone or relevant policy update. Escalate overdue reviews and rejected evidence. Keep expired exceptions visible until renewed by the proper authority or resolved, rather than allowing automatic extension.

One record should show the requirement, supporting evidence, reviewer conclusion, operational decision and residual risk owner. Preserve disagreements and limitations.

The board's decision page

Give directors the business exposure, the evidence boundary and the decision required. Put technical detail behind an inspectable reference.

BOARD QUESTION	REQUIRED ANSWER
Why act on this scope?	Named business services, protection needs and decision timing
What do we know?	Accepted baseline, evidence date, coverage and unknowns
What changed?	Verified results against the previous reporting scope
What remains exposed?	Critical dependencies, unresolved requirements and exceptions
What is the decision?	Approve, defer or redirect a specified next step
What does it require?	Funding, accountable owner and acceptance milestone
When will we reconsider?	Next review date and earlier escalation triggers

Brief directors after baseline acceptance and at the December gate. The sponsor owns the recommendation. The CISO interprets technical evidence. Finance confirms estimates, procurement supplier commitments and service owners operating consequences.

NIST Organizational Profiles communicate progress between current and target outcomes. This template applies that principle to affected services and remaining work. Insert actual evidence before circulation. [EX04]

Match claims to evidence. Distinguish observed pilot behavior from planned implementation. Label forecast dates as targets and roadmaps as supplier statements. Compliance claims require applicable requirements and supporting assessments.

Record the resolution. Document approved actions, conditions, resources and owners. Record risk acceptance separately. Return missed gates with consequences and revised decisions. Preserve original targets rather than silently moving them.

What it approved, who owns delivery, which exposure remains and what evidence it expects at the next review.

Rehearse the difficult decision

A fictional supplier delay and a failed compatibility test can reveal governance gaps before a production change creates them.

INJECT	DECISION TO REHEARSE
Supplier milestone moves	Who updates the plan and verifies the revised commitment?
Compatibility result fails	Who blocks progression and approves the retest criteria?
Business requests acceleration	Who can accept residual risk, and on what evidence?
Unexpected fallback appears in a mock log	Who interprets it and invokes the response procedure?
Board asks for assurance	What can be stated accurately about remaining exposure?

Fictional scenario: a sensitive-records service passes one laboratory upgrade path but fails a required partner configuration. The supplier delays its supported release while the business requests acceleration.

NIST SP 800-84 addresses exercise design and evaluation. This proposed Qtonic Quantum discussion uses simulated records and decisions, requiring no attacks, live traffic changes or third-party access. [EX06]

Run the exercise. Include service owners, security, operations, procurement, legal and the sponsor, with a facilitator and recorder. Present injects sequentially. Use actual decision authorities and document locations.

Capture corrective actions. Record unclear ownership, missing evidence, conflicting thresholds and decisions beyond authority. Assign owners and due dates. Discussion demonstrates decision preparedness. It neither validates cryptographic implementation nor proves incident-response performance.

A corrected decision path, a prioritized action list and an agreed follow-up review. Keep the scenario's invented facts out of external claims.

The vendor interview

Move the conversation from a roadmap slide to supported releases, explicit boundaries and evidence the buyer can review.

ASK	REQUEST AS EVIDENCE
What works today?	Supported release notes, configuration and limitations
What cryptographic properties change?	Algorithms, parameters, protocol profile and trust boundary
What remains conventional?	Dependencies, fallback rules and unsupported paths
Where has it been tested?	Test conditions, results and known interoperability issues
What is validated?	Applicable certificates, versions and operating conditions
How is it operated?	Lifecycle, monitoring, incident and restoration procedures
What happens if the roadmap slips?	Named escalation, revised milestones and alternatives
How do we leave?	Export formats, transition assistance and exit costs

Send questions in advance. Require written answers for the exact product, release and deployment model. Capabilities may differ across a portfolio. Record available, limited-release, planned and unsupported separately.

CISA, NSA and NIST recommend vendor engagement. NIST places supplier risk within organizational risk management. These questions request evidence and assert no vendor failure. [EX01, EX07]

Close with ownership. Assign missing answers to supplier representatives and buyer reviewers with response dates. Absent evidence remains open diligence. Infer neither support nor deliberate misrepresentation.

Compare fairly. Apply identical service requirements and test boundaries to candidates. Separate mandatory gates from preferences. Document trade-offs between stronger evidence and additional integration effort rather than accepting portfolio-wide claims.

A useful supplier answer can be linked to a release, reproduced within an agreed scope and assigned to an accountable owner.

The evaluable RFI

Define the required service outcome and response format before asking the market to explain its capabilities.

