AUGUST 2026

APPLIED QUANTUM

THE APPLIED QUANTUM CCF CBOM CONFORMANCE STATEMENT

What a cryptographic bill of materials must carry for each CCF layer to be computable

Version 1.0-RC – August 2026

Steve Vaile and Marin Ivezic, Applied Quantum

Disclosure: Applied Quantum provides post-quantum migration advisory services. This work is published openly under CC BY 4.0 and is computable without engaging Applied Quantum.

COPYRIGHT AND LICENSE

DISCLAIMER

This document is provided as professional guidance based on the authors' and Applied Quantum's practitioner experience and publicly available standards, regulations and industry research. It does not constitute legal, regulatory, financial or compliance advice. Organisations should consult qualified legal counsel, auditors and regulatory authorities for guidance specific to their jurisdiction, sector and circumstances.

The regulatory instruments, certification records, standards and vendor capabilities referenced in this document reflect the state of the landscape as of August 2026, and that landscape moves. Readers should verify current status against primary sources (regulators and supervisory authorities, NIST, EMVCo and PCI SSC, the CycloneDX specification, public certification listings, vendor documentation) before making decisions.

References to specific vendors, products or tools are for illustrative purposes and do not constitute endorsement.

This is a v1.0 release candidate: v1.0 final publishes in November 2026 after a pilot cycle. Open items are public on the roadmap at CCFramework.org, and corrections are published as dated entries on its errata page.

ABOUT THIS DOCUMENT

Document type	Normative conformance statement
Parent document	The Cryptographic Concentration Framework – Universal – v1.0-RC (August 2026)
Intended audience	CBOM producers and consumers, tooling vendors, and assessment teams verifying computability
Assumed knowledge	The Applied Quantum CBOM Profile (v1.0-RC or later) and CycloneDX 1.6/1.7
Scope	Which Profile fields CCF consumes, at which conformance level, for which layer. This document defines nothing itself.

Status	Version 1.0-RC – release candidate; v1.0 final November 2026 after pilot

VERSION HISTORY

Version	Date	Changes
1.0-RC	August 2026	First public release, as a release candidate; drafted through four external review rounds and a family-wide line-edit pass.
1.0-RC	7 September 2026	Layer 3 row states the CycloneDX 1.7 deprecation of signatureAlgorithmRef; Section 5 wording repaired.
1.0-RC	8 September 2026	Section 2 defines the assessment supplement as a logical record set; field requirements by layer and the missing-data table restored; uncertainty states aligned to the Universal's eight-state table; supplier response states aligned to the Profile enumeration. Prose revised throughout. No figure changed.

HOW TO USE THIS DOCUMENT

This statement is read with the Applied Quantum CBOM Profile, v1.0-RC or later, which defines every field named here, and with the CCF Universal Framework, whose layers set the requirements. It states only which fields CCF consumes, at which conformance level, for which layer.

ACCOMPANYING RESOURCES

The framework family publishes at CCFramework.org: the Universal Framework, the Payments and Financial Services extensions, the payments whitepaper, the CBOM Conformance Statement, the Technical Companion and the instruments, together with the public roadmap, the errata and corrections page, the provenance survey and the frontier-census methodology.

Every canonical figure in the family comes from the reference implementation, with ten canonical test vectors that fix each one exactly. Both are open under Apache-2.0 on the Applied Quantum GitHub, and any implementation that reproduces the fixtures is conformant.

The Applied Quantum CBOM Profile, the input data contract, publishes at CBOMProfile.org. The Applied Quantum PQC Migration Framework, whose sector taxonomy the extensions follow, publishes at PQCFramework.org. Practitioner background and adjacent analysis sits on PostQuantum.com, as further reading rather than a normative source.

TABLE OF CONTENTS

Requires the Applied Quantum CBOM Profile **v1.0-RC or later**, which defines every field named here. This document states only which fields CCF consumes, at which conformance level, for which layer. It defines nothing itself.

PURPOSE AND USE

This statement specifies what an assessment team must receive before it can compute and report each CCF output. It translates the Universal Framework into a practical data contract, distinguishing native CycloneDX fields, Profile properties and assessment facts that need a linked supplement. Its purpose is to prevent a technically valid inventory from being mistaken for a complete concentration or coverage assessment.

Inventory owners use this statement to scope a response to the Data Request. Tooling teams use it to implement output-specific validation. Assessment owners use it to state the achieved CCF and EC data levels and explain which results remain unavailable or qualified. The Universal Framework governs the calculations; the CBOM Profile governs property names, types and carriage.

