

QUANTUM CORE INSTITUTE

Decision Record Template

Making a decision to wait as governed as a decision to act

Field	Value
Document ID	QCI-T4
Version	V1.2 – September 23, 2026
Applies to	QCI-4.3-02 (accepted risks and exceptions), QCI-4.2-02 (roadmap decisions), QCI-2.2-01 (obligations register); Clause 9.6 and Annex G.3; QCI-M1 chapter 6 and stage 3, Sequence
Use	One record per decision: to wait in a domain, to accept a vendor roadmap, to depart from hybrid mode, to choose a compensating control over a migration
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

Some domains are not ready to move: public web PKI before browser trust stores hold post-quantum roots, identity federation before vendors ship, a device fleet that cannot be patched. Waiting in those domains can be correct, within the organization's obligations and risk appetite (Annex G.3). It is governed when it has an owner, a rationale, an interim treatment, a review date and review triggers, and it is drift when it has none. The decision record is the artifact that separates the two, and it is the same artifact a regulator asks for two years later when the question is why the organization had not moved.

WHY THE REQUIREMENT EXISTS

QCI-4.3-02 sets what an accepted risk must record, and QCI-4.2-02 sets what a roadmap decision must weigh. A decision record proves someone decided, on a date, with an expiry and triggers. Every choice the migration method produces is written in this one shape, so that a wait, a supplier acceptance and a profile choice can all be found, reviewed and expired the same way. A decision record never clears an exposure flag (QCI-5.3-01) and never lifts a gate.

2 The record

Field	Content
Decision ID	Sequential identifier, never reused.
Decision	One sentence, in the form “we will” or “we will not yet”.
Domain(s) and systems	Annex G domain numbers and QASI system identifiers affected.
Trigger	What raised the decision: a QASI flag, a vendor response, an agility proof gap, a regulatory date.
Options considered	Each option in one line, including the one chosen and why the others were not.
Rationale	The reasoning against the QCI-4.2-02 factors: horizons, present capture exposure, consequences, dependencies, lead time, end-of-support, applicable deadlines.
Obligations check	The QCI-2.2-01 register entries the decision touches, confirming no applicable deadline is missed. A 2035 planning target is not permission to miss an earlier deadline.
Interim treatment	What limits the exposure while the decision stands; compensating controls are not assumed to remove HNDL risk (QCI-5.3-02).
Evidence references	QASI rows, vendor responses, test results, external sources relied on.
Owner	Name and role.
Approved by	Name and role, authorized under the risk appetite statement to accept the exposure for the period stated.
Decided on	Date.
Review date	Date after which the decision lapses unless explicitly renewed. Required.

Field	Content
Conditions for revisiting early	Events that reopen the decision before the review date: a vendor ships, a standard finalizes, a capability estimate moves.
Linked exception	Exception register ID, where the decision creates or extends an exception.
Status	Open; renewed on (date); superseded by (ID); closed on (date).

3 Worked record

Field	Entry
Decision ID	DEC-007
Decision	We will not yet migrate public-facing TLS server certificates to ML-DSA.
Domain(s) and systems	5 PKI and certificates; WEB-001, WEB-004, API-002
Trigger	Roadmap sequencing, QCI-M1 stage 3, Q3 2026
Options considered	(a) Issue ML-DSA server certificates now: no browser trust store holds an ML-DSA root, clients would fail. (b) Hybrid or composite certificates from a public CA: not available for public trust. (c) Wait, and move private trust chains and machine identity first: chosen.
Rationale	Verification horizon on these certificates is under 400 days; forgery exposure begins when an adversary can forge, and present capture does not apply to authentication. Key establishment on these endpoints is on an approved RFC 10024 hybrid profile (DEC-003). Private PKI is in migration under DEC-005. Lead time to switch is short once browsers trust ML-DSA roots.
Obligations check	No applicable obligation requires post-quantum server authentication before 2031 (EO 14412 does not apply; register entry OBL-04 reviewed).
Interim treatment	Short certificate lifetimes; CA agility confirmed under QCI-4.7 test T-11.
Evidence references	QASI WEB-001, WEB-004, API-002; discovery evidence per QCI-T1, run August 12, 2026; browser trust-store status as of September 2026; obligations register OBL-04
Owner	Head of PKI
Approved by	CISO, risk appetite statement section 4
Decided on	September 18, 2026
Review date	March 18, 2027
Conditions for revisiting early	Any major browser ships ML-DSA server certificate support by default; a public CA offers publicly trusted ML-DSA or composite certificates; NIST IR 8547 finalizes with an earlier date.

Field	Entry
Linked exception	None; exposure is within appetite for the period.
Status	Open

COMMON MISTAKE

Writing the decision after the fact, when an 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.