

QUANTUM CORE INSTITUTE

Standards-first governance for post-quantum cryptography risk

# QCI-QS1

## Quantum Readiness and Post-Quantum Cryptography Governance Standard

|                              |                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------|
| Document ID                  | QCI-QS1                                                                                         |
| Version                      | 2.3                                                                                             |
| Status                       | Issued edition. Active.                                                                         |
| Publication date             | September 23, 2026                                                                              |
| Effective date               | September 23, 2026                                                                              |
| Supersedes                   | Version 2.2, June 8, 2026. Transition is governed by Clause 1.3.                                |
| Technical reference baseline | Verified September 23, 2026; see Clause 2 and Annex E.                                          |
| Publisher                    | Quantum Core Institute Inc.                                                                     |
| License                      | Free to download, cite, and adopt. Attribution required. May not be modified and redistributed. |

*This standard establishes requirements for governing quantum-related cryptographic risk, maintaining a validated inventory, measuring readiness, overseeing suppliers, and reporting to the governing body. It separates conformance from maturity and requires evidence of both management decisions and deployed protection.*

## Rights and publication control

QCI-QS1 is published by the Quantum Core Institute as public infrastructure. It may be referenced freely in organizational governance documentation, regulatory submissions, procurement instruments, and vendor assessments, provided that attribution to the Quantum Core Institute is maintained and the version and date are cited.

The standard may not be modified and redistributed, or reproduced in whole for commercial gain, without written consent from the Quantum Core Institute. Conformance and methodology claims are governed by Clause 1. A reference to this edition cites Version 2.3 and its publication date.

© 2026 Quantum Core Institute. QCI-QS1 is a standard of the Quantum Core Institute. Commercial engagements that apply this standard reference it as methodology and are separate from the standard itself.

Suggested citation: Quantum Core Institute. QCI-QS1 Quantum Readiness and Post-Quantum Cryptography Governance Standard. Version 2.3. September 23, 2026.

Version 2.3 is the issued edition. It was published and takes effect on September 23, 2026 and supersedes Version 2.2 dated June 8, 2026. The authoritative reference register in Annex E was verified at the publication date. Adoption and edition transition are governed by Clause 1.3.

## Foreword

QCI-QS1 organizes five integrated components: the Quantum Risk Governance and Assessment Framework (QRAF); the Quantum Attack Surface and Cryptographic Dependency Inventory (QASI); the Q-Risk Score; the Vendor Roadmap Request Pack; and the Board Briefing Insert. The eight QRAF assessment domains and five scoring pillars remain distinct. The domains organize assessment work; the pillars determine the readiness score.

Version 2.3 retains pillar weights of 20, 20, 20, 25, and 15 and score caps of 60, 70, and 80. Version 2.3 adds a fixed scoring profile, changes the vendor gate, and moves the upper readiness band to 81–100. These substantive interpretation changes mean scores from earlier editions are not directly comparable without restatement. Annex F identifies the changes.

The standard governs cryptographic risk arising from AI systems when they are in scope. It does not govern model behavior, output safety, or AI risk generally. Human and workload identity are recorded separately; AI is a cross-cutting application of the same governance and assurance controls.

The governance cadence, maturity rubric, thresholds, and conformance rules are QCI requirements. They are not attributed to NIST, NSA, or another external authority. External standards and guidance support the technical and policy context described in Clause 2 and Annex E.

## Contents

Contents are generated when the document is opened in Word.

## Part A Normative requirements

Clauses 1–8 are normative. Each requirement paragraph has a stable QCI identifier. Tables expressly incorporated by a requirement are part of that requirement. Clause 9 and Annexes A–G are informative and introduce no additional conformance obligations. In this document, “shall” specifies a requirement, “should” a recommendation, and “may” a permission. A note or example does not create an exemption from a requirement.

## 1 Scope and conformance

### 1.1 Scope

This standard applies to systems, data, cryptographic services, products, and third parties where cryptography protects confidentiality, integrity, authenticity, identity, or transaction trust. It covers risk from quantum-vulnerable cryptography and the security and operational risks of its replacement. It does not require a prediction of when a cryptographically relevant quantum computer will exist.

**QCI-1.1-01** The organization shall define an assessment boundary identifying the legal entity or business unit, locations, environments, systems, services, critical data flows, supplier dependencies, assessment date and period, and applicable jurisdictional, sectoral, and contractual obligations. The executive sponsor shall approve the boundary. Shared trust, key management, and supplier dependencies material to in-scope services shall be included even when operated outside the organizational boundary.

**QCI-1.1-02** The organization shall document exclusions and their rationale, identify the approving owner, and evaluate whether each exclusion removes a material dependency. Criticality shall consider operational, financial, confidentiality, integrity, authenticity, legal, and safety consequences. A system, flow, or supplier whose failure could exceed approved risk appetite shall be classified as critical. A critical dependency shall not be excluded solely because evidence or supplier access is unavailable.

### 1.2 Conformance determination and claims

**QCI-1.2-01** The organization shall maintain a conformance record for every QCI requirement identifier and its incorporated criteria. The record shall state applicable or not applicable, rationale, evidence, assessor, assessment date, and conforming or nonconforming result. Conditional requirements may be not applicable only when the stated condition is absent and evidence supports that conclusion. Requirements shall not be omitted solely because they are difficult to meet.

**QCI-1.2-02** A conformance claim shall be made only when all applicable requirements are met. An accepted operational risk or approved exception shall not convert an unmet requirement into conformance. This edition does not permit a qualified conformance claim. An organization with

open nonconformities may state that it has been assessed against this standard, provided that it discloses the nonconformities and does not describe the result as conformity.

**QCI-1.2-03** A claim shall identify the standard version and edition date, assessment boundary and period, determination date, assessor and assessment type, and the location of the supporting conformance record. Assessment type shall distinguish self-assessment from independent assessment. The claim shall disclose scope limitations and shall not imply enterprise-wide coverage for a restricted assessment. Use of this standard shall not be described as QCI certification unless separately authorized by an established QCI certification scheme.

**QCI-1.2-04** The organization shall report conformance status separately from the Q-Risk Score. A score measures evidence-supported readiness maturity; it is not a probability of compromise, guarantee of quantum resistance, certificate of security, or determination of regulatory compliance. Nonconforming organizations may calculate a score, with the nonconforming status displayed alongside it.

### 1.3 Adoption and edition transition

**QCI-1.3-01** An organization adopting the issued version 2.3 shall record its adoption date and assessment basis. It shall complete the identity-field split and other changed records by its first quarterly assessment after adoption and no later than 90 calendar days after adoption. It shall not claim version 2.3 conformance until all applicable requirements are met. Earlier-edition claims shall identify their actual edition. This transition does not defer an earlier external obligation.

**QCI-1.3-02** The organization shall disclose edition, scoring-profile, scope, denominator, and evidence-rule changes that affect a reported trend. It shall restate prior scores using the current method and retained evidence, or mark the time series as not directly comparable. It shall not fabricate missing historical evidence.

## 2 References and external applicability

### 2.1 Reference status

There are no external documents incorporated in full as indispensable normative dependencies for QCI-QS1 governance conformance. The specific requirements in Clauses 1–8 are self-contained. Selection or use of a cryptographic mechanism remains subject to the applicable technical specification, approved organizational profile, and binding external requirements under Clauses 2.2 and 4.5. Annex E distinguishes final standards, drafts, guidance, policy, and illustrative industry specifications.

FIPS 203, FIPS 204, and FIPS 205 specify ML-KEM, ML-DSA, and SLH-DSA respectively. They do not by themselves specify all protocol integration, key lifecycle, or system assurance requirements. SP 800-227 addresses KEM use; CSWP 39upd1 addresses crypto agility. IR 8547 remains draft transition guidance at the reference baseline date. Source status and organizational applicability are separate questions.

## 2.2 Obligations and reference maintenance

**QCI-2.2-01** The organization shall maintain an applicability register listing each relevant external obligation or adopted technical profile, issuer, exact document title and revision, date, authoritative URL, applicable sections, status, affected systems and suppliers, required actions and deadlines, exception authority, accountable owner, and last verification date. It shall distinguish law, regulation, contract, binding policy, organizational policy, recommendations, and drafts. A general migration target shall not override an earlier applicable deadline.

**QCI-2.2-02** The Quantum Risk Owner, with legal/compliance and engineering owners, shall review the register at least quarterly and on notification of material policy, standard, errata, vulnerability, or supplier changes. The organization shall record the impact decision, required action, owner, and due date. A new edition of an external document shall not silently replace an approved technical profile without impact review.

**QCI-2.2-03** Where requirements conflict, the organization shall document the conflict and obtain a determination from its competent compliance and technical authorities before deployment. QCI conformance shall not be used to waive a binding external requirement. Experimental or draft mechanisms shall be identified as such and governed by Clause 4.5.

## 3 Terms and definitions

**Quantum-related cryptographic risk:** Exposure arising from quantum-vulnerable cryptography, dependencies that delay its replacement, or insecure implementation of the transition.

**Post-quantum cryptography (PQC):** Cryptographic algorithms designed to resist attacks by classical and quantum computers. The term does not imply an unconditional security guarantee.