1. SCOPE OF THE CONFORMANCE CLAIM

This statement defines the minimum input needed for CCF outputs. The conformance levels describe which layers become computable, not pass or fail. It is a consumer contract, not a replacement for the CBOM Profile or the CycloneDX base schema. A conformance claim identifies a service population, assessment date, exact Profile and method revision, achieved data level, EC marker and any limitations.

Data availability and assessment maturity are separate. CCF-3 does not mean that an assessment has reached M3, that the whole estate has been discovered or that its technical assertions have been independently verified. Conversely, a governed assessment can use a lower data level and report the outputs that level supports. The Universal Framework's M3 institution-reporting gate applies independently.

A claim may cover a declared subset, but that subset must be visible wherever the claim or resulting figures are reported. Missing applicable required data is a qualification, not an acceptable silently omitted field. A requested target level must not be presented as the achieved level merely because a questionnaire was issued.

2. REQUIRED EVIDENCE PACKAGE

The input is a **CBOM plus a linked assessment supplement**. A producer may deliver one BOM per service or a shared BOM with complete service mappings. A shared asset must not be duplicated simply to provide multiple service, path or evidence contexts.

The **assessment supplement** is the collective name for the service and scope register, the resolution and counting ledger, the relationship register, the evidence and determination records, the coverage and gap statement and the supplier-response register. These are logical records the Data Request already requires; no `appliedquantum:*` property is implied.

Package element	Minimum content
CBOM snapshot	Selected CycloneDX version; applicable native fields and Profile properties; stable record references; producer and snapshot identification
Service and scope register	Service owner, boundaries, included classes, applicable functions, target state and tolerance mapping
Resolution and counting ledger	Canonical asset identity, source aliases, service, layer applicability, primary unit, cohort cardinality and unresolved assignments
Relationship register	Ancestry and other reach edges; custody/generation origin; asset-to-path mapping; ordered hops and population segments where needed
Evidence and determination records	Claim-level source, date, deployment scope, E-code, limitations, conflicts and contextual judgements. Corroboration of a supplier attestation against a certification record is recorded as a separate attribute; the evidence basis stays E4
Coverage and gap statement	Per-service enumeration basis, observed and unobserved classes, numerator/denominator, owner and limitations

Package element	Minimum content
Supplier-response register, where used	Request scope, dates and full/partial grade. Response states use the Profile's `lineage:disclosureStatus` values: `disclosed`, `declined`, `pending`, `no-response`, `not-requested`. Silence after the deadline is `no-response`; explicit refusal and a deflected reply are `declined`, with "deflected" recorded in the register's reason field

The records do not require seven separate files or databases. They may be maintained in an assessment workbook, controlled tables or a linked evidence system. Their identifiers must allow the calculation to be reconstructed without guessing which record or revision was consumed.

The Profile does not currently contain dedicated properties for canonical cohort counts, complete ordered-hop topology, every generation-point relationship, all own-state conditions, service-specific criticality, or a full per-claim evidence model. This supplement carries those facts. Its fields are assessment fields, not newly registered `appliedquantum:*` properties.

3. CONFORMANCE LEVELS

The levels are cumulative for the applicable scope. All levels require a service mapping, the coverage qualification and an evidence record. Requirements apply by asset type and output, not universally to every CBOM component.

Level	Required content	Layers computable	Typical source
CCF-1	Profile Tier 1, plus `appliedquantum:pqc:vulnerabilityStatus`, plus `conc:serviceRef` and `conc:evidenceTier`, plus `pki:trustAnchorRef` and the path record's `negotiatedOutcome`	1, 3, 5	Existing discovery tooling with service mapping added
CCF-2	Adds `custody:*` and the five `conc:criticality*` booleans	1, 3, 4, 5, and flagged-only indices at every computable layer	Enrichment from custody inventories and risk determination

Level	Required content	Layers computable	Typical source
CCF-3	Adds `pedigree.ancestors`, `lineage:*` and `entropy:*`	All six	Vendor engagement and manual evidence chaining

Effective Coverage requires `path:pathId`, `path:counterpartyRef`, `path:counterpartyClass`, `path:counterpartyTargetState` and, wherever the class is `population`, `path:populationTargetPct`, at any level.

Coverage marker. Alongside CCF-1/2/3, an assessment states a separate marker for coverage data. **EC-0** means no path data and coverage not computable. **EC-1** means bilateral path records are complete. **EC-2** means multi-hop and population records are complete. The CCF level and the EC marker are independent claims, and a CCF-3 label is never read as implying coverage computability. An assessment without them still computes concentration. It cannot compute coverage.

