QUANTUM CORE INSTITUTE

QCI Practitioner Handbook

Implementing QCI-QS1 without learning everything the hard way

Field	Value
Document ID	QCI-QS1-H
Version	V2.3 – September 23, 2026
Applies to	QCI-QS1 Quantum Readiness and Post-Quantum Cryptography Governance Standard, Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers, so that later renumbering of the standard does not invalidate this Handbook.
Status	Informative companion to QCI-QS1. Nothing in this Handbook creates, modifies, or interprets a requirement. Where this Handbook and the standard differ, the standard governs.
Supersedes	QCI-QS1-H V2.2 (June 8, 2026). The QCI-QS1-A Implementation Guide v2.1 remains retired; archived copies remain available for citation continuity.
License	Free. No form wall. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

Contents

1 Read this first

QCI-QS1 defines what a quantum readiness program must do. This Handbook shows how to do it, why each requirement exists, and how programs fail against it. The standard is dry on purpose. Auditability requires language an assessor can test, and “keep it honest” is not a testable provision. The judgment, the worked examples, and the war stories all live here instead.

Read the two documents differently. Cite the standard. Argue with the Handbook. When they appear to disagree, the standard wins, and we would like to hear about it. From this edition the Handbook cites the standard by requirement identifier (QCI-4.1-01, QCI-6.3-01 and so on) rather than by clause number, because identifiers are stable across editions and clause numbers were not.

One rule precedes every worksheet in this book. Assign your executive sponsor and your Quantum Risk Owner before you open anything else. Without named owners, every tool that follows becomes a document-filing exercise rather than a governance program. QCI-4.1-01 makes ownership a requirement. Experience makes it the first one.

A note on scope. The standard governs cryptographic risk, including cryptographic risk arising from artificial intelligence (AI) systems. It does not govern model behavior or AI risk generally, and neither does this Handbook. Where you see “where AI systems are in scope,” that condition

is doing real work. An organization with no AI systems in scope records AI applicability as none and moves on (QCI-5.2-03).

A note on this edition. Version 2.3 of the standard fixed the scoring profile, changed the supplier gate so that an exception no longer substitutes for an attestation, moved the top band to 81, and replaced the five-component agility proof with a test-and-acceptance requirement. Chapters 3, 4, 7 and 8 changed accordingly; chapters 13 and 14 are new. Appendix C lists the changes.

2 The 90-day establishment sequence

This sequence takes a new program from nothing to its first Q-Risk Score (Quantum Risk Score) snapshot and governing-body insert in about 90 days. It is deliberately achievable. Perfect is not the goal. Owned and measured is. Clause 9.1 of the standard describes the same sequence and says what this Handbook repeats: it is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Weeks 1 to 2	Establish	Assign the executive sponsor and Quantum Risk Owner. Declare the assessment boundary and the criticality criteria (QCI-1.1-01, 1.1-02): which systems and which critical data flows are in. Seed the obligations register (QCI-2.2-01). Identify the steering function members. Note that coverage is fixed by the standard at 95 percent of validated critical systems and flows (gate G60); there is no threshold to set.	Approved boundary statement. Named roles. Obligations register started.
Weeks 3 to 6	Inventory	Build linked QASI (Quantum Attack Surface and Cryptographic Dependency Inventory) records for the highest-priority systems and the critical flows between them, starting with identity and public key infrastructure (PKI) and regulated data. Validate every record with the named system owner and a technical reviewer, not just with engineering (QCI-5.1-02). Split human and workload identity (QCI-5.2-02). Capture the linked AI records where they apply.	Validated QASI records for highest-priority systems and flows. Coverage computed for each, numerator and denominator published (QCI-5.1-03).
Weeks 7 to 9	Analyze	Set confidentiality and verification horizons per record, as dates. Identify harvest now, decrypt later (HNDL) exposure: which systems hold data that must stay confidential, or signatures that must stay verifiable, beyond the migration window. Raise the exposure flags of QCI-5.3-01 and record treatment status separately (QCI-5.3-02). Issue Annex C requests to the top five critical suppliers with a 60-day deadline (QCI-7.2-04).	Exposure flag count. Top-10 remediation list. Supplier requests issued with dates.

Timeframe	Phase	What to accomplish	Output
Week 10	Score	Produce the first Q-Risk Score snapshot with evidence links, labelled self-assessment (QCI-1.2-03), with every gate result stated. Be honest. A low first score is a baseline, not a failure. The score only moves when the program moves.	Q-Risk Score snapshot with assessment type and conformance status. Pillar and gate gaps identified.
Weeks 11 to 12	Plan and report	Draft the post-quantum cryptography (PQC) migration roadmap with milestone types per QCI-4.2-02. Open the exception register (QCI-4.3-02). Deliver the first governing-body insert (Annex D, QCI-8.1-01).	Roadmap draft. Exception register open. Insert delivered.

COMMON MISTAKE
Organizations spend weeks 1 to 4 trying to inventory every system rather than starting with the highest-risk ones. A complete QASI for your top 20 critical systems is worth more than a partial QASI for everything you own. Coverage breadth matters. Coverage depth on the right systems matters more. But read the denominator rule: a critical item enters the population when it is identified, even before its record is complete (QCI-5.1-01), so depth first does not mean pretending the rest is not there.

COMMON MISTAKE
Treating week 10 as a deadline for a good score. The first score exists to be a baseline. Programs that polish the number before producing it spend the next year defending a fiction, and the gates in QCI-6.3-01 exist precisely to make that expensive.

3 Scoring in practice

The computation is QCI-6.1-02 and the worksheet is Annex B. Score each pillar 0 to 5 against the cumulative rubric for that pillar, then compute 4×L1 + 4×L2 + 4×L3 + 5×L4 + 3×L5 and apply the gates. The arithmetic takes a minute. The calibration is where programs go wrong, so this chapter is about calibration.

3.1 What the levels actually look like

The scale runs 0 Unaware, 1 Aware, 2 Defined, 3 Implementing, 4 Managed, 5 Assured. The rubrics in Clauses 6.6 to 6.10 are cumulative: a level is awarded only when every criterion at that level and every lower level is supported, and a failed criterion cannot be averaged away (QCI-6.1-01). The boundary that matters most is 2 to 3, because it is the line between paper and motion. Calibration guidance per pillar:

- **P1 Governance.** Level 2: a policy exists and the governing body heard a presentation once. Level 3: named owners, quarterly cadence running, escalation thresholds defined under QCI-4.3-01 and used at least once. The test is cadence, not documents.
- **P2 Visibility.** Level 2: an inventory exists for some systems. Level 3: the two coverage metrics exist with published numerators and denominators, every record has a named

owner and a technical reviewer, and records carry evidence references that meet QCI-5.4-01. An inventory nobody validated is level 2 wearing level 3 clothing, and a scan-reach figure is not a coverage metric.