**Cryptographically relevant quantum computer (CRQC):** A quantum computer capable of defeating a cryptographic protection at a scale relevant to the assessed use.

**Cryptographic dependency:** A cryptographic use or supporting service, implementation, key, certificate, trust anchor, protocol, product, or supplier upon which a system relies.

**Confidentiality horizon:** The date until which information must remain confidential, or a duration with an explicit start date. **Verification horizon:** The date until which authenticity, integrity, provenance, or nonrepudiation evidence must remain verifiable. These horizons are assessed separately.

**Harvest now decrypt later (HNDL):** Collection of encrypted information or protected key material for potential future decryption. Updating current protection cannot erase copies already obtained by an adversary.

**Crypto agility:** The organizational and technical ability to replace or adapt cryptographic mechanisms with controlled, repeatable effort while preserving security and operations. Planned component or platform replacement may be necessary for constrained or immutable systems.

**High-impact finding:** A nonconformity or weakness assessed as exceeding approved risk appetite or threatening a binding obligation or safety objective.

**Critical trust pathway:** An end-to-end dependency chain protecting a critical operation, including relevant endpoints, intermediaries, authentication, key establishment, trust anchors, and key management.

**Validated inventory record:** A record whose accountable system or flow owner, with an authorized technical reviewer, confirms its identity, dependency links, evidence, completeness disposition, and freshness under Clause 5.1. Owner acknowledgement alone does not verify unknown cryptographic attributes.

**Cryptography Bill of Materials (CBOM):** A machine-readable description of cryptographic assets and relationships for a product or deployment. A CBOM may support inventory evidence but is not proof of complete deployment coverage.

**Discovery output:** Findings generated by examining code, binaries, hosts, network endpoints, configuration, or other sources. Scan reach describes what the tool examined; it is distinct from owner-validated inventory coverage.

**Cryptographic domain:** A category for organizing dependencies and migration activity. The thirteen non-exclusive categories in Annex G include two foundation layers and eleven technology domains. A system can carry multiple domain tags.

**ML-KEM:** The module-lattice-based key-encapsulation mechanism in FIPS 203. **ML-DSA:** The module-lattice-based signature algorithm in FIPS 204. **SLH-DSA:** The stateless hash-based signature algorithm in FIPS 205.

**KEM:** A mechanism for establishing a shared secret using encapsulation and decapsulation.

**Key wrapping:** Protection of an existing cryptographic key using a separate key-encryption mechanism. A complete scheme may combine a KEM, key derivation, and symmetric key wrapping.

**PQ/T hybrid:** A specified combination of post-quantum and traditional mechanisms of the same function, such as key establishment. Its security depends on the construction, implementation, and verification or negotiation policy. Hybrid key establishment does not itself establish post-quantum authentication.

**AI system:** A system that trains, fine-tunes, stores, serves, or coordinates machine-learning models. **AI artifact:** A dataset, model weight/parameter set, registry entry, signed provenance record, or other asset produced or consumed by an AI system. Channel and identity dependencies are linked to the artifacts and services they protect.

**Governing body:** The board, designated board committee, or equivalent accountable oversight body for the organization. **Independent assessor:** A competent reviewer who did not design, implement, or operate the controls being assessed and has no responsibility for the assessed outcome.

## 4 Governance and accountability

### 4.1 Ownership and resources

**QCI-4.1-01** The organization shall appoint an executive sponsor accountable for quantum readiness and a Quantum Risk Owner accountable for program execution. It shall assign documented responsibilities to engineering/architecture, system and data owners,

procurement/vendor risk, incident response, legal/compliance, and assurance. A cross-functional steering function shall resolve dependencies and delivery decisions. Roles may be combined where conflicts are managed; independent-assessment requirements remain applicable.

**QCI-4.1-02** The governing body shall receive reporting at least quarterly, approve risk appetite and escalation authority, and review delivery capacity and funding decisions. The executive sponsor shall maintain a resourced roadmap with accountable owners, dependencies, estimated effort/cost, committed capacity, start and completion milestones, acceptance criteria, and decisions required. Resource shortfalls shall be recorded as delivery risks rather than hidden by later dates.

## 4.2 Required governance artifacts

**QCI-4.2-01** The organization shall maintain an approved quantum risk policy and assessment scope; an enterprise risk-register section; the obligations/profile register; a dependency-aware migration roadmap; the QASI and coverage reports; a quarterly conformance record and Q-Risk assessment; supplier evidence and exceptions; migration/test and incident evidence; and the quarterly governing-body insert. Records may be integrated into existing management systems if their content and traceability are preserved.

**QCI-4.2-02** Each roadmap decision shall consider confidentiality and verification horizons, present capture exposure, consequences, supplier and trust dependencies, implementation lead time, operational constraints, end-of-support, and applicable deadlines. Planning, procurement, pilot, production acceptance, and retirement shall be separately identifiable. Long-lead hardware and trust-anchor changes shall start when the risk/dependency analysis requires; there shall be no mandatory sequence that postpones all signature or hardware work until key-exchange work is complete.

## 4.3 Risk appetite and exceptions

**QCI-4.3-01** The organization shall define escalation thresholds for high-impact exposure, missing ownership or evidence, overdue milestones, failed tests, unauthorized fallback, supplier failure, and impending obligation or exception deadlines. It shall define urgent notification time limits and authorities in its policy and act within those limits rather than waiting for the next quarterly report.

**QCI-4.3-02** Each accepted risk or operating exception shall identify affected assets and requirements, rationale, exposure and residual risk, treatment/compensating controls, owner, competent approving authority, approval date, expiry, review triggers, remediation dates, and exit or replacement strategy where feasible. An infeasible exit shall have a documented rationale and alternative treatment. Exceptions shall be reviewed at least quarterly and on a material trigger; renewal shall be an explicit decision before expiry. Unapproved or expired exceptions shall be escalated. Conformance treatment remains subject to Clause 1.2.

## 4.4 Cryptographic incident readiness

**QCI-4.4-01** Incident procedures shall cover algorithm or implementation compromise, stolen keys or seeds, trust-anchor/certificate failure, signature forgery, unauthorized downgrade, harvested ciphertext or key-envelope exposure, supplier cryptographic failure, and emergency migration. Procedures shall assign containment, impact assessment, evidence preservation,

escalation/communications, revocation, trusted recovery, and return-to-service criteria. They shall distinguish observed compromise, suspected exposure, and uncertainty; absence of observable HNDL activity shall not establish absence of exposure.

**QCI-4.4-02** The organization shall exercise representative critical signing, communications, storage/key-management, and supplier scenarios at least annually and after material architectural changes that invalidate prior exercises. It shall document participants, conditions, outcomes, corrective actions, owners, and due dates. Integrated exercises may cover multiple scenarios. Recovery shall not rely solely on cryptographic evidence from a mechanism believed compromised.

**QCI-4.4-03** Where AI systems are in scope, exercises and procedures shall additionally address D7-AI-1 provenance forgery affecting datasets, models, registries, signatures, or attestations; D7-AI-2 harvested AI assets protected by vulnerable key establishment or key envelopes; and D7-AI-3 downgrade of workload or agent channels. Re-signing shall first establish artifact integrity and provenance using trusted evidence under Clause 4.6. These scenarios concern cryptographic incidents, not general AI behavior or safety.

## 4.5 Approved cryptographic profiles

**QCI-4.5-01** The organization shall maintain approved, restricted, experimental, and prohibited cryptographic profiles. Each profile shall identify function, algorithm and parameter set, protocol/construction and version, encoding/credential dependencies, required security strength/category, implementation/version constraints, applicable technical standards and errata, allowed operating modes, rationale, owner, approval date, and review date. Supported capability, configured capability, and observed production use shall be distinguished.

**QCI-4.5-02** Production changes shall use an approved profile and applicable technical specifications. Experimental mechanisms shall be isolated or subject to a documented, time-limited risk decision specifying data and deployment restrictions. Selection for future standardization, a draft specification, or a supplier's "quantum-safe" label shall not alone establish production approval. Algorithm or implementation advisories shall trigger impact review under Clause 2.2.

**QCI-4.5-03** A hybrid profile shall specify its components, combiner or protocol construction, authentication mechanism, negotiation and verification policy, and permitted fallback behavior. Key establishment and authentication shall have separate posture records. Unauthorized classical fallback shall be prevented or detected and acted upon within the defined policy limit. Any permitted fallback shall have an approved scope, expiry, monitoring, and residual-risk record. Dual-signature verification shall follow the approved security construction; accepting either signature shall not be assumed to preserve protection when one algorithm fails.

**QCI-4.5-04** A KEM-based key-protection profile shall separately identify encapsulation, key derivation, symmetric key wrapping or authenticated encryption, recipient authentication/trust, and bulk-data encryption. It shall not describe ML-KEM alone as directly encrypting an existing data key. Hybrid use shall be a documented applicability and engineering decision, including transition/retirement criteria where an interim construction is used.

## 4.6 Key and trust lifecycle

**QCI-4.6-01** The organization shall govern cryptographic key and seed generation, entropy assurance, custody/access, purpose separation, distribution, cryptoperiods/rotation, backup/recovery, revocation, compromise response, archival needs, and destruction. Controls shall be proportionate to key purpose and applicable profiles. Secret keys and seeds shall not be stored in the QASI. Where stateful signatures are used, the profile shall prevent one-time signing-state reuse across backup, restore, replication, failover, and migration.

