

QUANTUM CORE INSTITUTE

Exception Register Template

Where third-party oversight is real or theatrical

Field	Value
Document ID	QCI-T3
Version	V1.2 – September 23, 2026
Applies to	QCI-4.3-01, QCI-4.3-02 (accepted risks and exceptions), QCI-7.3-01 (supplier exceptions), QCI-7.2-04 (response deadline); Practitioner Handbook chapter 8; QCI-M1 stage 4, Procure
Use	One register per organization, reviewed at least quarterly and on material triggers; top critical-supplier exceptions and decisions go in the governing-body insert under QCI-7.3-01 and QCI-8.1-01
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

QCI-4.3-02 sets what every accepted risk or operating exception must record: affected assets and requirements, rationale, exposure and residual risk, treatment, owner, approving authority, approval date, expiry, review triggers, remediation dates, and an exit or replacement strategy or a documented rationale where exit is infeasible. QCI-7.3-01 adds the supplier specifics: missed commitments, concentration and subservice dependencies, customer actions. This template holds both in one register, because an assessor asks for them together, and because an approved exception never lifts gate G70 (QCI-6.3-01).

WHAT THE ASSESSOR WILL ASK

Show me the exception register, not the success stories. An empty register at a large institution is its own finding. A supplier who has not answered by the QCI-7.2-04 deadline is an exception, not a pending item, and the exception does not pass G70.

2 Register columns

Column	Content	Rule
Exception ID	Sequential identifier.	Never reused.
Type	Vendor non-response; vendor inadequate roadmap; vendor no attestation; internal risk acceptance; agility proof gap.	One type per entry.
Supplier or system	Vendor name, or QASI system ID for an internal exception.	Must exist in the QASI vendor field or system list.
Annex G domain(s)	Domains affected.	At least one.
What was requested and when	Pack issued date; sections; follow-ups with dates.	Dates, not “recently”.
What was received	Nothing; partial answers; roadmap without dates; answers without attestation.	Quote the vendor where the answer is the finding.
Exposure and residual risk	Systems, horizons and QCI-5.3-01 exposure flags that depend on this item; residual risk after treatment.	Drawn from the QASI, not restated.
Treatment and remediation dates	The action that closes the exception, with owner and milestone dates.	Required (QCI-4.3-02).
Compensating controls	What limits the exposure meanwhile: segmentation, rotation, minimization, contract clause.	Required where feasible; “none” is an allowed and visible answer.
Exit or replacement strategy	Dual-source, replacement, or contractual milestone with consequence; where infeasible, the documented rationale and alternative treatment.	Required, or the infeasibility rationale (QCI-4.3-02).
Approved by	Name and role of the competent approving authority.	Must match the authority defined under QCI-4.3-01.

Column	Content	Rule
Approved on / expires on	Approval date and expiry date.	An exception without an expiry is a policy change that skipped governance. Expired or unapproved exceptions are escalated (QCI-4.3-02).
Review triggers	Events that reopen the exception before expiry: supplier change, missed milestone, vulnerability advisory, obligation deadline.	At least one.
Review evidence	Date and outcome of each quarterly review and each triggered review.	Every quarter, including the quiet ones.
Renewal decision	Explicit renewal before expiry, by whom, on what date; or closure.	Renewal is a decision, never a lapse.
Governing-body visibility	Included in the insert this quarter (yes/no), including cases with no feasible exit.	Yes for top exceptions on critical suppliers (QCI-7.3-01).

3 Worked entry

Column	Entry
Exception ID	EXC-014
Type	Vendor no attestation
Supplier or system	Identity provider (federation); QASI SSO-001
Annex G domain(s)	9 identity and access; 12 third-party
What was requested and when	Pack issued March 3, 2026; sections A to F; follow-ups April 7 and May 12
What was received	Answers to A, B, C. Vendor declines to sign attestation: “our counsel does not permit forward-looking statements.”
Exposure and residual risk	SAML signing on RSA-2048, hard-coded (rigid-component flag); 47 service certificates of unclear ownership (missing-ownership flag); audit logs with a 7-year verification horizon. Residual: forgery exposure on federation until ML-DSA signing is available
Treatment and remediation dates	Contractual milestone for ML-DSA signing option by Q4 2027 in renewal; owner: head of IAM; milestone: renewal signature, November 2026
Compensating controls	Certificate inventory reconciliation completed; token lifetime reduced to 8 hours
Exit or replacement strategy	Dual-source evaluation of a second identity provider scheduled Q1 2027
Approved by	CISO, under risk appetite statement section 4
Approved on / expires on	June 20, 2026 / December 20, 2026

Column	Entry
Review triggers	Supplier publishes an ML-DSA signing date; renewal terms change; any federation-signing vulnerability advisory
Review evidence	Q3 2026 review September 15: renewal negotiation in progress; no change
Renewal decision	Due before December 20, 2026; CISO
Governing-body visibility	Yes, Q2 and Q3 inserts; G70 held at 70 while open

COMMON MISTAKE

Letting a compensating control become the permanent answer. Temporary controls have a documented tendency to become permanent fixtures. The expiry date exists so that the register asks the question again, on a date, whether anyone wants it asked.