INCLUDE	REQUIRE IN THE RESPONSE
Service and deployment boundary	Supported use cases, assumptions and exclusions
Functional cryptographic requirements	Mechanism, protocol profile, parameters and dependencies
Operating environment	Supported platforms, versions and resource needs
Assurance requirements	Evidence identifiers and the exact validated boundary
Interoperability and transition	Coexistence, fallback, testing and restoration approach
Delivery and lifecycle	Available capability versus dated roadmap commitments
Evidence handling	Collection, access, retention, export and deletion controls
Commercial structure	Pricing basis, support, renewals and exit provisions

Use an RFI to expose feasibility, dependencies and evidence gaps before committing. Procurement owns process. Architecture and security set requirements. Service owners define constraints. Legal and compliance determine applicable provisions.

NIST supply-chain guidance supports acquisition-risk management. Tailor this procurement aid to jurisdiction, mission and acquisition rules. It supplies no statutory language. [EX07]

Define evaluation. Mark requirements mandatory or desirable, with response fields, acceptable evidence and reviewers. Separate documented from planned capability. Weighted totals must not offset failed mandatory security requirements.

Define the pilot. Specify paid or unpaid participation, environment provision and results ownership. Establish evaluation rights and confidentiality before sharing sensitive architecture. Tie later acceptance and payment to verified deliverables.

The buyer can explain why each candidate advances, what remains unverified and which evidence the next phase must produce.

05 The Qtonic Quantum approach

Make expertise inspectable.

People / 80

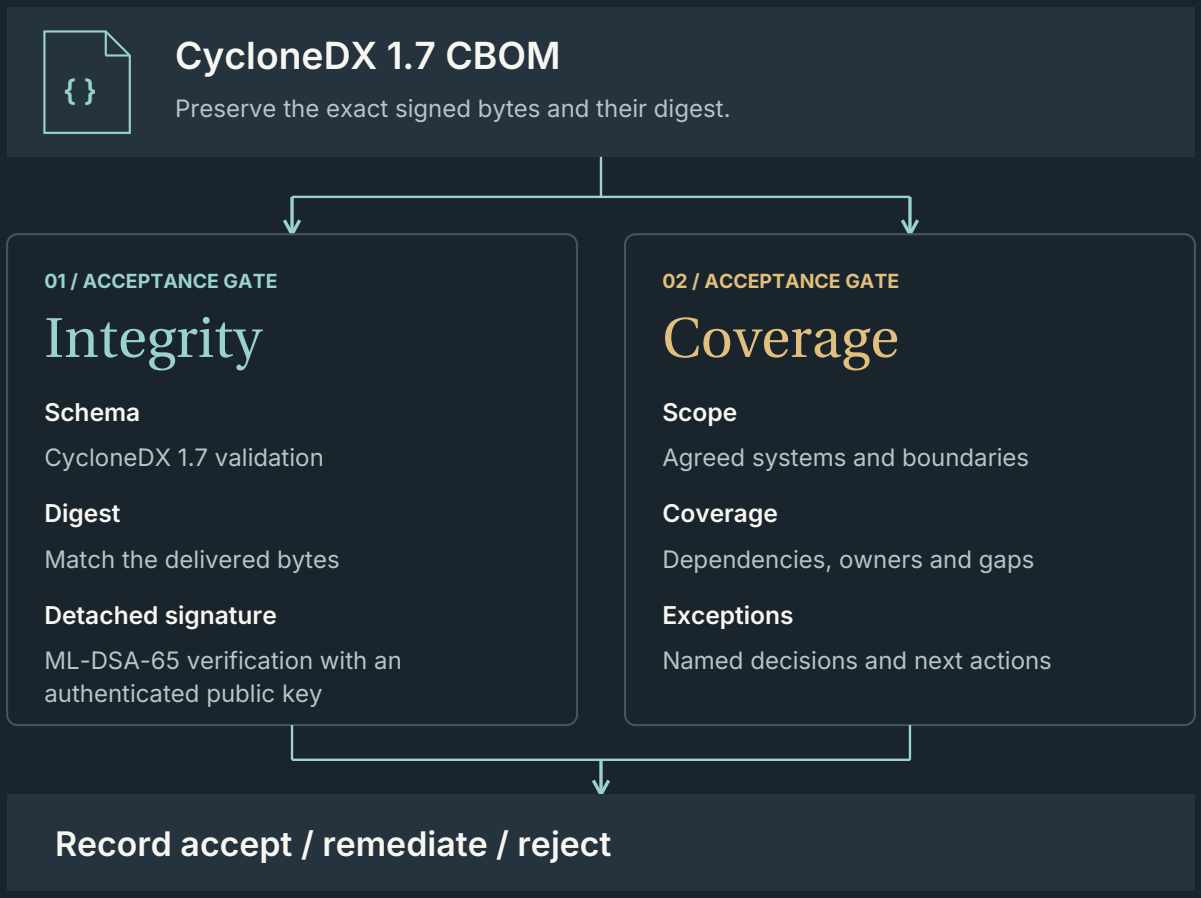
QScout Gold / 81

CBOM handover / 84

QSCOUT GOLD / BUYER ACCEPTANCE

Authentic is not complete.

