

QUANTUM CORE INSTITUTE

QCI-M1 Migration Governance Method

Governing post-quantum migration across every cryptographic domain

Field	Value
Document ID	QCI-M1
Version	V2.0 – September 23, 2026. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
Applies to	QCI-4.1 to 4.3, 4.7, 4.8, 5.1, 5.3, 5.4, 6.3, 7.2, 7.3; Clauses 9.6 and 9.7; Annex G; Handbook chapter 14
Status	Methodology. QCI-M1 applies the standard; it does not create, modify, or interpret a requirement. Clause 9.6 of the standard states that QCI-M1 is separate and not required for conformance. Where this method and the standard differ, the standard governs.
Scope of this edition	The published skeleton: stages, gates, ownership, decision records and assessment-pack structure. The engagement kit that applies it is available from the publisher.
License	Free. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

1 Why a method

QCI-QS1 defines what a quantum readiness program must have. The Practitioner Handbook explains why each requirement exists and takes a new program to its first Q-Risk Score in 90 days. Nothing in either says how to govern execution when the migration spans thirteen cryptographic domains, dozens of suppliers and several years. That gap is where programs stall after their first score. Each domain has its own product market, its own lead time and its own evidence type. QCI-M1 gives each domain a stage, a gate, an owner and a closing artifact, and ties the gates to the ones the standard already enforces.

WHY THIS IS METHODOLOGY AND NOT STANDARD

The standard stays testable and vendor-free. A method carries judgment: how to sequence, when to wait, what counts as enough. The standard's rights page draws the line, and Clause 9.6 says QCI-M1 is not required for conformance. It is published so that clients, assessors and suppliers share one vocabulary.

2 Five principles

1. **Inventory before remedy.** No domain enters Procure until its QASI records name the system, the owner, the horizons and the cryptographic use with its profile (QCI-5.2-01). Buying ahead of the inventory purchases the wrong thing for the wrong system.
2. **Sequence by exposure, lead time and dependency, not by a fixed order.** QCI-4.2-02 requires every roadmap decision to weigh confidentiality and verification horizons, present capture exposure, consequences, dependencies, lead time, end-of-support and applicable deadlines, and forbids postponing all signature and hardware work until key exchange is done. HNDL exposure on communications and key envelopes usually moves early; long-lead trust-anchor and hardware work often starts in parallel.
3. **A profile is a decision.** Every production change uses an approved profile under QCI-4.5-01. A hybrid profile specifies its construction, authentication, negotiation and fallback policy (QCI-4.5-03); a PQC-only profile records the regime that requires it. Neither is a default.
4. **Buy agility, not an algorithm.** Gate G80 asks whether the profile can change again without replacing the platform. A product that hard-codes an algorithm has reproduced the condition being remediated.
5. **A decision to wait is a decision.** Waiting is governed when it has an owner, a rationale, an interim treatment, a review date and review triggers, all within the organization's obligations register (QCI-2.2-01) and risk appetite (QCI-4.3-02). Otherwise it is drift.

3 The six stages

Every domain in Annex G passes through six stages. Stages repeat per domain and per quarter; a program will have domains at different stages at once, and that is the expected state.

Stage	Question it answers	Principal output	Exit gate
1 Discover	Where does this domain use cryptography, and who owns it?	Linked QASI records (system, use, flow, trust, supplier) with discovery evidence per QCI-5.4-01	Every critical system and flow has a validated record: owner, technical reviewer, known values or explicit unknowns (QCI-5.1-02); evidence within 90 days (QCI-5.1-04)
2 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)	No record without horizons and flags; the domain's above-appetite exposures listed with treatment or escalation
3 Sequence	In what order, and what waits?	Resourced roadmap entry with owner, milestone types and acceptance criteria (QCI-4.2-02), or a decision record	Milestone with owner and date, or a decision record with review date and triggers
4 Procure	Who supplies the change, and on what terms?	Annex C responses, adequacy determinations (QCI-7.2-03), attestations (QCI-7.2-02), exception entries (QCI-7.3-01)	Every critical supplier has a current adequate response and attestation, or a registered exception; deadlines per QCI-7.2-04
5 Prove	Does it work, and can we change it again?	QCI-4.7-01 test results and QCI-4.7-02 acceptance; completion evidence per QCI-6.2-02	At least one critical transition accepted; for G80, a critical trust pathway tested within twelve months
6 Assure	Can an assessor walk from the claim to the artifact?	Assessment pack per QCI-4.8-01; pillar contribution; governing-body insert line	An assessor reaches any artifact from any claim in under five minutes

COMMON MISTAKE

Running the six stages once, for the whole estate. The stages are per domain. Data in transit can be at Prove while identity is still at Sequence, and the governing-body insert should show exactly that.