The layer-2 index computes at CCF-1 with no supplier data, using the institution's own executing implementation families. The CCF-3 lineage and design fields feed reach. The outputs view below distinguishes these primary-unit indices from the advanced relationship analysis.

Level	Minimum additional resolution	Outputs enabled on the declared applicable population
CCF-1	Algorithm classification, executing implementation family, primary accepted trust anchor and observed protocol outcome, together with counted identities and service mapping	Layer 1 baseline; layer 2, 3 and 5 indices; largest shares; reach where relationships are independently available
CCF-2	CCF-1 plus custody-family/manufacturer context and assessed criticality tests	Adds layer 4, flagged-only views and relevant custody/manufacturer reach
CCF-3	CCF-2 plus generation-point identities and the advanced ancestry/design evidence and	Adds layer 6 and systematic advanced reach analysis, with any remaining membership uncertainty

Level	Minimum additional resolution	Outputs enabled on the declared applicable population
	relationship records	bounded and reported

A layer that is genuinely inapplicable does not prevent a level claim where its non-applicability is established. An applicable layer whose required identity is unknown must be qualified. If partial data supports a subset, report that output and its basis; an unresolved boundary counts as one unit at its known population and carries its uncertainty in reach.

CCF-3 does not require an assertion that every ancestor or design is known. It requires the generation-point data needed for its index and explicit treatment of the advanced relationship evidence, including residual unknown populations. A disclosure-status code without the generation/relationship inputs does not by itself establish CCF-3. Unknown membership may support a bounded result; unknown asset counts or unexamined applicable layers cannot be concealed as complete advanced resolution.

The claim should state the target, achieved scope and outstanding gaps. For example: "CCF-2 for the assessed card-authorisation population; EC-1 for bilateral key-establishment paths; whole-estate discovery coverage unknown for issued-device cryptography. Generation provenance requested; CCF-3 not claimed."

3.1 Interpretation of conformance levels

A CCF-1 assessment is finished work. It computes the three of six layers listed in the conformance table over the estate it covers and states which layers were computed. It is not a partial or failed CCF-3. The executing-family index at layer 2 is also available at CCF-1, as the outputs view shows.

A higher level is not a better risk result. Moving up usually makes the reported numbers worse because newly visible dependencies appear. An index that rises after a discovery improvement is working correctly. The level describes the data available, not the quality of the institution's risk position.

CCF-3 may be unreachable through no fault of the institution. Advanced lineage and key-generation evidence at layers 2 and 6 depends on supplier disclosure. An institution refused by every supplier can remain at CCF-2 despite having made the required requests. The framework then reports the disclosure response rate, which allows a reviewer to assess the institution's work separately from the supplier evidence gap.

The levels describe the ceiling on what can be measured, not whether what was measured is good. Data levels remain distinct from assessment maturity, and the M3 institution-reporting gate applies independently.

4. FIELD REQUIREMENTS BY LAYER

CCF layer	Fields consumed	Level
1 Algorithm	`algorithmProperties.primitive`, `.parameterSetIdentifier`, `.ellipticCurve` (`curve` accepted for 1.6); `cryptoProperties.oid`; `appliedquantum:pqc:vulnerabilityStatus`	CCF-1
2 Lineage *(the layer-2 index itself computes at CCF-1; these fields feed reach)*	`pedigree.ancestors`; `appliedquantum:lineage:evidence`, `:disclosureStatus`, `:cmvpCertificate`	CCF-3
3 Trust root	`certificateProperties.issuerName`, `.signatureAlgorithmRef` (deprecated in CycloneDX 1.7; `relatedCryptographicAssets` accepted in its place), `.notValidAfter`; `appliedquantum:pki:trustAnchorRef`, `:crossSignedBy`, `:trustAnchorOperator`	CCF-1
4 Custody	`relatedCryptoMaterialProperties.securedBy`; `appliedquantum:custody:platform`, `:firmwareFamily`, `:oemOrigin`, `:certificate`	CCF-2
5 Protocol	`protocolProperties.type`, `.version`, `.cipherSuites`; `appliedquantum:path:negotiatedOutcome`, `:observationWindow`	CCF-1
6 Key generation	`appliedquantum:entropy:sourceDesign`, `:generationDesign`, `:drbgSpecification`, `:esvCertificate`, `:evidence`	CCF-3
All layers	`appliedquantum:conc:serviceRef`, `:evidenceTier`; per-service `:discoveryCoverage` with `:discoveryMethod` and `:assessmentDate` (a document-level summary may be derived, never substituted)	CCF-1