**QCI-4.6-02** Trust migration shall include certificate chains, roots, trust-store distribution, issuance and revocation services, offline verifiers, code/firmware update verification, and recovery paths. Re-signing or renewal of historical evidence shall first establish trusted artifact integrity and provenance; it shall preserve relevant historical validation, timestamp, and trust-chain records. Unverifiable artifacts shall be quarantined or handled through an approved exception, not automatically re-signed.

**QCI-4.6-03** Storage migration decisions shall assess the bulk cipher/mode, key generation/custody, current and historical key envelopes, backups/replicas, and potential capture. Sound AES-256 encryption does not require replacement solely because of the quantum threat; compromised keys, insecure modes, or exposed key protection may require new data keys and re-encryption. The organization shall document its rewrap, rekey, re-encrypt, retain, or retire decision and residual exposure. Updating present copies shall not be reported as remediation of copies already harvested by an adversary.

## 4.7 Migration testing and acceptance

**QCI-4.7-01** Each production migration shall have a risk-appropriate test and acceptance plan covering end-to-end interoperability, actual algorithm negotiation, authentication and trust validation, invalid key/ciphertext/signature inputs, downgrade/fallback, message/certificate size and fragmentation where relevant, resource exhaustion, capacity/latency, backup/restore, failover, and authorized rollback. Omitted test categories shall have a documented technical non-applicability rationale. Test environments and configurations shall be representative of the affected critical pathway.

**QCI-4.7-02** Before acceptance, engineering and the accountable service owner shall approve results, failure dispositions, operational monitoring, support readiness, recovery procedures, residual exceptions, and an observation period proportionate to the change. Rollback that restores vulnerable protection shall be governed as an exception. Completion shall require evidence of effective production configuration, removal or explicit exception of legacy paths, and disposition of obsolete keys, certificates, and configurations. A pilot or vendor release alone shall not count as production migration.

## 4.8 Evidence and assurance

**QCI-4.8-01** Every conformance result, maturity criterion, coverage claim, and migration-completion claim shall link to attributable, dated evidence applicable to the assessed scope and configuration. Evidence records shall identify producer, reviewer, integrity/provenance controls, retention period, and access restrictions. The policy shall retain each assessment pack through at least the next annual assurance cycle and longer where obligations require. Sensitive inventories and supplier evidence shall be protected from unauthorized access and alteration.

**QCI-4.8-02** Assessors shall have documented competence appropriate to the cryptographic, operational, and governance subjects assessed. They shall define risk-based sampling, including all unresolved high-impact exceptions and representative critical pathways, and retain population, selection rationale, evidence, findings, and closure verification. Sampling shall not alter inventory or migration denominators. Level 5 in any pillar shall require independent review of that pillar within the previous 12 months and after material changes that invalidate the review.

**QCI-4.8-03** Assurance records shall distinguish supplier assertion, algorithm testing, cryptographic-module validation, and full-system acceptance. Where external obligations require module validation, the record shall identify certificate, status, covered implementation/version/configuration, relevant algorithms, and caveats. A validated algorithm or module shall not be represented as assurance of the complete deployed system. The organization shall track nonconformities to owners, due dates, and verified closure.

## 5 Inventory and visibility

### 5.1 Population and coverage

**QCI-5.1-01** The organization shall inventory all identified in-scope critical systems and critical data flows, including outsourced dependencies. It shall reconcile the population at least quarterly against authoritative service/asset records, architecture and data-flow records, procurement/cloud records, and available discovery evidence. It shall document unresolved population discrepancies and a plan to discover material dependencies beyond the initial population. New critical items shall enter the denominator when identified, even if their records are incomplete.

**QCI-5.1-02** Each system and critical-flow record shall have a named accountable owner and technical reviewer. Validation shall check all required fields or justified non-applicability, dependency links, evidence relevance, and current configuration. Unknown values shall remain explicit, with risk, owner, due date, and investigation plan. A record with unknown algorithm, profile/parameters, critical trust dependency, or key-protection mechanism shall not count as validated coverage for scoring. Unknown optional descriptive details shall not alone invalidate coverage.

**QCI-5.1-03** The organization shall separately calculate system coverage and critical-flow coverage as 100 times the number of current validated critical records divided by the complete identified critical population in that category. It shall publish numerator, denominator, unvalidated/unknown count, exclusions, reconciliation gaps, and changes since the prior assessment. No applicable items shall be reported as not applicable with rationale, not as 100 percent. Decommissioned items may leave a denominator only with evidence and a recorded change. Scan reach shall never replace these metrics.

**QCI-5.1-04** Validation shall be renewed at least quarterly, with critical evidence no older than 90 calendar days unless a documented review within that period confirms unchanged configuration and continuing relevance. Material system, supplier, key/trust, protocol, or deployment changes shall trigger revalidation before affected coverage or completion claims are retained. Stale evidence shall not support a gate or maturity criterion. Automated change monitoring may support revalidation but does not remove owner accountability.

## 5.2 Required QASI records

**QCI-5.2-01** The QASI shall retain a system-level summary linked to one or more cryptographic-use, critical-flow, trust/key-dependency, and supplier/product records as needed to represent actual dependencies. The following field groups are required. A field shall contain a known value, an explicit unknown under Clause 5.1, or a justified not-applicable value. Multiple cryptographic uses or AI artifact classes shall not be collapsed into one ambiguous value.

| Record group                  | Minimum fields                                                                                                                                                                                                                                                                         |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                 | Unique ID and name; service/environment; criticality and rationale; owner/reviewer; data classification; confidentiality end date and verification end date; human identity dependencies; workload identity dependencies; cryptographic domain tags; linked uses, flows and suppliers. |
| <b>Cryptographic use</b>      | Use ID and system link; function/purpose; algorithm and key size/parameter set; protocol/profile/construction and version; library/module and exact deployed version; endpoint/component; supported, configured and observed status; current and target posture.                       |
| <b>Flow</b>                   | Flow ID; source, destination and termination/intermediary points; data/service purpose; criticality; owner; protection and authentication at each relevant hop; linked uses/trust dependencies; capture exposure and horizons.                                                         |
| <b>Trust and keys</b>         | Reference IDs for keys/certificates/trust anchors; purpose and issuer/recipient relationships; key-management method; key-establishment, KDF, wrap and bulk cipher/mode where relevant; lifecycle and recovery dependencies; associated policy/profile. No secret material.            |
| <b>Supplier and product</b>   | Supplier and service/product ID; release/configuration and customer deployment; shared responsibilities; evidence/attestation dates; roadmap and support/end-of-life status; linked uses, exceptions and contractual obligations.                                                      |
| <b>Treatment and evidence</b> | Exposure type and risk flags; approved profile and crypto-agility status; treatment state and residual risk; compensating controls; owner and target dates; evidence/finding IDs, provenance and review date; validation status; linked change, test and exception records.            |

**QCI-5.2-02** Cryptographic domain tags shall use the Annex G identifiers or a documented local taxonomy mapped to them. Multi-tagging is permitted. A critical system with no classification shall be treated as an incomplete record. Human identity shall cover relevant federation, SSO, token signing, smart cards and passkeys. Workload identity shall cover machine, service, workload and agent credentials, issuance, authentication, and verification roots. Classical public-key inventory shall include applicable RSA, finite-field DH/DSA, ECDH, ECDSA, and EdDSA uses rather than relying on an undifferentiated “ECC” label.

**QCI-5.2-03** For AI systems, linked records shall additionally capture each material artifact class; separate confidentiality and provenance/verification horizons; model/dataset/registry signing and provenance schemes; workload/agent identity dependencies; channel key-establishment and authentication profiles; and the complete artifact-key protection construction. A non-AI system shall record AI applicability as none, with no additional AI scoring penalty. The AI requirements shall be assessed in their relevant existing pillars; no separate AI pillar or bonus shall be added.

## 5.3 Exposure and treatment flags

**QCI-5.3-01** The organization shall separately record exposure and treatment status. Minimum exposure flags shall cover vulnerable protection of long-lived confidentiality; signature/trust dependencies with long verification horizons; unknown algorithms/profiles or critical trust/key protection; missing ownership or evidence; critical supplier evidence gaps; rigid or unsupported components; inadequate discovery provenance; and unauthorized fallback. AI artifact exposures shall use the same rules and identify their artifact class. An approved migration plan shall not clear an exposure flag.

**QCI-5.3-02** Treatment status shall distinguish untreated, approved plan, implementing, overdue, mitigation verified, and residual risk accepted. Horizon analysis shall use dates or durations with explicit start dates and consider present capture and migration lead time. Missing migration dates shall be recorded as unknown and escalated, not used to suppress a flag. Mitigation closure shall require evidence of the relevant reduction in exposure; segmentation, rotation, minimization, or tokenization shall not be assumed to remove HNDL risk without analysis of the protected path and dependencies.