3.1 Stage 1: Discover

Inputs: the assessment boundary (QCI-1.1-01), the reconciled critical population (QCI-5.1-01), discovery output, existing certificate, key and supplier inventories. Activities: run or collect discovery; check each output with QCI-T1; reconcile conflicting sources (QCI-5.4-02); build the linked records; validate each with its owner and technical reviewer. Unknown values stay explicit with an owner and a due date. Output: validated records, and a coverage figure computed per QCI-5.1-03 with numerator and denominator.

3.2 Stage 2: Classify

Inputs: validated records; data classification; retention and regulatory obligations from the register. Activities: set confidentiality and verification horizons as dates or durations with a start date; assess present capture exposure; apply the exposure flags; set treatment status

separately. An approved plan never clears a flag (QCI-5.3-01). Output: the domain's exposure ranked, with the horizon arithmetic done per record.

3.3 Stage 3: Sequence

Inputs: classified records across all domains; the obligations register. Activities: weigh the QCI-4.2-02 factors; set milestones by type (planning, procurement, pilot, production acceptance, retirement) with owners, capacity and acceptance criteria; record resource shortfalls as delivery risks; or record a decision to wait under QCI-T4. Output: the roadmap entry, which is a ticket in a backlog rather than a line in a slide.

3.4 Stage 4: Procure

Inputs: the domain's supplier records. Activities: issue Annex C sections A to F, and G where applicable, with a deadline no later than 60 days (QCI-7.2-04); score responses with QCI-INT-2; determine adequacy under QCI-7.2-03; obtain the authorized attestation; evaluate new procurements under QCI-7.1-02; register exceptions under QCI-4.3-02 and 7.3-01. Output: attestations on file, contract milestones where chosen, the exception register current. A supplier that has not answered by the deadline is an exception, and an exception does not pass G70.

3.5 Stage 5: Prove

Inputs: the approved profile and a critical trust pathway. Activities: run the QCI-4.7-01 test categories with QCI-T2; obtain QCI-4.7-02 acceptance; retire legacy paths; dispose of obsolete keys. Output: an accepted production transition that counts toward completion under QCI-6.2-02, and for G80 a pathway test within twelve months with limits disclosed. A pilot, a vendor release or an accepted risk is not completion.

3.6 Stage 6: Assure

Inputs: every artifact the domain produced. Activities: assemble the assessment pack in the structure of chapter 7; record producer, reviewer and integrity controls on each item (QCI-4.8-01); record the pillar contribution and the reason for the delta; write the domain's line in the insert (QCI-8.1-01). Output: a pack an assessor can traverse, and a score that moved for a documented reason.

4 Gates as stage exits

Gate (QCI-6.3-01)	Cap	Condition	Stage that satisfies it
G60 Inventory	60	Both critical-system and critical-flow validated coverage $\geq 95\%$; no unresolved material population discrepancy	Discover and Classify complete for every domain holding a critical system or flow
G70 Suppliers	70	Every critical supplier has a current, adequate, product- and deployment-specific response and authorized attestation. An operating exception is not a substitute	Procure complete for every critical supplier; exceptions remain on the register and do not lift the cap

Gate (QCI-6.3-01)	Cap	Condition	Stage that satisfies it
G80 Agility	80	At least one critical trust pathway passed a representative end-to-end test under QCI-4.7 within twelve months and after any invalidating change; limits disclosed	Prove complete on at least one critical pathway

Below the gates, each stage exit is checked per domain at the quarterly cycle. A domain that fails its exit does not advance, and the reason is recorded. That record is what an independent assessor under QCI-1.2-03 assesses against.

WHAT THE ASSESSOR WILL ASK

Show me which domains are at which stage, and show me the domain that has not started. A program that can answer both has a migration under governance. A program that reports one stage for everything has a slide.

5 Ownership across domains

Unassigned risk does not get managed. QCI-4.1-01 assigns responsibilities to engineering and architecture, system and data owners, procurement and vendor risk, incident response, legal and compliance, and assurance, with a cross-functional steering function. The method maps those roles to each stage; an organization records its own in the engagement kit's RACI template.