- **P3 Exposure management.** Level 2: classifications exist. Level 3: confidentiality and verification horizons are recorded as dates per critical system and flow, the exposure flags are raised and reviewed, and treatment status is recorded separately. The horizon question has an answer per critical record, not per policy.
- **P4 Migration and agility.** Level 2: a roadmap document. Level 3: migration work appears in engineering backlogs with tickets, an approved cryptographic profile exists (QCI-4.5-01), and at least one trust pathway has a test plan under QCI-4.7-01 in progress. Roadmaps do not migrate anything. Tickets do. Completion means accepted production configuration with legacy paths retired (QCI-6.2-02), not a vendor release.
- **P5 Third party.** Level 2: supplier letters drafted. Level 3: requests issued to all critical suppliers with the 60-day deadline, responses tracked against the adequacy criteria of QCI-7.2-03, the exception register live. A supplier who has not answered is an exception, not a pending item, and no exception passes gate G70.

Level 5 in any pillar requires independent review of that pillar within the previous twelve months (QCI-4.8-02). Self-assessed level 5 is not a level the standard recognizes.

3.2 Self-assessed versus independently assessed

These are different claims, and the standard treats them that way. QCI-1.2-03 requires any conformance claim, and by QCI-1.2-04 any reported score, to identify the assessor and the assessment type, distinguishing self-assessment from independent assessment, and to state the boundary, the period and where the conformance record can be found. An independent assessor, in the standard's definition, did not design, implement or operate the controls being assessed and has no responsibility for the outcome. Record the assessment type on the worksheet every quarter, including the quarters nobody external will see. The habit is what prevents the mistake.

Use of the standard is not QCI certification, and QCI-1.2-03 says so. An organization may say it has been assessed against QCI-QS1, by whom, and with what result. It may not say it is QCI-certified.

> **WHY THE REQUIREMENT EXISTS**
> A self-assessed 74 and an independently assessed 74 are not the same number, and a counterparty relying on the wrong one is relying on something that was never claimed. QCI-1.2-03 turns an honesty norm into a conformance requirement, which protects the institutions that were already honest. QCI-1.2-04 adds the second half: a score is never a conformance statement, and the two are reported side by side.

> **WHAT THE ASSESSOR WILL ASK**
> Show me the prior four quarterly worksheets. The fastest credibility test available is whether the assessment-type box was filled in before anyone asked for it, and whether conformance status sits beside the score rather than inside it.

4 The crypto agility test

No score above 80 without a demonstrated crypto-agility test, and gate G80 in QCI-6.3-01 defines what demonstrated means: at least one critical trust pathway has passed a representative end-to-end test under QCI-4.7 within the previous twelve months and after any invalidating material change, with the pathway and the limits of the test disclosed. This chapter is about running that test without fooling yourself.

QCI-4.7-01 lists eleven things the test plan must cover: interoperability end to end, actual algorithm negotiation, authentication and trust validation, invalid inputs, downgrade and fallback, message and certificate size, resource exhaustion, capacity and latency, backup and restore, failover, and authorized rollback. A category you omit needs a written technical reason. The environment must represent the pathway you are claiming for, and the relationship to production traffic is stated, not assumed.

QCI-4.7-02 is the half that programs skip. Before a migration is accepted, engineering and the accountable service owner sign off on the results, the disposition of every failure, monitoring, support readiness, recovery procedures, residual exceptions and an observation period. A rollback that puts vulnerable protection back into production is an exception with an expiry, not an undo. And completion, the thing P4 counts, means effective production configuration with legacy paths removed and old keys disposed of. A pilot is not completion. A vendor release is not completion.

> **COMMON MISTAKE**
> The lab-test trap. A proof on a non-production system with no load characteristics satisfies nothing unless the system is genuinely not load-sensitive. Assessors will ask for the load profile used and compare it to actual traffic. Have that comparison ready before they ask. And read the date: a test older than twelve months has lapsed for G80, however unchanged the system.

One successful pathway lifts the gate. It does not make the estate agile. P4 levels 4 and 5 under QCI-6.9-01 require representative tests across each materially distinct protocol, trust, key-management and deployment pattern, with an equivalence analysis where tests are shared. The standard keeps the two apart on purpose, and Clause 9.2 of the standard says why: so that one demonstration is not mistaken for enterprise readiness.

Readers of the previous edition will remember five components. They are all still there, inside the eleven categories and the acceptance rule: change capability is categories 1 to 3, the operational procedure is the acceptance record, executed rollback is category 11, load performance is categories 7 and 8, and trust chain validation is category 3 with restore and failover behind it. QCI-T2, the test and acceptance protocol, carries the crosswalk and a plan template.

If you cannot complete the test yet, document the gap, apply compensating controls where feasible, and set a remediation milestone. The cap at 80 stays in effect until the test exists, and that is the system working as designed.

5 QRAF: governance that survives budget season

QRAF (the Quantum Risk Governance and Assessment Framework) exists to prevent a predictable failure. Quantum risk gets treated as future cryptography work until it becomes present operational exposure, and the transition between those states never announces itself. The framework forces three things early: assigned ownership, measured exposure, and progress proven with evidence rather than optimism.

The governance principle underneath every role in QCI-4.1-01 is simple. Unassigned risk does not get managed. The governing body owns oversight and risk appetite. The executive sponsor, usually the Chief Information Security Officer (CISO) or Chief Information Officer (CIO) and sometimes the Chief Risk Officer (CRO), owns accountability. The Quantum Risk Owner runs the program day to day. Procurement owns supplier evidence, engineering owns execution, legal owns horizons and disclosure, incident response owns the playbook of QCI-4.4-01, and assurance owns the evidence rule. A cross-functional steering function resolves the dependencies between them. If any of those sentences has no name attached in your organization, you have found this quarter's first deliverable.