A signed inventory needs two kinds of evidence.



Proposed buyer model / page 84. A valid signature does not prove that the inventory is complete.

Buyer acceptance model / companion requirements on page 84

Expertise with people behind it

Qtonic Quantum brings published defense leadership and specialist experience to the practical work of cryptographic transition.

PUBLISHED PROFILE	ROLE OR SPECIALIST CONTRIBUTION
Lt. Gen. Mark E. Weatherington, USAF (Ret.)	Chairman, Defense Innovation Council
Lt. Gen. Roger L. Cloutier Jr., USA (Ret.)	Founding Chair, Allied Defense Council
Lt. Gen. Milford H. Beagle Jr., USA (Ret.)	Senior Leader, Allied Defense Council
Brig. Gen. Shan Bagby, USA (Ret.)	Military medicine and healthcare leadership in the published specialist network

These are published roles in Qtonic Quantum's leadership and specialist network. The engagement identifies who will actually lead the work. A military title does not imply government endorsement or review of this report. [CO05]

The PQC Discovery Index, edition 2026.5, ranks QScout Gold Pulse first among 14 products at 9.42/10. Its published row label is "QScout Pulse Gold". Qtonic Quantum sponsored and contributed the evidence work and builds the product. Its row has deeper live evidence than peer rows, which largely use public documentation. Treat this as a dated, disclosed comparison. [PC04]

PUBLISHED PERSPECTIVE

From Qtonic Quantum's 2029 research note

"I spent my career in environments where encryption failure means mission failure. Qtonic Quantum applies that standard to enterprise systems."

Lt. Gen. Mark E. Weatherington, USAF (Ret.) [PC09]
Chairman, Defense Innovation Council

Start with QScout Gold

Create the governed cryptographic baseline, then keep the decision current with QScout Gold Pulse.

QScout Gold is the established assessment offering for a deeper cryptographic baseline. Its product schedule includes vulnerability assessment, timeline-to-threat modeling, prioritized remediation pathways, CBOM delivery, cryptographic digital-twin handoff and board reporting. The order defines the authorized scope and deliverables. [PC01]

Use the Q4 inventory decision to start a real product conversation. Describe the external endpoint population, internal systems, cloud and identity scope, evidence access and intended business decision. Qtonic Quantum supplies the current quotation and applicable terms.

01

Agree the assessment depth

Surface addresses external visibility. Silver adds authorized deeper assessment. Gold brings the internal cryptographic and migration view. Select the tier with the evidence owner. [PC01, PC02]

02

Set the first-result milestone

"First results in 72 hours" is the company's stated initial-result objective. Confirm the delivery clock, required inputs and result depth in the order. [PC07]

03

Accept the evidence package

Require the CycloneDX 1.7 CBOM, its verification receipt, scope and gaps, and a prioritized decision record. Use page 84 to specify the handover. [PC01]

04

Keep it current with QScout Gold Pulse

QScout Gold Pulse carries the baseline forward through continuous monitoring of the agreed surface. Connect material changes to review, validation and remediation ownership. [PC03]

Request a QScout Gold assessment

qtonicquantum.com/contact

Find. Prove. Fix.

One connected product path: discover cryptographic exposure, validate material risk and execute an accountable migration program.

QSCOUT LAYER	BUYER PURPOSE
Surface	Establish the externally observable exposure baseline
Silver	Add authorized artifact and credentialed assessment depth
Gold	Build the deeper cryptographic baseline and migration decision record
QScout Gold Pulse	Keep the agreed assessment surface and evidence current

QScout Gold establishes the governed baseline. QScout Gold Pulse keeps that decision record current. Together they connect cryptographic discovery, harvest-now exposure, crypto-agility assessment, signed evidence and migration priorities. Crypto-agility assessment identifies change constraints and evidence needed to replace dependencies. [PC01, PC03, PC05]

QScout produces a CycloneDX 1.7 Cryptographic Bill of Materials. CBOM delivery is part of the Gold product definition. Its scope, verification package and residual gaps belong in the agreed handover. [PC01]

QStrike / Prove. Validate selected material risks within the signed engagement scope and retain the result, method and limits. The published boundary makes no direct encryption-break or production-key-break claim. [QQ02]