## 5.4 Discovery and vendor evidence

**QCI-5.4-01** For each field derived from discovery output, the evidence reference shall identify the tool and exact version; materially relevant configuration/ruleset; examined scope and run date, using repository/commit, image digest, host, endpoint, or network range as appropriate; omitted scope and reason, or inability to report omissions; stable finding ID and location; and output artifact location plus digest algorithm and digest. It shall map the finding to the QASI field and retain producer, reviewer, confidence/disposition, and validation date. A digest shall not alone be treated as proof of authorship or authenticity.

**QCI-5.4-02** The organization shall reconcile conflicting static, runtime, configuration, and supplier evidence and record false-positive and unresolved dispositions. Where tool limitations leave material visibility unknown, it shall use another evidence method or record an operating exception and incomplete coverage. Scan reach may be reported alongside provenance, explicitly labeled as such. Schema validity or scanner success shall not establish inventory completeness.

**QCI-5.4-03** Vendor CBOM evidence shall meet the same scope, attribution, finding-location, integrity, and review objectives. Where no discovery tool produced the CBOM, the vendor generation method, schema/version, authorized producer, production date and product/release scope shall replace inapplicable scan-tool fields; omissions and limitations shall be explicit. The receiving organization shall validate relevance to its deployment. Vendor intellectual-property restrictions may change the evidence-access mechanism but shall not convert unsupported claims into validated coverage.

# 6 Q Risk readiness scoring

## 6.1 Profile and calculation

**QCI-6.1-01** The organization shall assess each applicable pillar using the fixed **QCI-QS1 2.3 Core** profile and the criteria in Clauses 6.6–6.10. It shall use integer levels 0–5, award the highest level for which every criterion at that level and all lower positive levels is supported, and

treat unsupported, contradictory, or stale evidence as failure of the affected criterion. It shall not average away a failed criterion, award fractional levels, or substitute narrative intent for evidence. Conditional criteria are satisfied only by evidence of performance or evidence that their stated condition is absent.

| Pillar | Subject                                    | Weight |
|--------|--------------------------------------------|--------|
| P1     | Governance and accountability              | 20     |
| P2     | Crypto visibility and QASI completeness    | 20     |
| P3     | Data longevity and exposure management     | 20     |
| P4     | PQC migration readiness and crypto agility | 25     |
| P5     | Third-party readiness                      | 15     |

**QCI-6.1-02** For five applicable pillars, the raw score R shall equal  $4 \times L1 + 4 \times L2 + 4 \times L3 + 5 \times L4 + 3 \times L5$ , where L1–L5 are the awarded levels. The final score shall be the minimum of R and every cap triggered under Clause 6.3. All results are integers and shall not be rounded. The report shall show pillar levels, weighted contributions, raw score, each gate result and reason, final score, band, scope, conformance status, and assessment date.

**QCI-6.1-03** A pillar shall be not applicable only where its entire subject population is demonstrably absent. Absence shall be independently checked by the relevant business/technical function and documented in the assessment. No weight shall be redistributed and no automatic maximum credit awarded. Where any pillar is not applicable, the organization shall publish the applicable pillar levels and an applicability statement without a 0–100 total or readiness band. An organization with no identified critical population shall not present a total score as comparable until scope and criticality are substantiated. AI absence alone does not make a pillar not applicable.

## 6.2 Maturity meaning and measurement rules

The six levels are 0 Unaware, 1 Aware, 2 Defined, 3 Implementing, 4 Managed, and 5 Assured. These labels summarize the detailed criteria; they do not replace them.

**QCI-6.2-01** Metric percentages used in this clause shall retain full calculation precision for threshold decisions and display at least one decimal place. Numerators, denominators and category definitions shall be retained. A zero denominator shall be handled as an evidenced absent condition, not manufactured success. A critical population discrepancy that could materially change a metric shall prevent the affected criterion or gate from passing until resolved.

**QCI-6.2-02** Migration completion shall be measured over critical systems or flows identified as requiring transition in the approved risk assessment. Completion shall mean accepted production protection or verified decommissioning with vulnerable dependency retirement under Clause 4.7. Supplier availability, a plan, an accepted risk, or a pilot shall not count as completion. The baseline and all additions/removals shall be recorded; deferring an item shall not remove it from the denominator. Systems already meeting the approved target profile shall be supported by current evidence and reported separately from newly migrated items.

## 6.3 Gates and comparability controls

**QCI-6.3-01** The organization shall apply the following gates consistently after calculating the raw score. A failed gate applies regardless of the result of other gates. A gate may be passed on an absent condition only where that specific population is demonstrably absent under Clause 6.2; this does not override the no-total rule for an absent pillar.

| Gate                     | Pass condition                                                                                                                                                                                                                              | Failed gate cap |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>G60<br/>Inventory</b> | Both critical-system and critical-flow validated coverage are at least 95 percent, with no unresolved material population discrepancy. Where one category is absent, evidence substantiates absence and the other meets the threshold.      | 60              |
| <b>G70<br/>Suppliers</b> | Every critical supplier has a current, adequate product/deployment-specific roadmap response and authorized attestation assessed under Clause 7. An approved operating exception is not a substitute.                                       | 70              |
| <b>G80<br/>Agility</b>   | At least one critical trust pathway has passed a representative end-to-end crypto-agility test under Clause 4.7 within the previous 12 months and after any invalidating material change. The pathway and limits of the test are disclosed. | 80              |

**QCI-6.3-02** Peer comparisons shall use the same edition and Core profile, period basis, criticality criteria, scope category, and metric definitions, and shall disclose material differences in estate size, sectors, obligations, AI applicability, supplier reliance and evidence quality. Where these conditions are not established, the score shall be labeled an internal readiness snapshot, not a like-for-like benchmark. Organization-specific thresholds or alternative weighting may be reported only as separately named supplemental metrics, never as the Core score.

## 6.4 AI and supplier posture

**QCI-6.4-01** Where critical suppliers operate AI platforms, ML infrastructure, model registries, or AI artifact key management, their cryptographic posture shall be included in P5 using Clause 7 and questions G1–G5 in Annex C. Internal AI asset visibility, exposure, migration, and incident evidence shall also contribute to P1–P4 where relevant. The same evidence may support different criteria only where the distinct purpose of each use is recorded.

## 6.5 Reporting and bands

**QCI-6.5-01** The organization shall produce and archive the score assessment at least quarterly, including evidence references, pillar decisions, changes, gate effects, nonconformities, and the reporting elements in Clause 8. The score shall use the following bands. Scores at exactly 60, 70, or 80 do not imply that the corresponding above-cap gate has passed.

| Final score  | Band       | Interpretation                                               |
|--------------|------------|--------------------------------------------------------------|
| <b>0–19</b>  | Exposed    | Limited evidence of an established readiness program.        |
| <b>20–39</b> | Behind     | Initial awareness or defined elements with substantial gaps. |
| <b>40–59</b> | Mobilizing | Evidence of coordinated preparation and early execution.     |

| Final score | Band                 | Interpretation                                                                                          |
|-------------|----------------------|---------------------------------------------------------------------------------------------------------|
| 60–80       | Advancing            | Progress with remaining gate, coverage, or execution limitations.                                       |
| 81–100      | Defensible readiness | Higher evidence-supported maturity with all score gates passed; not a security or compliance guarantee. |

## 6.6 P1 governance rubric

**QCI-6.6-01** P1 shall be awarded cumulatively against this table. Independent assurance for level 5 is as defined in Clause 4.8.

| Level | Required evidence                                                                                                                                                                                                                 |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | One or more level 1 criteria are unsupported.                                                                                                                                                                                     |
| 1     | Named sponsor and Quantum Risk Owner; documented initial scope and initial quantum-risk entry.                                                                                                                                    |
| 2     | Approved policy, roles, risk appetite, obligations register, resourced roadmap and exception process; a completed governing-body briefing.                                                                                        |
| 3     | At least one quarterly inventory–assessment–action–report cycle completed; roadmap actions have recorded outcomes; incident procedures cover all applicable Clause 4.4 scenarios.                                                 |
| 4     | Two consecutive quarterly cycles completed on time; every overdue action and resource shortfall is escalated with an authorized decision; applicable incident exercise coverage is current and corrective actions are controlled. |
| 5     | Independent review confirms all P1 criteria and evidence traceability; no overdue high-impact governance nonconformity; governing body has reviewed program effectiveness and approved resulting actions.                         |

## 6.7 P2 visibility rubric

**QCI-6.7-01** P2 shall be awarded cumulatively against this table, using the separate coverage measures in Clause 5.1.

| Level | Required evidence                                                                                                                                                                                                |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | One or more level 1 criteria are unsupported.                                                                                                                                                                    |
| 1     | Initial critical-system and flow populations, owners and discovery sources identified; unknowns explicitly recorded.                                                                                             |
| 2     | Required QASI record structure and validation process operating; at least 50 percent validated coverage in each applicable category; reconciliation and discovery limitations documented.                        |
| 3     | At least 80 percent validated coverage in each applicable category; linked use/trust/supplier records maintained; material changes enter the revalidation process.                                               |
| 4     | At least 95 percent validated coverage in each applicable category; discovery provenance satisfies Clause 5.4; no unresolved material population discrepancy; unknowns and stale records have owned remediation. |
| 5     | 100 percent validated coverage in each applicable category; independent sampling confirms accuracy, links and current evidence; no unresolved high-impact visibility finding.                                    |