5.1 The eight domains, and how each one fails

The standard lists the QRAF domains in Clause 9.7 and keeps a straight face doing it. Here is the same table with the failure modes restored, because recognizing the failure is how you diagnose the domain.

Domain	What it measures	How it sounds when it is failing
D1	Governance and accountability	"It's IT's problem."
D2	Crypto asset visibility	"We do not know what we use."
D3	Data longevity exposure	"We assumed short shelf life."
D4	PQC migration readiness	"We are waiting on vendors."
D5	Third-party exposure	"Outsourced risk is still ours, apparently."
D6	Identity and trust dependencies	"Certificate sprawl."
D7	Incident and resilience	"No playbook." For AI systems: "The model registry trusts a signature that quantum capability can forge."
D8	Assurance and auditability	"Slides instead of proof."

The domains organize review; they carry no second weighted score (Clause 9.7). The pillars determine the score. Every assessed claim, in either, links to attributable, dated evidence (QCI-4.8-01). The workflow repeats quarterly: initiate, inventory, analyze, score, plan, execute, assure, report. Boring on purpose. Programs survive on cadence, not enthusiasm.

> **WHY THE REQUIREMENT EXISTS**
> Quarterly cadence is in the standard (QCI-4.1-02) because annual quantum reviews die in scheduling. A quarterly rhythm matches the board pack that already exists, which means the program borrows a heartbeat instead of needing its own.

6 QASI: building an inventory that is not theater

The QASI answers the question the governing body will eventually ask: are we exposed, and can you prove the answer either way. It maps cryptography use, trust dependencies, critical flows and horizons to systems and suppliers, as linked records rather than one wide row (QCI-5.2-01). Three rules of construction: inventory material systems and flows first, prioritize coverage of the systems that matter over exhaustive precision, and validate every record with its named owner and a technical reviewer.

6.1 Worked examples

Four completed records follow, condensed to the fields that carry the lesson. Field values are representative. Use them to calibrate what a well-completed record looks like, not as templates to copy. Flags are named in the words of QCI-5.3-01.

Example 1: Payment authorization API

Field	Entry
Criticality / classification	High / Regulated
Confidentiality horizon	10 years from transaction date (PCI DSS and contract obligation). Verification horizon: 7 years for signed authorizations.
Cryptographic uses	TLS key establishment: ECDH P-256. TLS authentication: RSA-2048 certificate. Transaction signing: ECDSA P-256. Storage: AES-256-GCM; data key wrapped under RSA-2048 in cloud KMS. Recorded as four linked use records, not one cell.
Key management	Cloud KMS with HSM backing for signing keys; key envelope history retained
PQC support status	Roadmap. Supplier committed to a hybrid key-establishment profile by Q3 2027; attestation on the Annex C form received, dated
Crypto agility status	Partial. Configuration change possible; QCI-4.7 test plan drafted, not executed under load
Exposure flags / treatment	Vulnerable protection of long-lived confidentiality; critical supplier evidence gap on the KMS subservice. Treatment: approved plan
Target remediation	December 2027, hybrid key establishment; KEM-based data-key protection scheme (ML-KEM, KDF, wrap) per QCI-4.5-04 to follow

Example 2: Internal identity provider (SSO)

Field	Entry
Criticality / classification	High (single point of authentication failure) / Confidential. Human identity record under QCI-5.2-02; the service accounts it issues are separate workload identity records

Field	Entry
Horizons	Confidentiality: active credentials 1 year. Verification: audit logs 7 years; signed assertions 90 days
Cryptographic uses	SAML signing: RSA-2048. OIDC signing: ECDSA P-256. TLS 1.3 with X25519 key establishment
Trust dependencies	Public CA external. Internal root CA for internal services; migration path not yet recorded (QCI-4.6-02)
PQC support status	None. Supplier has no published roadmap; request issued, 60-day deadline set
Crypto agility status	None. Signing algorithm hard-coded in federation config
Exposure flags / treatment	Signature and trust dependency with long verification horizon; missing ownership (47 service certificates with unclear owners); rigid component. Treatment: untreated
Target remediation	Engineering assessment required before a date can be committed; recorded as unknown and escalated under QCI-5.3-02

Example 3: Substation gateway (operational technology)

Field	Entry
Criticality / classification	High (physical consequence) / Internal
Horizons	Confidentiality: telemetry 3 years. Verification: device trust must hold for the 18-year fleet life, recorded as a date
Cryptographic uses	Firmware signing: ECDSA P-256. Management plane: TLS 1.2. Field bus: legacy protocol with no authentication, recorded as a critical flow with no protection at that hop
Key management	Supplier-held signing keys. Device certificates not rotatable without site visit
PQC support status	None. Supplier roadmap requested, response pending, deadline in 41 days
Crypto agility status	None. Algorithm fixed in device firmware
Exposure flags / treatment	Low for confidentiality. Authenticity exposure is the finding: signature and trust dependency with long verification horizon; critical supplier evidence gap; rigid component. Treatment: mitigation verified (network segmentation, verified by architecture review, documented as a risk decision with an owner and review date). The flags stay raised.
Target remediation	Tied to fleet refresh. Long-lead decision recorded under QCI-4.2-02; procurement language for PQC agility added to the next tender (QCI-7.1-02)

Example 4: Model registry (AI system, linked records per QCI-5.2-03)

Field	Entry
Criticality / classification	High / Confidential
AI artifact class	Model weights and registry signatures
Horizons	Confidentiality: 7 years. Provenance and verification: 10 years
Model signing scheme	ECDSA P-256
Workload and agent identity	Registry service credential: X.509, RSA-2048, issued by the internal CA
Inter-agent channel protection	Classical TLS; key establishment ECDH P-256
AI artifact key protection	Data key wrapped under RSA-2048; full scheme recorded per QCI-4.5-04
Exposure flags / treatment	Vulnerable protection of long-lived confidentiality and long verification horizon on quantum-vulnerable signing and wrapping; artifact class identified. Treatment: untreated, no approved plan
Target remediation	Establish artifact integrity and provenance first (QCI-4.6-02), then re-sign critical artifacts with ML-DSA (Module-Lattice-Based Digital Signature Algorithm) and move key protection to a KEM-based scheme using ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), a KDF and symmetric wrap, per Clause 9.3

What these examples show. None of the four records is clean, and that is the point. A well-completed QASI record does not mean the problems are solved. It means the exposure is visible, owned, and tracked. The SSO example carries multiple flags and no committed date, which is a significant finding, and it is still infinitely more useful than a blank record or a record that claims PQC-ready without evidence. The substation example shows the other discipline: where cryptography is absent and segmentation is the control, write that down as a decision with an owner, verify it, and leave the flag raised, because QCI-5.3-01 says a plan does not clear a flag and QCI-5.3-02 says segmentation is not assumed to remove HNDL risk. An undocumented compensating control is just an assumption with seniority.