QSolve / Fix. CISO-led, vendor-neutral advisory turns the evidence into migration priorities, owners, dependency decisions and verified closure. It connects the quarter's work to the longer transition. [PC01, QQ03]

QHunt / For the warfighter

Qtonic Quantum Corp states that it deploys and operates QHunt for Department of War and mission owners. This distinct product combines quantum cyber risk with traditional High, Critical and exploitable vulnerability intelligence on an authorized mission surface. Restricted, air-gapped and on-premise delivery stays inside the customer boundary, with a non-destructive default and named stop conditions. [QH01, QH02]

Company-stated outputs include an evidence ledger, a CycloneDX 1.7 CBOM signed with ML-DSA-65, verification receipts, disclosed gaps and next-work priorities. Medium findings do not enter the headline count. These outputs are not validated by this report's local experiments. [QH02]

QHunt mission enquiries: qtonicquantum.com/leadership

Naming note: Department of War is an authorized secondary designation. Statutory references to the Department of Defense remain controlling unless changed by law. [DN01]

QShield / SAFE/29

Connect the operating implementation, the demonstrated use case and the authorization decision to the exact release.

Company implementation position: Qtonic Quantum reports SAFE/29 with QShield v1.0 as built and operating. This edition records that company statement. It does not treat an engineering specification alone as proof of a particular release or deployment. [PC07]

QShield Packet Runtime is the software packet-protection implementation within SAFE/29. The submitted S29SP-1 profile specifies ML-KEM-1024 key establishment and ML-DSA-87 authentication. SAFE/29 connects protection to authority, evidence, portfolio decisions and an eventual native-PQC exit. [QQ10]

The 31 August engineering document is a target build order with explicit release states. Its proposed platform coverage and completion gates must be reconciled to the actual version being offered. A laboratory result for one platform does not establish every platform in the plan. [QQ10]

Inspect the release

Request the version or tag, signed manifest, named platform and reproducible demonstration. The evidence should identify the implemented profile, traffic coverage, recovery behavior and known limits.

Inspect the acceptance boundary

Use the customer's environment and requirements to decide suitability. The experiments in this report are separate from QShield testing. Implementation status, independent assessment and authorization are distinct claims.

This report makes no claim of FIPS 140-3 validation, DoW CIO ATLAS authorization or operational deployment approval.

The CBOM should survive the handover

QScout Gold's inventory becomes more valuable when a recipient can inspect its structure, establish its origin and reuse it in the next decision.

QScout Gold includes a CycloneDX 1.7 CBOM. The published 2026.5 evidence record describes signed inventory with a detached ML-DSA-65 signature, public verification key and procedure, reviewed on 15 August. This is a dated product-evidence record, distinct from this report's local measurements. [PC01, PC05]

Request the current signed sample and verification bundle through the Proof Center or company desk. Public sample availability is governed by the newsroom's publication controls. Confirm the exact released artifact and its verification procedure at the time of the engagement. [PC08, CB01]

What the handover contains

The machine-readable CBOM, declared scope and collection date, detached signature, signer identity and key provenance, pinned schema and verification procedure. Preserve exact bytes and software versions.

What the recipient verifies

Schema validation succeeds. The digest matches. The signature verifies with the trusted key. Scope and gaps reconcile to the agreed population. Supply the actual result receipt, not only a product description.

What the buyer owns

A portable inventory and evidence record that can move into procurement, architecture, audit and migration planning. The signer proves origin and integrity under the chosen trust model. Coverage and accuracy still require the assessment evidence.

ATTACHED PROCUREMENT TOOL

Adapt the attached sheet for your RFP.

Save the one-page PDF using the paperclip or the PDF Attachments panel. Verify its SHA-256 on page 45. [CT01]

Qtonic_Quantum_CBOM_Acceptance_Requirements.pdf

One page / six acceptance clauses

Checksum / page 45

Turn the next decision into action

Use QScout Gold to establish the baseline, QScout Gold Pulse to maintain visibility and QSolve to direct the transition.

Request a QScout Gold assessment for the agreed service and endpoint population. Confirm the quotation, evidence package and delivery milestones before collection. Use the current product schedule and signed order. [PC01, CO01]

Explore Qtonic Quantum's leadership and specialist expertise across enterprise technology, cybersecurity and government at qtonicquantum.com/leadership. The website link and QR code are on page 92. [CO05]

01 **Name the business decision**

Bring the service, protection objective, decision owner and consequence of delay.

02 **Define the Gold scope**

Agree endpoints, internal dependencies, permitted access and exclusions. Use the current product schedule and written quotation.

