

QUANTUM CORE INSTITUTE

Discovery Evidence Acceptance Checklist

Deciding whether discovery output and vendor CBOMs are evidence

Field	Value
Document ID	QCI-T1
Version	V2.0 – September 23, 2026. Rebuilt on QCI-5.4-01 to 5.4-03.
Applies to	QCI-5.4-01 (discovery provenance), QCI-5.4-02 (reconciliation and dispositions), QCI-5.4-03 (vendor CBOM equivalence), QCI-5.1-02 (unknowns), QCI-5.3-01 (inadequate discovery provenance flag); Annex C question A2 and G4
Use	Once per discovery output and once per vendor-supplied CBOM, before any field it populates enters the QASI
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

A field in the QASI derived from a scanner or a vendor CBOM is evidence only if its provenance can be established. QCI-5.4-01 lists what the evidence reference must carry; QCI-5.4-02 requires conflicting evidence to be reconciled and dispositions recorded; QCI-5.4-03 sets the equivalent for a CBOM no tool produced. This checklist turns those three requirements into a decision an analyst makes in minutes and a record an assessor can retrieve. Output that fails is held as an input, not discarded, until the missing element is supplied or another evidence method covers the field.

WHY THE REQUIREMENT EXISTS

A scanner cannot tell you what it did not find. A silent rule and an absent algorithm produce the same output, and a valid schema proves nothing about completeness. The defence is to require the tool, or the vendor, to state what was examined and what was not, so that a coverage claim is checkable. QCI-5.4-02 says it directly: scanner success shall not establish inventory completeness.

2 The checklist, QCI-5.4-01

Complete one row per output. Every element must be present for the output to be accepted as evidence. Elements 1 to 6 describe the run; 7 and 8 describe how the organization used it.

#	Element	What to look for	Present ?	Where recorded
1	Tool and exact version	Product name and version string; for open source, the commit where the tool reports one. "Latest" is not a version.		
2	Materially relevant configuration or ruleset	The rule set, policy or profile the tool ran with, by name and version; exclusions configured by the operator.		
3	Examined scope and run date	Repository and commit, image digest, host, endpoint, or network range as appropriate; date and time of the run.		
4	Omitted scope and reason, or inability to report	Files, hosts or components skipped, each with a reason (unsupported type, unreadable, excluded by policy), or an explicit statement that the tool cannot report omissions.		
5	Stable finding ID and location	An identifier that survives re-runs, and a location per finding: file and line, host and port, certificate subject and serial, or component identifier.		
6	Output artifact location, digest algorithm and digest	Where the output file is retained; the algorithm (SHA-256 or equivalent) and the digest of the file as received.		

#	Element	What to look for	Present ?	Where recorded
7	Mapping to the QASI field	Which QASI record and field each relied-upon finding populates.		
8	Producer, reviewer, confidence or disposition, validation date	Who ran it, who reviewed it, the disposition (accepted, false positive, unresolved) and the date the field was validated.		

A digest establishes that the file cited is the file received. It does not establish who produced it or that the content is authentic; that is what elements 1, 2 and 8 are for.

3 Vendor CBOMs, QCI-5.4-03

A CBOM supplied by a vendor in answer to Annex C question A2 or G4 must meet the same scope, attribution, finding-location, integrity and review objectives. Where no discovery tool produced it, replace elements 1 to 3 with:

#	Element	What to look for
1v	Generation method	How the CBOM was produced: tool, manual compilation, build pipeline export.
2v	Schema and version	The interchange schema and version, for example CycloneDX 1.6; the organization records the schema and validates its mapping to the QASI, per Annex E S20.
3v	Authorized producer, production date, product and release scope	The named producer, the date, and the exact product releases and deployment models the CBOM describes.

Elements 4 to 8 apply unchanged. The receiving organization validates relevance to its own deployment: a CBOM for release 4.2 is not evidence for the release 3.9 the organization runs. Intellectual-property restrictions may change how evidence is accessed; they do not convert an unsupported claim into validated coverage.

4 Decision

Result	Action
All elements present	Accept. Record the evidence reference in the QASI with the elements. Record the tool's own figure for what it read, if it gives one, beside the reference, labelled scan reach (QCI-5.4-02). Scan reach never replaces the coverage metrics of QCI-5.1-03.
Element 4 absent and the tool cannot supply it	Accept the findings as evidence for the fields they populate, and record incomplete coverage for what the tool could not see. Raise the inadequate-discovery-provenance exposure flag (QCI-5.3-01) on the affected records until a second evidence method covers the gap, or record an operating exception under QCI-4.3-02.

Result	Action
Any other element absent	Hold. Do not populate QASI fields from this output. Request the missing element from the operator or, for a vendor CBOM, from the vendor through the Annex C process; nonresponse enters the exception process at the QCI-7.2-04 deadline.
Static, runtime, configuration or supplier evidence conflict	Hold the affected field. Reconcile under QCI-5.4-02 and record the disposition: which source prevails and why, false positives, and unresolved items with owner and due date. An unresolved conflict on algorithm, profile, trust dependency or key protection leaves the record outside validated coverage (QCI-5.1-02).
Findings contradict a validated owner statement	Hold and escalate to the system owner and technical reviewer. The QASI records the validated answer; the finding becomes a question for the next validation.

COMMON MISTAKE

Recording the tool's coverage percentage as QASI coverage. Scan reach is how much of a directory or range a tool read. Coverage under QCI-5.1-03 is 100 times validated critical records over the identified critical population, computed separately for systems and flows, with numerator and denominator published. They are different numbers with different denominators, and only the second one passes G60.

5 Freshness

Discovery evidence supports a validated record only while it is current. QCI-5.1-04 requires critical evidence no older than 90 calendar days unless a documented review within that period confirms unchanged configuration and continuing relevance. Record the review, or re-run the discovery, before the 90 days lapse; stale evidence does not support a gate or a maturity criterion.

6 Record

Keep the completed checklist with the output file it assesses, in the assessment pack under QCI-4.8-01: producer, reviewer, integrity controls, retention through at least the next annual assurance cycle, and access restrictions on sensitive inventories. The checklist, the file and its digest are what an assessor asks for when tracing a QASI field to its artifact.