Stage	Accountable	Responsible	Consulted	Informed
Discover	Quantum Risk Owner	Architecture and engineering; system and data owners; technical reviewers	Procurement (supplier records)	Steering function
Classify	Quantum Risk Owner	System and data owners; legal and compliance (horizons, obligations)	Data governance	Executive sponsor
Sequence	Executive sponsor	Quantum Risk Owner; steering function	Architecture; legal	Governing body (via insert)
Procure	Procurement and vendor risk	Relationship owners; legal (contract milestones)	Quantum Risk Owner; architecture	Steering function
Prove	Architecture and engineering	Platform and operations teams; accountable service owner (acceptance)	Quantum Risk Owner; incident response	Executive sponsor
Assure	Quantum Risk Owner	Program office; assurance function	Independent assessor where engaged	Governing body

One team needs a named owner of its own: the boundary between the identity domain and any identity modernization program already running. Without it, credentials get issued twice and the inventories are never reconciled.

6 Decision records

Every choice the method produces is written in the shape QCI-4.3-02 requires for an accepted risk or exception: affected assets and requirements, rationale, exposure and residual risk, treatment and compensating controls, owner, approving authority, approval date, expiry, review triggers, remediation dates, and exit or replacement strategy, or a documented rationale where exit is infeasible. Renewal is an explicit decision before expiry; an expired exception is escalated. QCI-T4 is the template.

WHY THE REQUIREMENT EXISTS

A decision record is the artifact that proves someone accepted an exposure, on a date, with an expiry and a trigger to look again. It is also what makes a wait defensible to a regulator two years later, and it does not by itself clear an exposure flag or pass a gate.

7 The assessment pack

Each domain produces one pack per quarter, in a fixed structure, so that an independent assessor can compare packs across domains and institutions.

1. **Boundary statement** for the domain, consistent with QCI-1.1-01 and the exclusions of QCI-1.1-02.
2. **QASI extract**: linked records with QCI-5.4-01 provenance for discovery-sourced fields and explicit unknowns.
3. **Exposure and treatment summary**: horizons, flags, treatment status, above-appetite items and their escalation.
4. **Roadmap entry or decision record**, with owner, dates and triggers.
5. **Supplier file**: responses, adequacy determinations, attestations, exception entries.
6. **Test and acceptance file**: QCI-4.7 results, dispositions, acceptance record, observation period, legacy retirement and key disposition.
7. **Score contribution**: the domain's effect on each pillar, the delta since last quarter, and the reason.
8. **Index**: every claim linked to its artifact with producer, reviewer, integrity controls, retention and access restrictions (QCI-4.8-01).

8 Cadence

The method runs on the quarterly cycle of QCI-4.1-02 and QCI-6.5-01. Each quarter every domain reports its stage, gate status and delta; the Quantum Risk Owner consolidates the reports into the worksheet, records the assessment type (QCI-1.2-03), reports conformance status beside the score (QCI-1.2-04), and writes the insert with the elements of QCI-8.1-01. Evidence past 90 days is revalidated or reviewed. Urgent events follow QCI-4.3-01 without

waiting for the meeting. A domain at the same stage for three consecutive quarters with no decision record is escalated.

For a new program, the first pass is the 90-day sequence of Clause 9.1: ownership, boundary and population in weeks 1 to 2; linked inventory and validation in weeks 3 to 6; horizons, exposure and supplier engagement in weeks 4 to 9; first assessment, roadmap, test plan and insert in weeks 10 to 12. The sequence is a planning aid, not a conformance grace period.

9 Relationship to the standard and the Handbook

QCI-QS1 is the requirement. The Handbook is the explanation. QCI-M1 is the method by which a program meets the requirement across domains, quarter after quarter. Cite the standard, argue with the Handbook, run the method. The engagement kit adds the working templates, facilitation guides and calibrated examples, available from the publisher.

Annex A. Stage checklist

Stage	Exit condition	Yes / No
Discover	Every critical system and flow in the domain has a linked record with owner and technical reviewer	
Discover	Every discovery-sourced field carries the QCI-5.4-01 elements (QCI-T1)	
Discover	Critical evidence is within 90 days or has a documented unchanged-configuration review	
Classify	Every record carries confidentiality and verification horizons, exposure flags and treatment status	
Classify	AI records complete where AI systems are in scope (QCI-5.2-03)	
Sequence	A resourced milestone with owner exists, or a decision record with review date and triggers	
Procure	Every critical supplier has a current adequate response and attestation, or is a registered exception	
Prove	A QCI-4.7 test passed and acceptance recorded on at least one critical pathway; G80 date within twelve months	
Assure	Every claim in the pack links to a retrievable artifact with producer and reviewer	
Assure	The domain's pillar delta has a documented reason	

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).