03 **Accept the signed evidence**

Require the CBOM, verification receipt, coverage gaps and prioritized migration record.

04 **Fund the next step**

Use QStrike where validation is required and QSolve to assign owners, sequence change and resolve exceptions.

05 **Keep the baseline current**

Scope QScout Gold Pulse monitoring and the changes that trigger reassessment. Renew the evidence through the transition.

Meet Qtonic Quantum's leadership

qtonicquantum.com/leadership

A common language / A-L

These definitions support the report's decision frameworks. Specifications and engagement agreements remain authoritative for precise technical and contractual meaning.

AEAD Authenticated encryption with associated data: a construction providing confidentiality and integrity while authenticating designated data that remains unencrypted. Associated data is not made secret by authentication. [QQ12]

Algorithm A defined computational procedure. In this report, a cryptographic algorithm is one component of a larger implementation, protocol and operating environment.

Authentication Establishing confidence in an asserted identity or data origin. Its assurance depends on the mechanism, credentials, trust model and operating conditions. [QQ08]

CBOM Cryptography bill of materials: structured information about cryptographic assets and their relationships. A CBOM supports inventory. Completeness depends on how information was collected. [QQ09]

Crypto agility The capability to replace or adapt cryptographic mechanisms as needs change. This report treats discovery, governance, testing and maintenance as practical conditions for exercising that capability. [AR04]

Cryptoperiod The authorized period for using a particular key. It is distinct from how long information must remain confidential or how long evidence must remain verifiable. [QQ08]

Digital signature A cryptographic mechanism supporting verification of data integrity and signatory identity. A signature does not encrypt the signed content or independently establish the signer's authority. [QQ06]

Evidence boundary This report's term for the scope, method, time and conditions within which an observation or result supports a conclusion.

HNDL Harvest now, decrypt later: retaining encrypted communications for possible future decryption after the underlying protection can be defeated. It is a risk model, not evidence of collection from a particular organization. [AR06]

HSM Hardware security module: a physical device that protects and manages cryptographic keys and performs cryptographic processing. Verify the exact product and configuration. [QQ13]

KEM Key-encapsulation mechanism: algorithms used to establish a shared secret, typically for subsequent symmetric cryptographic protection. It does not itself provide every property of a secure session. [QQ05]

Lifecycle The period from introduction through operation, change and retirement. Assign owners to the transitions, not only to initial deployment.

A common language / M-Z

Use common terminology to make supplier responses comparable and prevent a narrow technical claim from becoming an unsupported assurance statement.

ML-DSA Module-lattice-based digital signature algorithm standardized in FIPS 204. It addresses signatures. It is not a bulk-data encryption algorithm. [QQ06]

ML-KEM Module-lattice-based key-encapsulation mechanism standardized in FIPS 203. Its parameter set and implementation must be specified when evaluating a deployment claim. [QQ05]

PQC Post-quantum cryptography: cryptographic approaches intended to resist attacks using both classical and quantum computers. The term expresses a security objective, not a guarantee against every attack. [QQ05, QQ06, QQ07]

Protocol The rules governing an exchange between participants. A protocol combines mechanisms, messages and state. Naming one algorithm does not describe the entire exchange.

Public-key cryptography Cryptography using a related public and private key. Confidentiality, key establishment and signatures use different constructions and require different migration decisions. [QQ08]

Readiness In this report, an evidenced ability to make and execute a defined protection decision. It must state the scope and conditions. It is not a universal certification.

Residual risk The risk remaining after a proposed or completed action. Record the rationale, accountable acceptance authority and conditions that require reconsideration.

SLH-DSA Stateless hash-based digital signature algorithm specified in FIPS 205. It provides a different signature construction from ML-DSA, with different implementation tradeoffs. [QQ07]

Symmetric cryptography Cryptography in which communicating parties use shared secret key material. Key protection and lifecycle remain important even when the data-protection algorithm is appropriate. [QQ08]

TLS Transport Layer Security: a protocol family for protected communications. TLS 1.3 separates key establishment, authentication and record protection. Assess the negotiated configuration. [QQ11]

Trust anchor A trusted key or related information that starts a verification relationship. Replacing a signing algorithm may also require changes in how trust is distributed. [QQ08]

Validation An evaluation against defined criteria. State exactly what was validated, by whom, under which program and within what configuration. The word alone establishes little.

Zeroization Erasing sensitive cryptographic material. The mechanism and evidence needed depend on the storage medium, component and threat model. [QQ08]

The source record / 1

Titles link to sources. OR01, TS01 and CT01 open the attached artifacts on page 45.

