

QUANTUM CORE INSTITUTE

Crypto Agility Test and Acceptance Protocol

The test that passes G80, and the acceptance that makes a migration count

Field	Value
Document ID	QCI-T2
Version	V2.0 – September 23, 2026. Rebuilt on QCI-4.7-01, QCI-4.7-02 and gate G80 (QCI-6.3-01).
Applies to	QCI-4.7-01 (test plan), QCI-4.7-02 (acceptance), QCI-6.3-01 gate G80, QCI-6.9-01 (P4 rubric levels 3 to 5), QCI-6.2-02 (completion); Clause 9.2
Use	Once per critical trust pathway for G80, repeated within 12 months and after any invalidating material change; for every production migration under QCI-4.7
Status	Public instrument. Applies QCI-QS1; creates no requirement. Where this instrument and the standard differ, the standard governs. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
License	Free. Attribution required. May be copied into an organization's own templates with attribution; may not be modified and redistributed as a QCI document.
Publisher	Quantum Core Institute Inc.

1 Purpose

Gate G80 caps the Q-Risk Score at 80 unless at least one critical trust pathway has passed a representative end-to-end crypto-agility test under QCI-4.7 within the previous 12 months and after any invalidating material change, with the pathway and the limits of the test disclosed. QCI-4.7-01 lists what the test must cover; QCI-4.7-02 says what acceptance requires before a migration counts as complete. This protocol is the runbook for both.

The G80 proof is deliberately narrower than the representative estate testing that P4 levels 4 and 5 require under QCI-6.9-01. One successful pathway lifts the gate. It does not demonstrate enterprise readiness, and the report says so.

WHAT THE ASSESSOR WILL ASK

Show me the pathway's QASI record and its criticality rationale, the test environment and how it represents production, the test categories you omitted and why, and the rollback record. A pilot, a vendor release, or a test on a non-critical endpoint satisfies none of these.

2 Preconditions

- The pathway is a critical trust pathway as defined in Clause 3: an end-to-end dependency chain protecting a critical operation, including endpoints, intermediaries, authentication, key establishment, trust anchors and key management. It is recorded in the QASI with linked use, flow and trust records (QCI-5.2-01) and its criticality follows QCI-1.1-02.
- The change uses an approved cryptographic profile under QCI-4.5-01, with function, algorithm and parameter set, protocol construction, and for a hybrid profile the combiner, authentication mechanism, negotiation and verification policy and permitted fallback (QCI-4.5-03).
- The test environment and configuration are representative of the affected pathway (QCI-4.7-01). The relationship to production is documented: identical, scaled by a stated factor, or not load-sensitive with justification.
- Every test category in chapter 3 is either planned or has a documented technical non-applicability rationale. Omission without rationale fails the plan.
- The accountable service owner and engineering have approved the test plan. Unsigned plans produce unowned results.

3 Test categories, QCI-4.7-01

#	Category	What the test must show	Evidence produced
1	End-to-end interoperability	Every component on the pathway completes the protected operation with the new profile: clients, intermediaries, partners, verifiers.	Interoperability matrix by component and version
2	Actual algorithm negotiation	The new algorithm is negotiated or in use, confirmed by inspection at both ends (negotiated group, certificate algorithm, KMS key type), not by configuration alone.	Inspection output before and after

#	Category	What the test must show	Evidence produced
3	Authentication and trust validation	Certificate chains, trust anchors, identity federation and verifiers validate under the new profile; key establishment and authentication are recorded separately (QCI-4.5-03).	Trust validation log per dependency
4	Invalid key, ciphertext and signature inputs	Malformed or invalid inputs are rejected; no fallback to an insecure state.	Negative test results
5	Downgrade and fallback	Unauthorized classical fallback is prevented or detected within the policy limit; any permitted fallback matches its approved scope and is logged.	Downgrade test results; monitoring evidence
6	Message, certificate size and fragmentation	Larger post-quantum keys, certificates and signatures traverse the pathway; fragmentation and MTU behaviour verified where relevant.	Size and fragmentation results, or non-applicability rationale
7	Resource exhaustion	Behaviour under handshake floods, memory and CPU pressure; no denial of service introduced by the new profile.	Load-abuse results
8	Capacity and latency	Latency (p50, p95, p99) and throughput before and after, under the documented load profile.	Measurement table; load profile; comparison to production
9	Backup and restore	Keys, trust stores and configuration restore correctly; for stateful signatures, no signing-state reuse across backup and restore (QCI-4.6-01).	Restore test record
10	Failover	Redundant components fail over without reverting to the vulnerable profile.	Failover test record
11	Authorized rollback	The prior configuration is restored under the documented procedure, with elapsed time recorded. A rollback that restores vulnerable protection in production is governed as an exception (QCI-4.7-02).	Rollback timing and inspection

4 Acceptance, QCI-4.7-02

Before a migration is accepted, engineering and the accountable service owner approve:

1. The test results and the disposition of every failure.
2. Operational monitoring for the new profile, including downgrade detection.
3. Support readiness and the recovery procedures.
4. Residual exceptions, each recorded under QCI-4.3-02 with expiry.
5. An observation period proportionate to the change, with its end date.

Completion, for the purposes of QCI-6.2-02 and the P4 rubric, additionally requires evidence of the effective production configuration, removal or explicit exception of legacy paths, and disposition of obsolete keys, certificates and configurations. A pilot, a vendor release, an accepted risk or a plan does not count as completion.

5 Results template

Field	Entry
Pathway (QASI system, flow and trust record IDs); criticality rationale	
Owner; engineering lead	
Profile before and after (QCI-4.5-01 reference); hybrid construction and fallback policy if any	
Environment; load profile; relationship to production	
Categories 1 to 11: result per category, or non-applicability rationale	
Failures and dispositions	
Rollback elapsed time; confirmed by inspection (yes/no)	
Monitoring, support readiness, recovery procedures approved (yes/no; by whom)	
Residual exceptions (QCI-T3 IDs); observation period end date	
G80 claim: representative end-to-end test passed (yes/no); date; valid until (12 months or next invalidating change); limits disclosed	
P4 contribution: does this test form part of representative coverage of a deployed pattern (QCI-6.9-01 levels 4 to 5)? Equivalence analysis reference if shared	
Assessment pack reference (QCI-4.8-01)	

COMMON MISTAKE

Testing the easiest pathway. The pathway you test should be the one your QASI says matters, with criticality High and a rationale under QCI-1.1-02. A proof on a development wiki's TLS endpoint tells the governing body nothing about the payments API, and the assessor will read the criticality rationale before the test results.

6 Crosswalk for readers of the Practitioner Handbook

Handbook V2.2 chapter 4 described the agility proof as five components. Those components are not a named set in version 2.3; they are covered by the QCI-4.7 categories as follows. Handbook V2.3 rewrites chapter 4 on this basis.

Handbook V2.2 component	Where it now sits
Algorithm change capability	Categories 1 to 3: interoperability, actual negotiation, trust validation; profile under QCI-4.5-01
Operational procedure	QCI-4.7-02 acceptance: documented recovery procedures, support readiness, monitoring
Rollback, executed	Category 11, authorized rollback, with elapsed time; production rollback to vulnerable protection is an exception
Performance impact, measured under load	Categories 7 and 8: resource exhaustion, capacity and latency, in a representative environment
Trust chain validation	Category 3, plus categories 9 and 10 for restore and failover of trust material

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).