> **COMMON MISTAKE**
> Letting the scanner write the inventory. Discovery tooling finds algorithms in code. It does not find the certificate estate, the service accounts, or the supplier-held keys, and those are routinely where the exposure sits. The scan is an input to the QASI. It is not the QASI. QCI-5.4-01 says what a scan finding must carry before it is evidence, and chapter 13 says how to read one.

7 Q-Risk Score: why the gates exist

The score is a comparable readiness snapshot, not a prophecy. It answers two questions: are we getting meaningfully safer, and how do we compare to peers using the same rubric. The bands in QCI-6.5-01 run from Exposed (0 to 19) through Behind, Mobilizing and Advancing to

Defensible readiness, which begins at 81, and the labels are calibrated to be reportable to a governing body without translation. A score of exactly 80 is Advancing.

Every scoring system invites gaming, and a self-assessed scoring system sends the invitation embossed. The gates in QCI-6.3-01 are the response: no score above 60 without 95 percent validated coverage of both critical systems and critical flows, none above 70 without a current adequate attestation from every critical supplier, and none above 80 without a representative end-to-end agility test under QCI-4.7 within the last twelve months. The gates are not pessimism. They are the reason a QCI-QS1 score from one institution can be compared with a score from another and mean something. And the profile is fixed: organization-specific thresholds or weights may be reported only as separately named supplemental metrics, never as the Core score (QCI-6.3-02).

> **WHY THE REQUIREMENT EXISTS**
> Without gates, the score inflates to wherever the most optimistic stakeholder needs it to be, and a comparable metric degrades into a mood ring. The gates anchor each scoring tier to a class of evidence that cannot be produced by enthusiasm. Version 2.3 closed the last soft spot: a registered exception used to pass G70, and it no longer does.

The temptations, so you can recognize them in the room. Scoring P2 on the inventory you intend to build. Scoring P5 on the supplier letters you intend to send. Averaging a strong pillar against a hollow one and reporting the average with a straight face; QCI-6.1-01 forbids it in words: no averaging, no fractional levels. The worksheet in Annex B resists all three if you fill in the evidence column honestly, which is why the evidence column is there.

One page, quarterly, is the whole reporting format: score and band with assessment type, gate results, movement since last quarter, the top three risk reducers delivered, the top three exposures still open, and the supplier exceptions list. If the scorecard needs a second page, something on the first page is hiding.

7.1 The five components in one breath

Component	What it is	Output	Watch out for
QRAF	Governance and assessment framework	Owners, cadence, evidence rules	Feels heavy before the first quick win lands
QASI	Inventory of crypto dependencies	Linked records with evidence, for systems and flows	Requires coordination across teams
Q-Risk Score	Comparable snapshot	0 to 100 plus movement, with gates and assessment type	The temptation to game it (see gates)
Vendor Pack	Third-party request and attestation (Annex C)	Responses plus officer-signed statement	Some suppliers stall (see chapter 8), and the score waits with them
Governing-body insert	Quarterly oversight summary (Annex D)	One governance page	Demands disciplined evidence collection

8 The vendor pack: getting answers from suppliers who would rather not

Most institutions do not control their own cryptography. Their suppliers do. The vendor pack exists to convert that dependency from an assumption into a documented, signed, and escalatable position. QCI-7.2-01 defines the minimum and Annex C operationalizes it: sections A to F covering product scope and cryptographic footprint, roadmap and milestones, agility and upgrade path, testing and assurance, customer obligations and support, and disclosure and incident readiness, plus G1 to G5 for AI suppliers, and the authorized attestation form of QCI-7.2-02 signable by an officer. The attestation is intentionally uncomfortable. Comfort is what the current state of supplier PQC communication has produced, and you have seen the current state.

Two numbers govern the process. The request sets a deadline no later than 60 days after issue (QCI-7.2-04), and the attestation is refreshed at least annually and on material cryptographic change (QCI-7.2-03). A response older than that, or superseded by a release, does not pass G70.

8.1 Reading the responses

Four options exist for every response, and each is a real strategy with a real cost:

Option	Pros	Cons
Accept the roadmap	Keeps momentum, leverages supplier capability	Roadmaps slip without consequence unless something makes slippage expensive, and a roadmap is not deployed protection (QCI-7.1-02)
Contractualize milestones	Creates enforceability and an audit trail	Adds cost and procurement friction
Dual-source or exit plan	Reduces concentration risk	Operational complexity and migration effort
Compensating controls	Buys time when the supplier lags	Temporary controls have a documented tendency to become permanent

Non-answers are answers. A supplier who cannot say which algorithms their product uses has told you the inventory does not exist. A supplier who will answer questions but not sign the attestation has told you where their counsel thinks the truth gets risky. Both go on the exception register under QCI-7.3-01 and QCI-4.3-02 with a remediation plan, compensating controls, and an exit strategy where feasible, and the top exceptions go in front of the governing body (QCI-7.3-01). Suppliers behave differently once they learn their name recurs in a board document.

An exception, however well managed, does not pass gate G70. The score stays at 70 until the attestation exists; the register is where the supplier’s name recurs until it does. That is a change from the previous edition, and it is the right one: the exposure sits at the supplier whether or not the customer has written it down neatly.

> **WHAT THE ASSESSOR WILL ASK**
> Show me the exception register, not the success stories. The register is where third-party oversight is either real or theatrical, and an empty register at a large institution is its own finding.

The question structure, sections A to G and the attestation form are published in Annex C. QCI-INT-2, the supplier response scoring rubric, is how QCI engagement teams turn a response into an adequacy determination consistently; chapter 13.4 gives the short version.

9 Briefing the governing body

Quantum risk is not a science project, and the governing-body insert should never read like one. It is a timeline and dependency problem. If data must stay confidential for years, then cryptography decisions today matter. If suppliers control crypto upgrades, then third-party controls are not optional. If the organization cannot inventory its cryptographic dependencies, it cannot credibly claim readiness. Those three sentences are the entire executive theory of the case, and they fit on one slide nobody will need.