TP01 The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, version 2.1
2024-12

TP02 Post-Quantum Cryptography: FAQs
Updated 2026-08-05

TP03 How (not) to Design and Implement Post-Quantum Cryptography
2021

TP04, EX01 Quantum-Readiness: Migration to Post-Quantum Cryptography
2023-08-21

TP05 Cybersecurity in an era with quantum computers: will we be ready?
2015

TP06, AR05, QQ05 FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard
2024-08-13

TP07, AR10, QQ06 FIPS 204: Module-Lattice-Based Digital Signature Standard
2024-08-13

TP08, QQ07 FIPS 205: Stateless Hash-Based Digital Signature Standard
2024-08-13

TP09 SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes
2020-10-29

TP10 What Is Post-Quantum Cryptography?
2024-08-13

TP11 Quantum Key Distribution (QKD) and Quantum Cryptography (QC)
Undated

TP12 SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation
2018-01

TP13 SP 800-227: Recommendations for Key-Encapsulation Mechanisms
2025-09-18

TP14 PQC Standardization Process
Checked 2026-09-07

TP15, AR15 Cryptographic Algorithm Validation Program
Updated 2026-08-12

TP16, UP02 Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks
2026-06-22

TP17 M-26-15: Execution of the Migration to Post-Quantum Cryptography
2026-06-24

TP18 Cryptographic Module Validation Program
Updated 2026-08-21

TP19 M-23-02: Migrating to Post-Quantum Cryptography
2022-11-18

TP20 IR 8547: Transition to Post-Quantum Cryptography Standards, Initial Public Draft
2024-11-12

TP21, EX02 Timelines for migration to post-quantum cryptography
2025-03-20

TP22 A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography
2025-06

TP23 Post-Quantum Cybersecurity Resources
Checked 2026-09-07

TP24 Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector
2026-01

TP25 G7 Cyber Expert Group Releases Roadmap for Coordinating the Transition to Post-Quantum Cryptography in the Financial Sector
2026-01-12

TP26 Security Directives and Emergency Amendments
Checked 2026-09-07

TP27 The NIST Cybersecurity Framework (CSF) 2.0
2024-02-26

TP28 Quantum Computing: Progress and Prospects, Chapter 4, pp. 110-112
2019

AR01, SC13, EX09 Migration to Post-Quantum Cryptography
Living project page

AR02, QQ09 Cryptography Bill of Materials (CBOM)
Undated

AR03, QQ08 SP 800-57 Part 1 Rev. 5: Recommendation for Key Management, Part 1 - General
2020-05-04

AR04, EX03 CSWP 39upd1: Considerations for Achieving Crypto Agility - Strategies and Practices
2025-12-19

AR06 RFC 9954: Hybrid Key Exchange in TLS 1.3
2026-07

AR07 RFC 10024: Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3
2026-08

AR08, QQ11 RFC 9846: The Transport Layer Security (TLS) Protocol Version 1.3
2026-07

The source record / 2

Titles link to sources. OR01, TS01 and CT01 open the attached artifacts on page 45.

AR09 RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
2008-05

AR11 SP 800-193: Platform Firmware Resiliency Guidelines
2018-05

AR12 RFC 9370: Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
2023-05

AR13 Shared Responsibility Model
Undated

AR14, SC07 SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security
2023-09-28

AR16, SC18 Cryptographic Module Validation Program - Validated Modules
Living program page

AR17 SP 1800-38C: Migration to Post-Quantum Cryptography - Quantum Readiness: Testing Draft Standards for Interoperability and Performance
2023-12

AR18, SC11, EX07 SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
2022-05

SC01 Project Leap phase 2: quantum-proofing payment systems
2025-12-11

SC02 The Security Rule
Reviewed 2026-03-19

SC03 Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)
2025-12-05

SC04 The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, Version 2.1
2024-12

SC05 NIST IR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks
2023-09-25

SC06 Model Rule 1.6: Confidentiality of Information
Undated

SC08 NIST SP 800-218: Secure Software Development Framework Version 1.1
2022-02-03

SC09 PQ.03: Post Quantum Cryptography - Guidelines for Telecom Use Cases
2024-10-04

SC10 Quantum Information Science
Undated

SC12 Cryptographic Module Validation Program: Modules In Process
Accessed 2026-09-07

SC14 NIST SP 800-61 Revision 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management
2025-04-03

SC15 NIST Cybersecurity Framework 2.0
2024-02-26

SC16 NIST SP 800-181 Revision 1: Workforce Framework for Cybersecurity
2020-11-16

SC17 Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions
2026-02-03

EX04 NIST SP 1301: NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles
2024-02-26

EX05 NIST SP 800-55 Vol. 1: Measurement Guide for Information Security: Volume 1 - Identifying and Selecting Measures
2024-12-04