## 6.8 P3 exposure management rubric

**QCI-6.8-01** P3 shall be awarded cumulatively against this table. Horizon-and-exposure coverage uses all critical systems and flows in scope as its respective denominators and counts only records with separate justified horizons, relevant exposure analysis, and owner confirmation.

| Level | Required evidence                                                                                                                                                                                               |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | One or more level 1 criteria are unsupported.                                                                                                                                                                   |
| 1     | Critical data/service categories and initial confidentiality, verification and HNDL concerns identified.                                                                                                        |
| 2     | Approved risk method and treatment rules; horizon-and-exposure coverage at least 50 percent in each applicable category; exposures separated from plans and accepted risk.                                      |
| 3     | Horizon-and-exposure coverage at least 80 percent in each applicable category; every identified above-appetite exposure has an approved owned treatment or escalated decision; treatment progress is evidenced. |
| 4     | Coverage is 100 percent; two quarterly reviews show current exposure/treatment records; overdue treatments and historical-copy limitations are explicitly reported; closures have verified mitigation evidence. |
| 5     | Independent review validates risk prioritization, horizons and a risk-based sample of mitigation closures; no unapproved above-appetite exposure and no overdue high-impact finding.                            |

## 6.9 P4 migration and agility rubric

**QCI-6.9-01** P4 shall be awarded cumulatively against this table. “Representative” testing at levels 4–5 covers each materially distinct critical protocol, trust, key-management, and deployment pattern; a documented equivalence analysis may justify shared tests.

| Level | Required evidence                                                                                                                                                                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | One or more level 1 criteria are unsupported.                                                                                                                                                                                                                           |
| 1     | Vulnerable dependencies and initial approved target candidates identified; engineering owners assigned.                                                                                                                                                                 |
| 2     | Approved profiles and a prioritized, resourced dependency roadmap with acceptance, recovery and retirement criteria; long-lead replacement decisions recorded.                                                                                                          |
| 3     | A representative pilot has passed applicable Clause 4.7 tests; at least one critical production transition is accepted, or current evidence establishes that no critical transition is needed because the entire critical population already meets its approved target. |
| 4     | At least 90 percent completion in each applicable critical transition category; every remaining item has an owned deadline and treatment; representative operational tests cover the deployed patterns and recovery/fallback behavior.                                  |
| 5     | 100 percent completion in each applicable category; no unauthorized legacy critical path; current representative tests and independent review confirm configuration, trust/key lifecycle, recovery and retirement evidence.                                             |

## 6.10 P5 supplier rubric

**QCI-6.10-01** P5 shall be awarded cumulatively against this table. Adequate evidence and current attestation have the meaning specified in Clause 7. Supplier percentages use all identified critical suppliers in scope.

| Level | Required evidence                                                                                                                                                                                                                                                      |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | One or more level 1 criteria are unsupported.                                                                                                                                                                                                                          |
| 1     | Critical suppliers identified; accountable relationship owners assigned; initial requests issued.                                                                                                                                                                      |
| 2     | Complete standard request issued to every critical supplier; response deadlines, adequacy criteria and exception register operating; at least 50 percent have current adequate responses and attestations.                                                             |
| 3     | At least 80 percent have current adequate responses and attestations; shared responsibilities and deployment obligations documented; missing/inadequate evidence is escalated and treated.                                                                             |
| 4     | Every critical supplier has current adequate response and attestation; material milestones and notification obligations are contractually established or have approved procurement exceptions; customer deployment evidence is distinguished from supplier capability. |
| 5     | Independent review confirms a risk-based sample of supplier claims against technical/customer evidence; every due material milestone is met or an approved alternative is deployed; no overdue high-impact supplier finding.                                           |

## 7 Third party oversight

### 7.1 Applicability and procurement

**QCI-7.1-01** The organization shall identify and assess suppliers materially affecting identity/trust, signing, secure communications, key management, regulated or long-lived confidentiality, transaction integrity, or relevant AI infrastructure. It shall include cloud, SaaS, managed services, embedded products and material subservice dependencies. Criticality shall follow Clause 1.1. Supplier scope shall identify products/releases, actual customer deployment, and ownership of configuration, testing, monitoring and remediation.

**QCI-7.1-02** New or renewed material procurements shall evaluate PQC profiles, migration support, upgrade cost/lead time, evidence access, support life, incident/change notification, and exit or substitution options. Material contractual gaps shall be resolved or accepted by the appropriate risk/procurement authority before commitment. A supplier roadmap shall not be represented as deployed protection.

### 7.2 Request content and evidence adequacy

**QCI-7.2-01** Every critical supplier request shall cover the following minimum questions, operationalized by Annex C: A product scope and cryptographic footprint; B milestones and supported standards/profiles; C agility, integration and upgrade path; D testing, validation and assurance; E customer responsibilities, commercial/support terms and dependencies; F disclosure and incident readiness. Applicable AI suppliers shall also receive G1–G5. The

request shall seek evidence attachments or controlled evidence access; unavailable evidence shall be explicitly identified and assessed as a limitation.

**QCI-7.2-02** The authorized attestation shall identify the supplier legal entity, customer-facing products/services and releases covered, as-of date, verified facts versus future commitments, algorithm/library inventory, migration milestones, customer transition steps, supported profiles, disclosure obligations, limitations and exclusions, evidence references, and signatory name, role, authority, signature and date. An officer or equivalently authorized signatory shall sign it. It shall not imply that all future commitments are presently implemented.

**QCI-7.2-03** A response shall count as adequate only when it addresses every applicable request area, identifies product/deployment scope, separates available/configured/deployed posture, supplies assessable evidence for material present-tense claims, and provides owned, dated commitments and limitations. The organization shall record engineering and vendor-risk acceptance or reasons for inadequacy. Attestations shall be refreshed at least annually and on material cryptographic change; customer relevance and material changes shall be checked quarterly. Superseded or materially invalidated evidence shall not pass G70.

**QCI-7.2-04** The request shall set a response deadline no later than 60 calendar days after issue, unless an earlier obligation applies. Nonresponse or inadequate response at the deadline shall enter the exception/escalation process. Risk acceptance may permit continued service but shall not satisfy G70. Supplier CBOM evidence shall be evaluated under Clause 5.4 and validation claims under Clause 4.8.

## 7.3 Exceptions and ongoing oversight

**QCI-7.3-01** Supplier exceptions shall meet Clause 4.3 and include missed commitments, concentration/subservice dependencies, compensating controls, feasible exit/replacement plans, and customer actions. Relationship owners shall track milestones and material changes at least quarterly. The governing-body insert shall include top critical supplier exceptions and decisions, including cases where no feasible exit exists.

# 8 Governing body reporting

## 8.1 Mandatory reporting elements

**QCI-8.1-01** At least quarterly, the governing-body insert shall include the assessment boundary, date, edition/profile and conformance status; pillar levels, raw and capped score or not-applicable explanation, band, gate outcomes and prior-period changes; validated system and flow coverage with numerators/denominators; unknown/stale evidence and scope changes; principal confidentiality and verification exposures, including AI where applicable; production migration completion versus supplier/pilot capability; critical supplier readiness and exceptions; crypto-agility test coverage and limitations; overdue milestones, failed tests, open high-impact findings and expiring exceptions; actions completed/planned; and decisions on resources, priorities, acceptance or remediation.

**QCI-8.1-02** Reporting shall distinguish maturity improvement from verified exposure reduction and shall not clear exposure because a plan or attestation exists. It shall state material limitations, accepted residual risk, historical-copy exposure, and non-comparable trends.

Significant urgent events shall follow Clause 4.3 escalation without waiting for a quarterly meeting.

## 8.2 Oversight decisions

**QCI-8.2-01** The governing body shall review named accountability, evidence quality, funding/capacity, third-party dependencies, risk appetite, and actions requiring approval. Decisions shall record owner, rationale, due date, and follow-up. An acknowledgement of a report shall not be recorded as risk acceptance unless the authorized body explicitly approves the identified risk under Clause 4.3.

## Part B Implementation guidance

Clause 9 and all annexes are informative. Their examples support the requirements in Part A; they do not add obligations or provide alternative scoring rules.

## 9 Practical implementation

### 9.1 Establishing the program

A 90-day establishment sequence can begin with ownership, scope, criticality and population reconciliation in weeks 1–2; linked inventory and evidence validation in weeks 3–6; horizon/exposure analysis and supplier engagement in weeks 4–9; and a first assessment, roadmap, test plan and board insert in weeks 10–12. This sequence is a planning aid, not a conformance grace period or a reason to defer urgent exposure. Existing management systems can hold the required records.

### 9.2 Demonstrating agility

A useful proof changes an approved cryptographic profile in a realistic critical pathway, verifies negotiation and authentication at both ends, measures operational impact, rejects invalid or downgraded operation, and demonstrates recovery. The minimum G80 proof is deliberately narrower than the representative estate testing required for P4 levels 4–5. Documentation of this distinction prevents one successful demonstration from being mistaken for enterprise readiness.

### 9.3 Protecting AI assets

Prioritize AI assets using the same confidentiality, verification, consequence and lead-time criteria as other assets. Authenticating training datasets with quantum-resistant signatures is supported by the joint AI Data Security guidance in Annex E. Broader controls over model registries, provenance chains, artifact keys and workload channels are QCI applications of cryptographic risk management.