The governing body is not being asked to pick algorithms. It is being asked to require five things every quarter: ownership (a named accountable executive), visibility (validated coverage for systems and flows, and top exposures), progress (production migration completed, distinguished from supplier or pilot capability), suppliers (attestations collected plus the exceptions list), and assurance (test coverage and its limits). Annex D is the template, QCI-8.1-01 lists the mandatory elements, and QCI-8.2-01 sets the posture: evidence-based reporting rather than narrative, third-party readiness treated as a governance topic rather than a procurement topic, and an acknowledgement of a report never recorded as acceptance of a risk.

On third parties, give the governing body the sentence that survives the meeting: third-party risk does not transfer, it compounds. Any supplier that cannot provide a credible roadmap and attestation becomes a managed exception with an exit plan or compensating controls, and holds the score at 70 while it does.

Closing perspective, suitable for the end of the insert and the end of this chapter. Quantum advantage will arrive unevenly. Quantum risk arrives asymmetrically. The organizations that come through well are the ones that inventory early, govern loudly, and migrate before the calendar forces their hand.

> **COMMON MISTAKE**
> Bringing the governing body a threat briefing instead of a governance ask. Boards process requests for decisions. A quarter of quantum education with no decision attached teaches the board that this topic never needs one. QCI-8.2-01 requires every decision to carry an owner, a rationale, a due date and a follow-up, which is the cure.

10 How readiness programs fail

The algorithms were finished in 2024. Every failure we observe since is organizational, and the patterns repeat with enough fidelity to deserve names. Each failure mode below pairs with the

provision that exists to prevent it. The patterns are composites drawn from public post-mortems and published assessments.

Inventory theater. A scan-generated algorithm list stands in for a cryptographic inventory, omitting certificates, supplier-held keys, and operational credentials, which is precisely where the exposure sits. The program reports visibility it does not have. Corrective: the QASI record groups of QCI-5.2-01 with named owners and evidence references meeting QCI-5.4-01, and gate G60, which makes unverified coverage unable to pay rent.

Orphaned ownership. Quantum migration files into the CISO's backlog with no executive owner and no governing-body reporting line, and dies at the first budget cycle. Corrective: QCI-4.1-01, which is three sentences long and eliminates the failure mode by itself when actually applied.

Calendar denial. The program schedules against an optimistic estimate of when quantum capability arrives, instead of against migration duration. The relevant arithmetic is data lifetime plus migration time versus time to capability, and for long-lived data that inequality can fail today regardless of when the capability lands. Corrective: the confidentiality and verification horizons and exposure flags of QCI-5.2-01 and 5.3-01, which force the arithmetic per system, and QCI-4.2-02, which forbids a sequence that postpones long-lead work.

Vendor faith. The institution assumes its core providers will handle the migration, which they will, on their schedule. Without contractual roadmaps and attestations, the institution's timeline is a hostage of the supplier's product cycle. Corrective: Clause 7 end to end, especially the exception register and its governing-body visibility, and gate G70, which now refuses to look away.

One-shot migration. The replacement algorithm gets hard-coded exactly the way the current one was, guaranteeing the next transition costs as much as this one. Crypto agility was the lesson, not the destination algorithm. Corrective: the agility status field, the approved profile of QCI-4.5-01 with its review date, the tested transition under QCI-4.7, and gate G80.

The double migration. Institutions running identity modernization (passkeys, new identity and access management (IAM) platforms, credential re-issuance programs) separately from PQC planning are scheduled to issue the same credentials twice and reconcile the inventories never. Version 2.3 gives this a handle: QCI-5.2-02 requires human and workload identity to be inventoried as distinct records, which is the shared inventory the two programs need. The cheapest available decision is still one re-issuance plan and one named owner for the seam between the programs, made before the identity program ships. QCI-QS1-C5 works the problem in full.

11 What auditors like to see

Assessors and auditors converge on the same expectations, and meeting them is cheaper before the engagement than during it.

- Evidence links from every claim to a ticket, report, export, or configuration artifact, with producer, reviewer and integrity controls. The unit of credibility is the link, and QCI-4.8-01 makes it a requirement rather than a courtesy.

- An artifact, not a screenshot of an artifact. A retrievable, version-controlled source beats an image of one pasted into a deck. Screenshots age. Sources answer follow-up questions. Clause 9.4 of the standard says the same thing more politely.
- Defined scope boundaries with rationale. “We excluded the test environment because” is a sentence auditors respect (QCI-1.1-02). Silent exclusions discovered mid-engagement are findings.
- Exception hygiene: approvals, expiry dates, review triggers and review evidence on every exception, including the comfortable ones (QCI-4.3-02). An exception without an expiry date is a policy change that skipped governance.
- Honest deltas. A score that moved down with a documented reason builds more trust than a score that only ever rises. Auditors have seen scores that only rise. They have opinions about them. QCI-1.3-02 requires restated or explicitly non-comparable trends when the method changes, which this edition did.
- Sampling you can defend. QCI-4.8-02 expects the assessor to record the population, the selection rationale and every unresolved high-impact exception. A sample that avoided the hard cases is not a sample.

> **WHAT THE ASSESSOR WILL ASK**
> Pick any claim in your governing-body insert at random and walk me to its artifact in under five minutes. Programs that can do this pass. Programs that need a week to reconstruct the trail have answered a different question.

12 Hard questions

“When is Q-Day?” Nobody knows, and anyone offering a date is selling something. The estimates that matter run from aggressive to conservative, and the planning arithmetic does not need the date: if data lifetime plus migration time exceeds the optimistic end of the range, the institution is already late, and that inequality is checkable today with the horizon fields you already have. The standard says the same in Clause 1.1: it does not require a prediction.

“Isn’t this vendor hype?” Much of the surrounding noise is. The core is not: the algorithms are standardized, the deprecation trajectory is published, and the harvest-now exposure on long-lived data is a present-tense collection problem, not a future decryption one. The discipline is separating the published record from the urgency manufactured around it, which is what evidence-based scoring is for, and why the obligations register of QCI-2.2-01 records the status of every source it cites.

“What about symmetric encryption?” It largely survives with adequate key sizes, and QCI-4.6-03 says so: sound AES-256 does not need replacing because of the quantum threat, though a compromised key or an exposed key envelope does. The break is asymmetric: RSA, elliptic curves, classic key exchange. That is exactly why this is an identity and signature problem as much as a confidentiality problem, since proving who did what is what the asymmetric layer does for a living.