EX06 NIST SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
2006-09-21

EX08 FIPS-validated cryptography - NIST CSRC Glossary
Accessed 2026-09-07

QQ01 QScout - Cryptographic Exposure Intelligence
Undated

QQ02 QStrike - Product Scope and Public Boundary
Undated

QQ03 QSolve - Human-Led Advisory
Undated

QQ10 SAFE/29 QShield submission and Engineering Build Specification v1.0 (company record)
2026-08-31

QQ12 RFC 9771 - Properties of Authenticated Encryption with Associated Data Algorithms
2025-05

QQ13 Hardware Security Module - CSRC Glossary
Undated

UP01 Treasury Announces the Quantum-Readiness Task Force
2026-08-24

CO01 Contact - Assessment Plan and Scoping Call
Undated

The source record / 3

Titles link to sources. OR01, TS01 and CT01 open the attached artifacts on page 45.

CO02 QStrike Challenge - Current Public Terms Boundary
Undated

UP03 Executive Order 14412, official Federal Register edition, sections 5(d) and 6(b)
2026-06-22

OR01 Qtonic Quantum local PQC study QQ-PQC-LOCAL-2026-09: embedded archive and checksum (see page 45)
2026-09-07

OR02 FIPS 203, Table 3: ML-KEM key and ciphertext sizes
2024-08-13

OR03 FIPS 204: ML-DSA sizes and rejection-sampling signing algorithm
2024-08-13

OR04 pqcrypto 0.3.4, implementation used in the experiment
Version 0.3.4

OR05 Qtonic Quantum Lab: evaluation overview
Reviewed 2026-09-08

OR07 Qtonic Quantum: published methodology
Reviewed 2026-09-08

OP01 Post-quantum TLS: Google Cloud load-balancer scope and rollout
Updated 2026-08-26

OP02 Google Cloud post-quantum cryptography roadmap
2026-08-11

OP03 Cloudflare Radar 2025 Year in Review: post-quantum traffic
2025-12-15

NW01 IonQ ECC-256 resource-estimate paper
Paper 2026-09-03, announced 2026-09-08

NW02 IonQ ECC-256 announcement and scope
2026-09-08

NW03 Automatic Key Exchange for origins
2026-09-08

NW04 Post-quantum authentication to origins
2026-07-29

NW05 Superion 256 announcement
2026-09-08

NW06 IonQ and Congruity360 agreement
2026-09-08

CO03, PC08 Qtonic Quantum media desk
Reviewed 2026-09-08

CO04 Qtonic Quantum terms of service
2026-04-20

CO05 Qtonic Quantum published leadership
Reviewed 2026-09-08

PC01 Qtonic Quantum Commercials Schedule, product definitions (company record)
Effective 2026-07-01, reviewed 2026-09-08

PC02 QScout Surface, Silver and Gold launch
2026-05-21

PC03 QScout Gold Pulse launch and continuous-monitoring scope
2026-05-21

PC04 PQC Discovery Index 2026.5: rankings and disclosure
Published 2026-08-15, reviewed 2026-09-08

PC05 PQC Discovery Index 2026.5: source record S01-S03
Source review 2026-08-15

PC06 Qtonic Quantum 2029 planning-control research note
Reviewed 2026-09-08

PC07 Commissioning feedback: QShield v1.0 status and QScout first-result objective (company record)
2026-09-08

CB01 Qtonic Quantum Proof Center and controlled diligence
Reviewed 2026-09-08

TS01 Qtonic Quantum local TLS study QQ-TLS-LOCAL-2026-09 (see page 45)
2026-09-08

TS02 OpenSSL 3.5: group selection and predicted key shares
Reviewed 2026-09-08

PC09 Mark E. Weatherington quotation: 2029 research note, Executive Summary
Verified 2026-09-08

PV01 C2PA and Content Credentials Explainer, goals and limitations
Version 2.2, reviewed 2026-09-08

CT01 CBOM acceptance requirements (see page 45)
8 September 2026

AU01 Author biography / approved public media kit
Reviewed 2026-09-08

AU02 Author-provided biography update (company record)
2026-09-08

QH01 QHunt: mission and OT assessment
Verified 2026-09-08

QH02 QHunt warfighter marketing brief (company record)
2026-09-08

DN01 Executive Order 14347: secondary defense titles, sec. 2
2025-09-05

Method and provenance

Sources, authorship and production notes.

External evidence

Primary standards, government publications, research papers and provider documentation support external claims. Latest selective news review: 8 September 2026, 19:12 UTC. Same-day developments appear on pages 6, 9, 14 and 33. Sources: pages 88-90.