For artifact-key protection, specify the whole scheme: KEM, KDF, symmetric key wrap or authenticated encryption, recipient trust, and bulk cipher. Re-sign only artifacts whose integrity and provenance have been established. Sound AES-256 data protection can remain appropriate, while vulnerable or compromised key protection requires separate treatment. A current rewrap does not undo historical capture of an old key envelope.

## 9.4 Preparing evidence for assessment

Organize each assessment as a trace from requirement or criterion to scope, record, configuration, evidence, reviewer and conclusion. Retain population and sampling decisions, not only favorable screenshots. Independent reviewers can test reproducibility by applying the same rubric to the same evidence pack; disagreements should identify the exact criterion or evidence interpretation rather than averaging the scores.

## 9.5 Selecting technology and hybrid profiles

Select products for supported profiles, evidence quality, interoperability, upgrade/replacement path, operational performance and lifecycle support. A tool's discovery output is an input to the QASI. A product that supports PQC may still deploy a classical profile until configured and verified.

Hybrid key establishment can provide resilience when its specified construction and implementation preserve the intended security properties. It does not automatically upgrade certificates, signatures or authentication. Use protocol-specific specifications such as RFC 10024 where applicable and record binding-regime constraints. Weigh complexity and transition cost, including any later move to PQC-only, rather than treating hybrid as universally mandatory.

## 9.6 Sequencing across domains

Use Annex G to expose unowned dependencies, not as a fixed migration order. HNDL can affect TLS, VPNs, messaging, key envelopes and archives. Long-lived signatures, trust anchors, secure boot and constrained devices can require early parallel investment because replacement lead times are long. Each active domain benefits from an owner, roadmap milestone, acceptance evidence and reviewed deferral rationale. QCI-M1, if used, is a separate methodology and is not required for QCI-QS1 conformance.

## 9.7 Using the five components and eight assessment domains

The QRAF coordinates decisions; the QASI describes dependencies and exposure; the Q-Risk Score summarizes evidence-supported maturity; the Vendor Pack obtains attributable supplier facts and commitments; and the Board Insert supports oversight. The following QRAF domains organize review, without adding a second weighted score.

| Domain                                  | Assessment focus                                            | Primary clauses |
|-----------------------------------------|-------------------------------------------------------------|-----------------|
| <b>D1 Governance and accountability</b> | Ownership, policy, resources and decisions                  | 1, 4.1–4.3, 8   |
| <b>D2 Crypto asset visibility</b>       | Population, linked inventory and discovery evidence         | 5               |
| <b>D3 Data longevity exposure</b>       | Confidentiality/verification horizons and residual exposure | 4.2, 5.3, 6.8   |
| <b>D4 PQC migration readiness</b>       | Profiles, dependencies, testing and retirement              | 4.5–4.7, 6.9    |
| <b>D5 Third-party exposure</b>          | Supplier evidence, obligations and exceptions               | 7, 6.10         |

| Domain                               | Assessment focus                                   | Primary clauses |
|--------------------------------------|----------------------------------------------------|-----------------|
| <b>D6 Identity and trust</b>         | Human/workload credentials, keys and trust chains  | 4.6, 5.2        |
| <b>D7 Incident and resilience</b>    | Enterprise scenarios, recovery and AI applications | 4.4, 4.7        |
| <b>D8 Assurance and auditability</b> | Evidence, competence and independent review        | 1.2, 4.8, 6     |

## Annex A QASI implementation template

Informative. Clause 5.2 defines the required information. A relational database, spreadsheet with linked tabs, or existing inventory platform can implement it. This template illustrates one consistent arrangement.

| Record set               | Key                 | Links and suggested implementation                                                                                                        |
|--------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Systems</b>           | System ID           | One summary per deployed system/environment; links to uses, flows and suppliers; owners, criticality, horizons, identity and domain tags. |
| <b>Uses</b>              | Use ID              | One record per materially distinct cryptographic use/profile/component; reference system, module/version and observed configuration.      |
| <b>Flows</b>             | Flow ID             | Source, destination and each material termination point; reference protecting uses and trust dependencies.                                |
| <b>Trust and keys</b>    | Dependency ID       | Non-secret key/certificate/trust references, lifecycle owner and key-protection construction; reference dependent uses.                   |
| <b>Suppliers</b>         | Supplier/product ID | Product/release and customer configuration; responsibilities, evidence, attestation, roadmap and exception links.                         |
| <b>Evidence</b>          | Evidence/finding ID | Artifact location, provenance, scope, date, integrity metadata, reviewer/disposition and freshness.                                       |
| <b>Risks and actions</b> | Risk/action ID      | Exposure, treatment, residual risk, owner/dates, acceptance or closure evidence.                                                          |
| <b>AI artifacts</b>      | Artifact ID         | Applicable system and artifact classes, separate horizons, signing/provenance, keys, identity and channels.                               |

A record can state “unknown — investigation action R-17, owner and due date” instead of pretending a missing value is not applicable. Such a record remains outside validated coverage

when the unknown affects the key fields identified in Clause 5.1. Domain tagging is required by Clause 5.2; this annex does not create that obligation.

For example, a payments API may have separate uses for TLS key establishment, TLS authentication, transaction signing, storage encryption and storage-key protection. Recording “TLS, RSA, AES” in one cell would not show which dependency needs migration or whether a supplier's claimed capability is enabled. The linked-use approach preserves that distinction.

## Annex B Score worksheet and worked examples

Informative. Clause 6 is authoritative. A completed worksheet includes each pillar level, criterion evidence, contribution, all gate outcomes, conformance status, and scope/profile details.

| Pillar               | Level | Weight | Contribution         |
|----------------------|-------|--------|----------------------|
| <b>P1 Governance</b> | L1    | 20     | 4 × L1               |
| <b>P2 Visibility</b> | L2    | 20     | 4 × L2               |
| <b>P3 Exposure</b>   | L3    | 20     | 4 × L3               |
| <b>P4 Migration</b>  | L4    | 25     | 5 × L4               |
| <b>P5 Suppliers</b>  | L5    | 15     | 3 × L5               |
| <b>Raw total</b>     | —     | 100    | Sum of contributions |

The examples below are arithmetic and gate test cases, not assertions that an organization has achieved a particular posture. Pillar evidence is assessed before calculation; the stated gate results are inputs to these examples.

| Case                             | Levels P1 to P5 | Raw | Gate result                           | Final                   |
|----------------------------------|-----------------|-----|---------------------------------------|-------------------------|
| <b>All gates pass</b>            | 4, 4, 4, 4, 4   | 80  | G60, G70 and G80 pass                 | 80 Advancing            |
| <b>Higher evidenced maturity</b> | 5, 4, 4, 4, 4   | 84  | All pass                              | 84 Defensible readiness |
| <b>Inventory shortfall</b>       | 5, 3, 5, 5, 5   | 92  | G60 fails; others pass                | 60 Advancing            |
| <b>Supplier exceptions only</b>  | 5, 5, 5, 5, 3   | 94  | G70 fails despite approved exceptions | 70 Advancing            |
| <b>Agility proof missing</b>     | 5, 5, 5, 2, 5   | 85  | G80 fails; others pass                | 80 Advancing            |
| <b>Multiple gates fail</b>       | 4, 3, 4, 2, 3   | 63  | G60, G70 and G80 fail                 | 60 Advancing            |
| <b>Low raw score</b>             | 1, 1, 1, 1, 1   | 20  | All gates fail                        | 20 Behind               |

Boundary check: 94 of 100 validated records fails the 95 percent threshold; 95 of 100 meets it. Both categories need a pass or evidenced absence. Rounding 94.96 percent does not produce a pass. A score of 80 remains Advancing; supplier exceptions do not replace attestations.

Evidence check: 80 percent current validated coverage supports at most P2 level 3. An evidenced absent P5 produces no total or band and no redistribution of its weight.

## Annex C Vendor roadmap request pack

Informative template implementing Clause 7. Use A–F for all critical suppliers and G for applicable AI suppliers. A response can identify evidence in an attachment or controlled access location. Distinguish present capability, customer deployment, future commitment and unknown information for every relevant answer.

### A Product scope and cryptographic footprint

**A1** Identify the legal entity, product/service, releases, deployment models, relevant subservices and customer environments covered. Identify exclusions and who controls configuration.

**A2** List cryptographic functions, algorithms/parameters, protocols/profiles, libraries/modules and exact supported releases; identify key/certificate/trust dependencies. Supply a scoped CBOM or equivalent evidence, its producer, generation method and limitations.

**A3** Distinguish available capability, defaults, enabled configuration and observed use. Identify known quantum-vulnerable uses and the customer-visible evidence that can confirm deployed posture.

### B Roadmap and milestones

**B1** Identify target approved standards and protocol profiles, parameter sets, planned release dates, pilot/production dates, dependencies and accountable milestone owners. Separate binding commitments from estimates.

**B2** Describe current limitations, interoperability dependencies, end-of-support and replacement requirements. Explain what happens if dates slip and how customers will be notified.

### C Agility and upgrade path

**C1** Describe algorithm/profile selection, credential and trust-anchor rollover, key migration, configuration interfaces, rollback controls, and legacy-path retirement. Identify changes that require replacement hardware or outages.