“Should we just deploy hybrid everywhere?” Hybrid is a decision, not a default. It can add resilience to key establishment when its construction, authentication, negotiation and fallback are specified and verified (QCI-4.5-03); it does nothing for signatures or authentication, it adds

complexity, and it may later need a transition to PQC-only. A binding regime such as CNSA 2.0 can require PQC-only. Record the reasoning either way. Chapter 13.1 has the longer answer.

“Does QKD change the plan?” No. Quantum key distribution protects one hop of one link, does nothing for signatures, credentials or trust chains, and does not pass any gate. Where it exists, it is a compensating control on named links, recorded as treatment with the flag still raised. QCI-PN-01 states the position so it need not be relitigated.

“Why is the standard free?” Because a standard you must pay to read is marketing collateral with delusions. Adoption is what makes a scoring rubric comparable across institutions, and comparability is the entire value of a score. Free is not generosity. It is methodology.

“We already did a PQC assessment.” Good, and one question determines what you bought: did it count the certificate estate, the operational credentials, and the supplier-held keys, or did it list the algorithms found in code? If the former, you are ahead of nearly everyone. If the latter, you have half an inventory and chapter 6 of this Handbook.

“How is this different from National Institute of Standards and Technology (NIST) and Federal Financial Institutions Examination Council (FFIEC) guidance?” It operationalizes them rather than competing with them. NIST defines the algorithms and the trajectory. Sector guidance sets expectations. QCI-QS1 supplies the governance machinery in between: who owns the migration, what the inventory must contain, how progress is scored without inflation, and what evidence the governing body sees quarterly. The citation discipline is deliberate: every normative anchor in the standard names its source and its status in Annex E, and Clause 2.1 states that no external document is incorporated as an indispensable normative dependency.

13 Selecting tools and providers

The standard names no tool and no provider, and conformance depends on none. What it does say is what a tool’s output must carry to count as evidence (QCI-5.4-01), how conflicting evidence is reconciled (QCI-5.4-02), what a cryptographic profile must specify before it goes to production (QCI-4.5-01 to 4.5-04), and what a supplier must answer to stay off the exception register (Clause 7). This chapter is the judgment between those provisions.

13.1 Four principles

A scan is an input to the QASI. It is not the QASI. Discovery tooling finds algorithms in code, protocols on the wire and certificates in stores. It does not find owners, horizons or supplier-held keys. Every field a tool populates needs the QCI-5.4-01 elements before it is evidence, and every record needs an owner and a technical reviewer before it is validated coverage (QCI-5.1-02). Scan reach may be reported beside coverage, labelled, and never instead of it.

Profiles, not products. A product that supports PQC may still be running a classical profile until it is configured and verified (Clause 9.5). QCI-4.5-01 distinguishes supported, configured and observed. Select for the profile you will approve, the evidence the supplier can give for it, and the upgrade path when the profile changes.

Hybrid is a decision, not a default. A hybrid key establishment profile can add resilience when its construction, authentication, negotiation and fallback policy are specified and verified (QCI-4.5-03). It does not upgrade signatures or authentication, and it carries complexity and a

later transition to PQC-only. Record the reasoning either way; a binding regime such as CNSA 2.0 may require a PQC-only profile.

Buy agility, not an algorithm. The G80 test asks whether the profile can change again without replacing the platform. A product that hard-codes ML-DSA has reproduced the condition the program exists to remediate, and it will fail the test the day a parameter set is deprecated.

> **COMMON MISTAKE**
> Reporting a tool's coverage figure as QASI coverage. QCI-5.1-03 defines coverage as validated critical records over the identified critical population, separately for systems and flows, with numerator and denominator published. A 67 percent scan-reach figure in the governing-body insert is inventory theater with a decimal point, and it does not pass G60.

13.2 Where to look, by domain

Annex G partitions dependencies into thirteen non-exclusive domains: two foundation layers (discovery and inventory; crypto-agility and governance) and eleven technology domains. A tool that is right for one is blind in another. The companion handouts QCI-QS1-C1 and C2 list options per domain without ranking them; the table here is the shape of the market, not a recommendation.

Domain group	What discovers it	What remediates it	The trap
Foundation: discovery and governance	Multi-method platforms; code, network and host scanners; the client's existing certificate and key inventories	Crypto-agility layers; the governance method itself	Buying discovery and governance from one supplier without noticing the lock-in
Communications: TLS edge, VPN, messaging	Active TLS and SSH scanners; passive traffic monitors	A CDN setting, a TLS policy, a firmware version; overlays where endpoints cannot change	Treating a TLS version as a verdict; TLS 1.3 over X25519 is vulnerable, over an RFC 10024 hybrid group it is not
Trust and identity: PKI, identity	Certificate lifecycle exports; certificate transparency search	Private CAs with ML-DSA; nothing yet for public web PKI or federation signing by default	Issuing credentials twice: the double migration of chapter 10
Keys and hardware: KMS, storage, devices	Cloud KMS APIs; host agents; firmware images	HSM firmware; a KEM-based key-protection scheme (KEM, KDF, wrap); device replacement planning	Calling a rewrap remediation when the old key envelope may already have been captured (QCI-4.6-03)
Application and sector: libraries, payments, digital assets	Source and binary scanners; SBOMs and CBOMs	Library upgrades; scheme and protocol timelines the organization does not control	Waiting for the protocol when address hygiene and key transport are already in the organization's hands

13.3 What credible discovery evidence states

QCI-5.4-01 lists eight things. The reasoning behind each is short. The tool and version, because two runs of one product can differ by a commit. The ruleset, because the same tool with a different policy finds different things. The scope and date, because a scan of one subdirectory reports everything about nothing. What was not examined, because a silent skip and an absent algorithm produce the same output and only the tool can tell them apart. A stable finding identifier and a location, because an assessor walks from the claim to the line, and again next quarter. A digest, because the file cited must be the file produced, and the digest alone is not proof of who produced it. The mapping to the field, and the producer, reviewer and disposition, because evidence is a record of a decision someone made. QCI-T1 is the checklist.

> **WHAT THE ASSESSOR WILL ASK**
> Pick any algorithm in your QASI and walk me to the scan that found it, the version and ruleset that ran, and the list of what that scan did not read. Programs that can do this in five minutes pass. Programs that produce a vendor PDF have answered a different question.