Original empirical research

The primitive study recorded 18,000 operation timings on 7 September. The TLS study recorded 80 certificate-verified handshakes on 8 September. Pages 41-45 disclose their methods, findings and limits. Both archives are attached, with checksums and instructions on page 45. Neither study tests a Qtonic Quantum product.

Company descriptions

Company publications, commercial definitions and commissioning statements support the company chapter. Company-reported QShield implementation, engineering targets and externally verified release evidence remain distinct. The Index sponsorship and uneven evidence depth are disclosed on page 80.

Accountability

Commissioned by Qtonic Quantum Corp. Research, writing, experiment execution and production used AI assistance. This commissioning credit does not claim independent human replication or technical sign-off.

Visuals and data

Five generated editorial scenes depict generic infrastructure, quantum research and migration work. They do not show actual Qtonic Quantum people, products or facilities. Vector figures use cited sources, disclosed models or recorded observations.

Provenance

The delivered PDF includes a C2PA Content Credentials manifest. It records provenance, not independent validation of these findings. [PV01] The official logo is unchanged. IQM informed the format brief. No IQM imagery, survey results or interview quotations are reproduced.

About the author

J. Nathaniel Ader is Co-Founder and Chief Innovation Officer of Qtonic Quantum Corp, founder of Qtonic Quantum Lab, and author of The Quantum Almanac 2026-2027. His work includes the development of QScout, QStrike and QHunt, with a focus on cryptographic debt, harvest-now-decrypt-later exposure and security testing. He connects these technical questions to governance, compliance and post-quantum migration decisions. His background spans finance and technology. He holds an MBA and a BA from New York University. [AU01, AU02]

QTONIC QUANTUM
POST QUANTUM READY

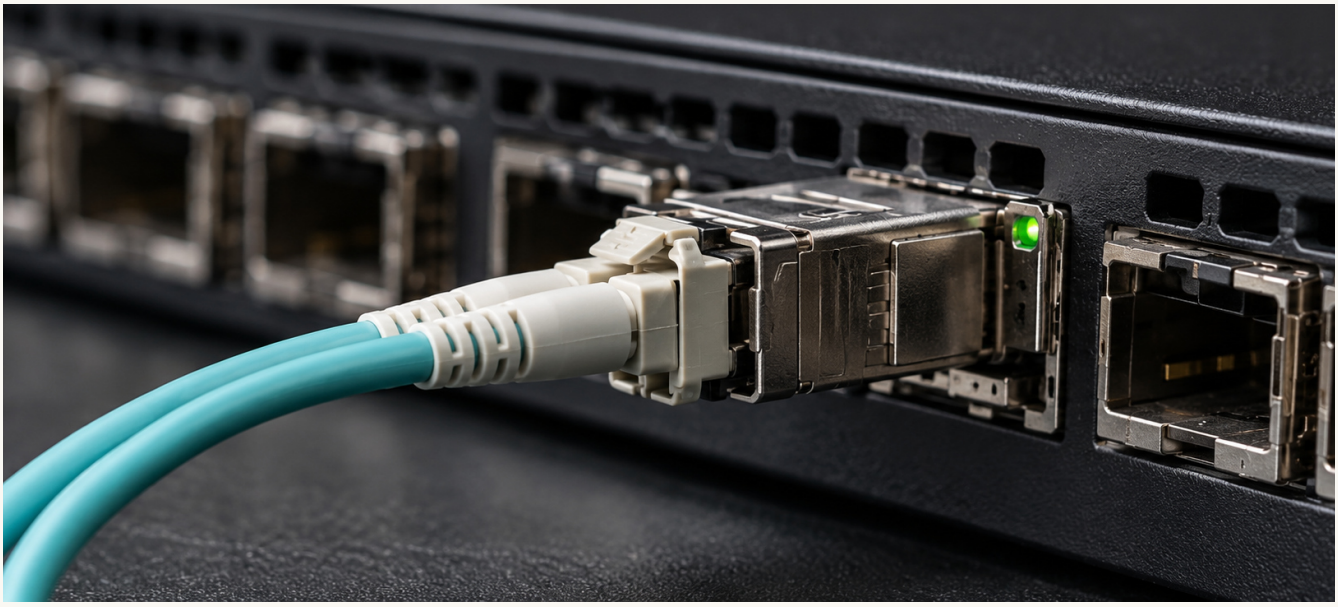
OUR LEADERSHIP

Meet the people behind the work.

Explore Qtonic Quantum's leadership, expertise and experience across enterprise technology, cybersecurity and government.

Explore our leadership

qtonicquantum.com/leadership



Network interconnect / generated editorial illustration