**C2** Describe supported hybrid or PQC-only constructions, authentication separately from key establishment, negotiation and fallback controls, and evidence of interoperability. Identify any experimental mechanisms.

### D Testing and assurance

**D1** Provide representative performance/capacity, interoperability, invalid-input, downgrade, recovery and resilience test results, with tested versions/configurations and known limitations.

**D2** Identify algorithm test results, module validation certificates/status/caveats, and independent reviews separately. Explain how these relate to the customer's actual deployment; do not imply full-system validation from algorithm tests alone.

## E Customer obligations and support

**E1** Identify configuration, trust-store, client/partner, key/certificate, testing and monitoring actions the customer must perform. Provide a responsibility matrix for the provider, customer and relevant subservice providers.

**E2** State licensing/upgrade costs, support life, lead times, service interruption expectations, contract milestones, evidence-access rights, change-notification terms and migration assistance. Describe data/key portability and feasible exit or substitution paths.

## F Disclosure and incident readiness

**F1** Describe cryptographic vulnerability disclosure, notification timing, emergency updates, key/trust compromise handling, rollback restrictions and customer communication channels.

**F2** Describe how material cryptographic changes trigger refreshed inventories, CBOMs, attestations and guidance. Identify the process for correcting inaccurate earlier claims and missed commitments.

## G AI platform cryptographic posture

**G1** Identify current signature and provenance mechanisms for training datasets, model artifacts, registries and attestations, including vulnerable RSA/ECDSA or other dependencies and affected versions.

**G2** Describe support and milestones for approved post-quantum signature profiles, such as applicable ML-DSA or SLH-DSA profiles, and how signing integrates with artifact provenance and verifier trust. Identify any signing framework/version; the framework itself is not proof of PQC support.

**G3** Describe service/workload/agent channel key establishment and authentication separately, including approved hybrid or PQC-only profiles, identity issuance, verification roots, actual deployment evidence and downgrade handling.

**G4** Provide a scoped CBOM or equivalent inventory for AI artifacts and dependencies, with updates on material change. Provide the provenance, scope, limitations, digest and generation-method evidence needed for Clause 5.4.

**G5** Describe protection of symmetric keys used for AI artifacts. Identify KEM, KDF, key-wrap/authenticated-encryption mechanism, recipient trust, bulk cipher/mode and lifecycle controls. Explain historical-key-envelope, rewrap/rekey, backup and recovery limitations.

## Authorized attestation form

Supplier legal entity: \_\_\_\_\_

Customer or intended reliance group: \_\_\_\_\_

Products/services and releases covered: \_\_\_\_\_

Deployment models and scope exclusions: \_\_\_\_\_

As-of date and evidence register: \_\_\_\_\_

We attest, within the scope and limitations recorded above and in the attached response, that the present-tense statements accurately describe the identified cryptographic functions, inventory and supported transition capabilities as of the stated date. We distinguish current implementation from roadmap commitments and identify material limitations, customer responsibilities, dependencies and unresolved risks. The attached roadmap identifies target dates and accountable owners. The response states our material-change, vulnerability and milestone-delay notification commitments. We acknowledge that the customer may rely on this attestation for governance and oversight; it does not assert that the customer's complete deployment is quantum resistant.

Limitations, qualifications and future commitments: \_\_\_\_\_

Authorized signatory name and role: \_\_\_\_\_

Basis of signing authority: \_\_\_\_\_

Signature and date: \_\_\_\_\_

The receiving organization records the responsible engineering reviewer, vendor-risk reviewer, adequacy decision, customer relevance, next review date and any exception. Blank fields in this form are response spaces, not publication placeholders.

## Annex D Governing body insert template

Informative. This structure supports Clause 8 and can be incorporated into an existing risk pack.

| Reporting item             | Content to present                                                                                                                      |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assessment identity</b> | Entity/service scope, assessment period, edition/profile, assessor type and conformance result.                                         |
| <b>Readiness</b>           | Five levels and contributions; raw/final score and band, or no-total rationale; all gate results; meaningful change since prior period. |
| <b>Visibility</b>          | System and flow numerator/denominator, unknown/stale records, reconciliation gaps and scope changes.                                    |
| <b>Exposure</b>            | Top confidentiality and verification risks, AI where applicable, historical-copy limitations and accepted residual risk.                |
| <b>Execution</b>           | Accepted production transitions, completion denominators, test coverage, failed tests, overdue milestones and legacy retirement.        |
| <b>Suppliers</b>           | Adequate current attestations versus missing/limited evidence; top exceptions, shared responsibilities and missed commitments.          |
| <b>Decisions</b>           | Resource needs, risk approvals, priorities, expiring exceptions, responsible owner and due date.                                        |

The narrative can explain a quarter in which documentation maturity rises but exposure remains unchanged. Counts of roadmaps, pilots or attestations are not counts of protected production services. A governing-body acknowledgement is recorded separately from an authorized acceptance of a specified risk.

## Annex E Authoritative reference register

Informative. Baseline verified 23 September 2026. These references support technical interpretation and applicability decisions; they do not transfer every external provision into QCI conformance. Organizations maintain their own current applicability register under Clause 2.2. QCI cadence, thresholds, scoring and conformance rules originate in this standard.

### E1 Technical standards and implementation guidance

**S1 NIST FIPS 203** — Module-Lattice-Based Key-Encapsulation Mechanism Standard. Final, 13 August 2024. Relevant to key establishment and profile selection in Clauses 4.5, 4.6 and 5.2. The publication page identifies potential errata; profile owners review applicable updates. .

**S2 NIST FIPS 204** — Module-Lattice-Based Digital Signature Standard. Final, 13 August 2024. Relevant to signatures and artifact/trust migration in Clauses 4.5–4.6. The record includes a 31 July 2026 potential-errata notice for profile-owner review. .

**S3 NIST FIPS 205** — Stateless Hash-Based Digital Signature Standard. Final, 13 August 2024. Relevant to approved hash-based signature profiles and their operational trade-offs. .

**S4 NIST SP 800-227** — Recommendations for Key-Encapsulation Mechanisms. Final, 18 September 2025. Relevant to secure KEM use and the distinction between key establishment and downstream protection in Clauses 4.5–4.6. .

**S5 NIST CSWP 39upd1** — Considerations for Achieving Crypto Agility Strategies and Practices. Original publication 19 December 2025, updated 29 June 2026. Current guidance superseding the original CSWP 39 record. Relevant to Clause 3 and Clauses 4.2, 4.7 and 9. .

**S6 NIST SP 800-208** — Recommendation for Stateful Hash-Based Signature Schemes. Final, October 2020. Relevant to controlled LMS/XMSS use and signing-state safeguards in Clause 4.6; not a general recommendation to use stateful signatures everywhere. .

**S7 IETF RFC 10024** — Post-Quantum Traditional PQ/T Hybrid Key Agreement Mechanisms for TLS 1.3. Proposed Standard, August 2026. Defines specific ECDHE/ML-KEM groups; relevant only where that TLS profile is selected. It does not make TLS authentication post-quantum. .

**S8 IETF RFC 9936** — Use of ML-KEM in the Cryptographic Message Syntax. Standards Track, March 2026. Section 2 identifies the separate KEM, KDF and wrapping components. An example integration source for Clause 4.5, not a mandatory protocol for all deployments. .

**S9 NIST SP 1800-38** — Migration to Post-Quantum Cryptography. Preliminary draft materials include cryptographic discovery and interoperability/performance testing. Relevant as informative implementation support for Clauses 4.7 and 5.4, not a final mandatory baseline. .

**S10 NIST Cryptographic Module Validation Program** — Maintained program and validation records, checked 23 September 2026. Relevant to verifying configuration-specific validation claims under Clause 4.8. Applicable obligations determine whether validation is required. .

### E2 Transition policy and jurisdictional guidance

**S11 NIST IR 8547 initial public draft** — Transition to Post-Quantum Cryptography Standards. Draft, 12 November 2024, still listed as draft at the baseline date. Its proposed transition trajectory is informative and does not replace earlier applicable policy or contract dates. .

**S12 United States Executive Order 14412** — Securing the Nation Against Advanced Cryptographic Attacks, 22 June 2026. Section 4 directs federal HVA/high-impact-system key-establishment transition by 31 December 2030 and signature transition by 31 December 2031, excluding NSS in that provision. Section 6 directs proposed FAR rulemaking; that direction is not itself a universal effective contractor clause. Applicability is assessed under Clause 2.2. .

**S13 OMB M-26-15** — Execution of the Migration to Post-Quantum Cryptography, 24 June 2026. Federal implementation policy excluding NSS; Section 3 addresses governance, risk prioritization, modernization, suppliers, automation and migration plans. The phased approach distinguishes priority migration from remaining-system migration. .

**S14 NSA CNSA Suite 2.0 and Quantum Computing FAQ** — Version 2.1, December 2024. The timetable discussion attributes the 1 January 2027 new NSS acquisition requirement to CNSSP 15 and describes end-2030 phase-out and end-2031 use requirements, with qualifications. NSS applicability, validation life, waivers and specific profiles require separate determination. .