13.4 Reading a supplier response

Non-answers are answers, and chapter 8 says so. QCI-7.2-03 says what adequate means: every applicable area addressed, the product and deployment scope identified, available, configured and deployed posture separated, assessable evidence for every present-tense claim, and owned, dated commitments with limitations. A response that names no algorithm, version or date is marketing, and it is inadequate. A response with a checkable item is evidence. A response whose items the analyst confirmed is verified. Pre-standard names are a tell: a supplier still writing “Kyber” and “Dilithium” without the FIPS number is describing an implementation that predates the standard, and the question is whether it was updated. And the attestation is signed by an officer on the Annex C form, or it is not an attestation.

14 Governing the migration across domains

The standard defines what a program must have. Chapters 2 to 12 take it from nothing to its first score. This chapter is what happens in the second year, when the migration spans thirteen domains, dozens of suppliers and a governing body that has heard the threat briefing twice and now wants a decision. The Institute publishes a method for that, QCI-M1, and this chapter is its summary. The standard says in Clause 9.6 that QCI-M1 is separate and not required for conformance; engagements apply it as methodology.

14.1 Six stages, per domain

Every domain passes through Discover, Classify, Sequence, Procure, Prove and Assure. The stages are per domain, not per program: data in transit can be at Prove while identity is at Sequence, and the governing-body insert should show exactly that. A program that reports one stage for everything has a slide.

Stage	Question	Exit
Discover	Where does this domain use cryptography, and who owns it?	Every critical system and flow in the domain has a validated record with an owner, a reviewer and evidence meeting QCI-5.4-01
Classify	What is exposed, for how long, and how badly?	Confidentiality and verification horizons, exposure flags and treatment status on every record (QCI-5.3-01, 5.3-02)
Sequence	In what order, and what waits?	A resourced roadmap entry with owner, milestone types and acceptance criteria (QCI-4.2-02), or a recorded decision to wait with owner, interim treatment and review date
Procure	Who supplies the change, on what terms?	Every critical supplier has a current adequate response and attestation, or is a registered exception under QCI-4.3-02 and 7.3-01; procurement evaluated under QCI-7.1-02
Prove	Does it work, and can we change it again?	The QCI-4.7 test passed and acceptance recorded under QCI-4.7-02; for G80, on a critical trust pathway within twelve months
Assure	Can an assessor walk from claim to artifact?	An assessment pack meeting QCI-4.8-01 that an assessor traverses in under five minutes

14.2 The gates as stage exits

The gates of QCI-6.3-01 already exist. The method makes them stage exits: Discover and Classify across every critical domain, to 95 percent validated coverage of both systems and flows, passes G60; Procure across every critical supplier passes G70, and no exception substitutes; Prove on one critical pathway within twelve months passes G80. A gate is then passed by finishing a stage rather than by argument, and a score that went down because a domain failed its exit is more credible than a score that only rises.

14.3 Sequencing is a risk decision, not an order

The previous edition of this material said key exchange first, signatures second, hardware third. The standard is more careful, and it is right. QCI-4.2-02 requires every roadmap decision to weigh confidentiality and verification horizons, present capture exposure, consequences, supplier and trust dependencies, lead time, end-of-support and applicable deadlines, and it forbids a mandatory sequence that postpones all signature or hardware work until key-exchange work is done. HNDL exposure on communications and key envelopes is present-tense and usually moves early. Long-lived signatures, trust anchors, secure boot and constrained devices have replacement lead times measured in years and often need parallel investment now. Annex G exposes unowned dependencies; it is not an execution order.

14.4 A decision to wait is a decision

Some domains are not ready: public web PKI before browsers trust post-quantum roots, identity federation before vendors ship, a device fleet that cannot be patched. Waiting there can be

correct, and Annex G says under what conditions: 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 in the obligations register (QCI-2.2-01). QCI-4.3-02 asks who can accept an exception and for how long; the decision record (QCI-T4) is the artifact that proves someone did, on a date, with an expiry and review triggers.

> **COMMON MISTAKE**
> Writing the decision after the fact, the week the auditor asks. A record dated the week of the audit with a review date already passed is worse than no record: it shows the organization knows what governance looks like and did not do it.

14.5 Ownership across thirteen domains

Unassigned risk does not get managed, and thirteen domains are thirteen chances to leave something unassigned. QCI-4.1-01 assigns responsibilities to engineering and architecture, system and data owners, procurement, incident response, legal and compliance, and assurance, with a cross-functional steering function to resolve dependencies. The method maps those roles to each stage, and it names one seam that needs an owner of its own: the boundary between the identity domain and any identity modernization program already running. Without that owner, credentials get issued twice and the inventories are never reconciled, which is the double migration of chapter 10 arriving on schedule.

14.6 The assessment pack

Each domain produces one pack per quarter in a fixed structure: boundary statement, QASI extract, exposure and treatment summary, roadmap entry or decision record, supplier file, test and acceptance file, score contribution with the reason for the delta, and an index linking every claim to its artifact with producer, reviewer and integrity controls (QCI-4.8-01). The fixed structure is what lets an independent assessor compare packs across domains and across institutions, and it is what makes an independently assessed score a different number from a self-assessed one, as QCI-1.2-03 requires it to be.

> **WHAT THE ASSESSOR WILL ASK**
> Show me which domains are at which stage, and show me the domain that has not started. Then pick a cell in the migration map and walk me to its record, its supplier response, or its decision record. A program that can answer both has a migration under governance.

14.7 Cadence

The method runs on the quarterly cycle of QCI-4.1-02 and QCI-6.5-01 and borrows its heartbeat from the risk pack that already exists. Each quarter every domain reports its stage, its gate status and its delta; the Quantum Risk Owner consolidates thirteen reports into the worksheet, records the assessment type, and writes the one-page insert with the elements of QCI-8.1-01. Evidence older than 90 days is re-validated or reviewed (QCI-5.1-04). A domain that reports the same stage for three consecutive quarters with no decision record is escalated under QCI-4.3-01. For a new program the first pass of the method is the 90-day sequence of chapter 2; Prove

and Assure begin in the second quarter for the first domain, which is usually data in transit, though QCI-4.2-02 may put a long-lead hardware decision beside it from the start.