**S15 NSA CNSA 2.0 advisory** — Commercial National Security Algorithm Suite 2.0, September 2022 version 1.0, official copy hosted May 2025. Source for suite context and category-specific planning, including early software/firmware signing. Read with later policy/FAQ and applicable product requirements; its dates are not a global enterprise deadline. .

**S16 UK NCSC** — Timelines for migration to post-quantum cryptography, March 2025 guidance. Milestones: discovery/initial plan by 2028; priority migration by 2031; completion by 2035. Scope-specific guidance, not a universal legal mandate. .

**S17 European Commission and NIS Cooperation Group** — Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, June 2025, with supporting FAQ information available in 2026. Recommends Member State transition starts by end-2026 and high-risk use-case transition by end-2030. National implementation determines specific obligations. .

**S18 UK NCSC** — Next steps in preparing for post-quantum cryptography, version 2.0, August 2024. Relevant sections discuss parameter choices, stateful signatures, hybrid complexity and transition to PQC-only where appropriate. This guidance supports a reasoned hybrid decision, not a universal preference. .

## E3 AI and illustrative inventory formats

**S19 NSA CISA FBI and allied agencies** — AI Data Security Best Practices for Securing Data Used to Train and Operate AI Systems. Cybersecurity Information Sheet, 22 May 2025, U/OO/157249-25. Its digital-signature recommendation concerns authentication of training and related datasets. QCI extends cryptographic governance to other in-scope AI dependencies without attributing every extension to the CSI. .

**S20 OWASP CycloneDX 1.6** — Industry specification, 2024. An illustrative CBOM interchange format. QCI does not require this format; an implementation records the actual schema/version and validates its mapping to required QASI information. .

**S21 OpenSSF Model Signing specification** — OMS version 1 family, industry specification. An illustrative model-signing format, not itself a post-quantum algorithm or required QCI dependency. Implementations record the exact specification release/commit and cryptographic profile rather than assuming format support establishes quantum resistance. .

Candidate algorithms and draft profiles are tracked separately from approved production mechanisms. At this baseline, NIST lists FIPS 206 as in development and HQC as selected for standardization. Future approval is not assumed. .

## Annex F Revision history and change log

Informative. This log describes text changes between editions. It does not assert that an adopting organization has implemented the requirements or that an independent field calibration has been completed.

### F1 Edition history

| Version | Date               | Revision                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.3     | September 23, 2026 | Issued edition. Adds determinate conformance rules and stable QCI requirement identifiers; a fixed Core scoring profile with cumulative integer rubrics, the 95 percent coverage gate for both critical systems and critical flows, and the supplier gate without an exception route; approved cryptographic profiles, key and trust lifecycle, migration testing and acceptance, and evidence and assurance requirements; discovery provenance and vendor CBOM equivalence; separate human and workload identity records; the obligations and applicability register; the current authoritative reference register; and the Annex G cryptographic domain taxonomy. Incorporates the dispositions of the review of 22 to 23 September 2026. |
| 2.2     | June 8, 2026       | Prior issued edition. Added AI cryptographic scope and the citation register.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2.1     | February 2, 2026   | Established the core governance, inventory, scoring, supplier and board components.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### F2 Substantive changes affecting adoption and scores

Pillar weights and numeric caps are unchanged. The Core profile now sets a common 95 percent inventory threshold for both critical systems and flows. The vendor gate no longer accepts an operating exception instead of adequate supplier evidence. The upper band begins at 81, so a score held at 80 by the agility cap is not described as Defensible readiness. Pillar-specific criteria, cumulative integer levels, no-total treatment of an absent pillar, and current-evidence rules replace discretionary interpretations.

Additional QCI policy choices are a maximum 90-day validation interval with documented unchanged-configuration review permitted; annual and material-change incident exercises; annual and material-change supplier attestation refresh; a maximum initial supplier response period of 60 days; and independent review for level 5 within 12 months and after invalidating changes. These are requirements of this edition, not externally mandated universal intervals.

The duplicated component specifications were consolidated into normative clauses and informative implementation templates. The QRAF domain map remains in 9.7, and the thirteen-domain taxonomy remains in Annex G. The misleading six-component/five-level counts and

unconditional source-traceability claims were removed. Unsupported predictions and obsolete blanket sequencing were replaced with attributable technical context and risk-based decisions.

### F3 Publication and adoption record

Version 2.3 was published and became effective on September 23, 2026. The adoption and claim rules in Clause 1.3 govern transition from Version 2.2: an adopting organization records its adoption date and assessment basis, completes the changed records within 90 days, and does not claim Version 2.3 conformance until all applicable requirements are met. Earlier scores need restatement or a comparability break; retained weights alone do not preserve comparability.

## Annex G Cryptographic domain taxonomy

Informative. The taxonomy organizes migration dependencies; it is not a disjoint partition or a universal execution order. Clause 5.2 requires classification using these identifiers or a mapped local taxonomy. Public-key dependencies can occur across the technology domains; some deployments are already post-quantum or use appropriate symmetric mechanisms. Foundation layers describe governance activities rather than algorithms to replace.

### G1 Foundation layers

| ID and domain                          | Purpose and mapping                                                                                                                                                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1 Discovery and inventory</b>       | Identify cryptographic uses and their system, flow and product relationships. QASI and discovery provenance: Clause 5; P2; QRAF D2. CBOMs support evidence rather than replace validation. |
| <b>2 Crypto agility and governance</b> | Ownership, profiles, obligations, risk, resources, roadmap, exceptions and reporting. Clauses 1–4, 6 and 8; P1/P4; D1/D4/D8.                                                               |

### G2 Technology domains

| ID and domain                             | Coverage and principal mappings                                                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3 Data in transit</b>                  | TLS endpoints, gateways, CDNs, load balancers and service mesh. Record key establishment and authentication separately. QASI uses/flows; P3/P4; D3/D4. AI channel protection where applicable. |
| <b>4 VPN IPsec SSH and remote access</b>  | Tunnels, administrative access and machine connections, including authentication credentials and negotiation. Uses/flows/trust; P4; D4/D6. AI channels where applicable.                       |
| <b>5 PKI certificates and signing</b>     | Roots, issuers, trust stores, code/firmware/document signing and timestamps; verifier and archival dependencies. Trust records; P4; D6. AI signing/provenance.                                 |
| <b>6 Key management and HSMs</b>          | HSM/KMS, establishment, wrapping, custody, recovery, rotation and lifecycle controls. Trust/key records; P4; D4/D6. AI key-protection construction.                                            |
| <b>7 Data at rest storage and backups</b> | Databases, file systems, replicas, archives and historical key envelopes. Separate bulk protection from key protection. Horizons/keys/risks; P3; D3. AI horizons and keys.                     |

| ID and domain                                    | Coverage and principal mappings                                                                                                                                                                                     |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>8 Application cryptographic libraries</b>     | Libraries, frameworks, runtimes and hard-coded dependencies in code and products. Exact deployed versions and upgrade paths. Uses/profiles; P4; D4. Cross-cutting AI implementation dependencies.                   |
| <b>9 Human and workload identity</b>             | SSO, federation, tokens, passkeys, smart cards, service/workload/agent credentials, issuance and verification roots. Identity/trust records; P4; D6. Agent identity and channel authentication.                     |
| <b>10 Messaging and collaboration</b>            | Secure email, messaging, collaboration and end-to-end channels; confidentiality and sender authentication. Flows/suppliers/horizons; P3/P5; D3/D5. HNDL applies where vulnerable key protection is used.            |
| <b>11 Devices firmware OT and hardware trust</b> | Embedded/constrained systems, secure boot, TPMs, update chains and industrial systems. Long-lead replacement and safe recovery. Agility/trust/roadmap; P4; D4/D7.                                                   |
| <b>12 Third-party SaaS and cloud</b>             | Provider-operated cryptography, managed services and material subservices. Customer/provider responsibilities and deployed-state evidence. Suppliers/uses; P5; D5. All applicable AI fields and supplier questions. |
| <b>13 Sector-specific protocols</b>              | Relevant payments, transaction signing, digital assets, custody and industry-specific protocols. Applicable standards and lifecycle constraints; uses/trust/suppliers; P3/P5; D5/D6.                                |

### G3 Applying the taxonomy

Use multiple tags when a service spans domains. Link each material domain dependency to an owner, roadmap decision, milestone and acceptance evidence. Domain 12 usually overlaps other domains because a supplier operates technology in them; domain 8 similarly crosses applications and services.

Sequence by exposure, lead time and dependencies. Confidentiality work can begin alongside long-lived signature and hardware replacement work. A decision to wait for an ecosystem capability can be valid only within the organization's obligations and risk appetite, with the owner, rationale, interim treatment and review date recorded under Part A. A 2035 planning target is not permission to miss an earlier applicable deadline.

For governing-body reporting, related dependencies can be grouped into communications, trust and identity, keys and hardware, application and sector services, and suppliers. Engineering retains the detailed linked inventory so the summary does not hide an unprotected hop or trust dependency.

*Publisher's note. Independent assessment under QCI-1.2-03 is available from the Quantum Core Institute at [quantumcoreinstitute.com/independent-assessment](https://quantumcoreinstitute.com/independent-assessment). Use of this standard is not QCI certification.*