Appendix A Requirement cross-reference

Where each Handbook chapter touches the standard (Version 2.3). Requirement identifiers are normative; clause and annex references are informative.

Handbook chapter	Standard locations
1 Read this first	Clause 1.1; QCI-1.2-03; QCI-4.1-01; QCI-5.2-03
2 The 90-day sequence	Clauses 4, 5; Clause 9.1; QCI-1.1-01, 1.1-02; QCI-2.2-01; QCI-7.2-04
3 Scoring in practice	QCI-1.2-03, 1.2-04; Clause 6; QCI-4.8-02; Annex B
4 The crypto agility test	QCI-4.7-01, 4.7-02; QCI-6.3-01 gate G80; QCI-6.9-01; Clause 9.2; QCI-T2
5 QRAF	QCI-4.1-01, 4.1-02; Clauses 4.1 to 4.4; Clause 9.7
6 QASI	Clause 5; QCI-5.2-01 to 5.2-03; QCI-5.3-01, 5.3-02; QCI-4.5-04; QCI-4.6-02; Clause 9.3; Annex A
7 Q-Risk Score	Clause 6; QCI-6.1-01, 6.1-02, 6.3-01, 6.3-02, 6.5-01; Annex B
8 The vendor pack	Clause 7; QCI-7.2-01 to 7.2-04; QCI-7.3-01; QCI-4.3-02; Annex C sections A to G and the attestation form
9 Briefing the governing body	Clause 8; QCI-8.1-01, 8.1-02, 8.2-01; Annex D
10 How programs fail	QCI-4.1-01, 4.2-02, 4.5-01, 5.2-01, 5.2-02, 5.3-01, 6.3-01; Clause 7; QCI-QS1-C5
11 What auditors like to see	QCI-1.1-02, 1.3-02, 4.3-02, 4.8-01, 4.8-02; Clause 9.4
12 Hard questions	Clauses 1.1, 2.1; QCI-2.2-01; QCI-4.5-03; QCI-4.6-03; Annex E; QCI-PN-01
13 Selecting tools and providers	QCI-5.4-01 to 5.4-03; QCI-4.5-01 to 4.5-04; QCI-7.2-03; Clause 9.5; Annex G; QCI-T1; QCI-QS1-C1, C2
14 Governing the migration across domains	QCI-4.2-02, 4.3-01, 4.3-02, 4.7-01, 4.7-02, 4.8-01, 5.1-04; QCI-6.3-01; Clause 9.6; Annex G; QCI-M1; QCI-T2 to T4

Appendix B Acronyms and key terms

Every acronym used in this Handbook, expanded. The first use of each concept in the chapters above is also written out in full. This table is the quick reference for any acronym encountered out of order, including the algorithm and protocol names that appear in the worked examples.

Acronym or term	Expansion
AES	Advanced Encryption Standard
AI	Artificial Intelligence

Acronym or term	Expansion
API	Application Programming Interface
CA	Certificate Authority
CBOM	Cryptography Bill of Materials
CDN	Content Delivery Network
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSA 2.0	Commercial National Security Algorithm Suite 2.0, the NSA algorithm policy for national security systems
CRO	Chief Risk Officer
CRQC	Cryptographically Relevant Quantum Computer
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman key agreement
ECDSA	Elliptic Curve Digital Signature Algorithm
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards, the NIST standards series (for example FIPS 203, 204, 205)
G60, G70, G80	The three score gates of QCI-6.3-01: coverage, supplier attestation, and agility test
HNDL	Harvest Now, Decrypt Later
HSM	Hardware Security Module
IAM	Identity and Access Management
KDF	Key Derivation Function
KEM	Key-Encapsulation Mechanism
KMS	Key Management Service
ML-DSA	Module-Lattice-Based Digital Signature Algorithm (NIST FIPS 204)
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism (NIST FIPS 203)
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
OT	Operational Technology
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PQ/T hybrid	A specified combination of post-quantum and traditional mechanisms of the same function

Acronym or term	Expansion
QASI	Quantum Attack Surface and Cryptographic Dependency Inventory
QCI	Quantum Core Institute Inc.
QCI-QS1	The Quantum Core Institute Quantum Readiness and Post-Quantum Cryptography Governance Standard
QCI-M1	QCI Migration Governance Method, a separate methodology not required for conformance
QCI-T1 to T4	QCI instruments: discovery evidence checklist, test and acceptance protocol, exception register template, decision record template
QKD	Quantum Key Distribution
QRAF	Quantum Risk Governance and Assessment Framework
Q-Day	Informal term for the point at which a quantum computer can break current public-key cryptography
Q-Risk Score	Quantum Risk Score, the comparable 0 to 100 readiness score defined in the standard
RSA	Rivest-Shamir-Adleman, the public-key algorithm named for its inventors
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (NIST FIPS 205)
SSH	Secure Shell
SSO	Single Sign-On
TLS	Transport Layer Security
X25519	An elliptic-curve Diffie-Hellman key agreement function

Appendix C What changed in V2.3

- All references to the standard now use QCI requirement identifiers. The clause numbers cited by V2.2 did not match the published v2.2 standard or the issued v2.3; Option A, correcting the Handbook, was chosen on September 23, 2026.
- Chapter 3.2 rewritten for QCI-1.2-03 and 1.2-04: independent assessment replaces external validation, and conformance status is reported beside the score.
- Chapter 4 rewritten: the five-component agility proof is replaced by the eleven test categories of QCI-4.7-01, the acceptance rule of QCI-4.7-02, and gate G80’s twelve-month window. The five components are mapped to the new categories.
- Chapter 7 restated for the fixed Core profile: Defensible readiness begins at 81; G60 requires 95 percent validated coverage of both critical systems and critical flows; G70 is no longer satisfied by a registered exception.
- Chapter 8 carries the 60-day response deadline, the annual attestation refresh, and the G70 consequence of an exception.

- Chapter 6 worked examples restated with confidentiality and verification horizons, named exposure flags, separate treatment status, human and workload identity records, and the KEM-based key-protection scheme.
- Chapter 2 no longer asks the program to set a coverage threshold; the standard fixes it.
- Chapters 13 and 14 added: selecting tools and providers, and governing the migration across the thirteen Annex G domains.
- Chapter 12 gains hybrid and QKD answers. Appendix A replaced. Appendix B extended.

This Handbook is informative. The standard is free to download, cite, and adopt at quantumcoreinstitute.com.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).