CCF layer	Fields consumed	Level
Criticality flag	The five `appliedquantum:conc:criticality*` booleans	CCF-2

4.1 CCF-1 carriers and qualifications

Required information	Native or Profile carrier	Qualification
Counted identity and service	Native component identity; `appliedquantum:conc:serviceRef`; counting ledger	`bom-ref` alone is not canonical identity across sources; cohort counts and layer applicability are retained in the ledger
Algorithm and parameter identity	`cryptoProperties.assetType`, applicable algorithm attributes and `cryptoProperties.oid` where assigned	Require curve, mode and parameter fields only where they apply; record a canonical alternative when no applicable OID exists
Quantum vulnerability classification	`appliedquantum:pqc:vulnerabilityStatus`	An unknown classification is retained and prevents an unqualified layer-1 population claim for those assets
Executing implementation	Native component `bom-ref`, `type`, `name`, `version`, supplier/build identity and dependency/provision links	Resolve the executing family in the ledger; ancestry is a different relationship, not the primary-family identifier
Certificate and accepted anchor	Applicable certificate identity, validity and signature/subject-key relations; `appliedquantum:pki:trustAnchorRef` and operator context	Accept version-correct legacy or newer relation forms; preserve roles and accepted-path policy
Cross-signing and	`appliedquantum:pki:crossSignedBy`	Absence of cross-

Required information	Native or Profile carrier	Qualification
alternatives	where present; relationship/policy supplement	signing is not the same as failure to investigate it; alternative-path effects are failure-mode-specific
Observed cryptographic outcome	`appliedquantum:path:negotiatedOutcome`, `:observationWindow`; relevant native protocol fields	Capability-only configuration is not an observed layer-5 result
Evidence	`appliedquantum:conc:evidenceTier` plus more specific records	Component defaults do not replace material per-claim exceptions

For CycloneDX 1.7, certificate `relatedCryptographicAssets` is an array of typed reference objects. It is not a simple string alias for `signatureAlgorithmRef`. The supported 1.6/1.7 mapping must preserve the distinction between certificate signing and subject public-key roles. Native `securedBy.algorithmRef` refers to an algorithm, not a hardware-module identity. `securedBy` remains present and is not deprecated in CycloneDX 1.7.

4.2 CCF-2 carriers and qualifications

Required information	Carrier	Qualification
Custody platform and firmware family	Native custody component plus `appliedquantum:custody:platform`, `:firmwareFamily`	Product branding is not sufficient family evidence
Manufacturer origin	`appliedquantum:custody:oemOrigin`	An undisclosed cloud module is retained as a boundary, not relabelled as its provider
Applicable certificate reference	`appliedquantum:custody:certificate` where such validation exists	No fictitious certificate is required where none exists;

Required information	Carrier	Qualification
		disclose the absence and evidence relied upon
Criticality test 1	`appliedquantum:conc:criticalityDerivesKeys`	Service/key-owner determination
Criticality test 2	`appliedquantum:conc:criticalityAuthorizesIrreversible`	Service/key-owner determination
Criticality test 3	`appliedquantum:conc:criticalityNotRevocable`	Requires the relevant service tolerance
Criticality test 4	`appliedquantum:conc:criticalityPastHorizon`	Requires the applicable horizon and validity context
Criticality test 5	`appliedquantum:conc:criticalityNoEquivalent`	Requires the operational-equivalent assessment

Unknown criticality is not false. Retain unresolved counts and qualify any flagged-only result. A single asset serving several services may require different determinations in the supplement; the same component-level boolean must not overwrite those differences.

4.3 CCF-3 carriers and qualifications

Required information	Carrier	Qualification
Known implementation derivation	`pedigree.ancestors` on implementation components, with relevant commits/patches/provenance	Nested chains remain distinct from direct multi-parent derivation; mere use is a dependency, not

Required information	Carrier	Qualification
		ancestry
Ancestry evidence and disclosure context	`appliedquantum:lineage:evidence`, `:disclosureStatus`; `:cmvpCertificate` where applicable	Missing/partial ancestry and deflected replies require an explicit supplement record
Generation point and asset origin	Native component/service identity and relationships, or the generation-origin ledger	No dedicated Profile generation-point property exists; current custody is not proof of generation origin
Entropy and generation design	`appliedquantum:entropy:sourceDesign`, `:generationDesign` where applicable	Broad classes and shared certification profiles must not be represented as established common implementation identity
Deterministic generator and validation	`appliedquantum:entropy:drbgSpecification`, `:esvCertificate` where applicable	Absence of an applicable ESV record does not justify inventing a certificate
Design evidence and reach	`appliedquantum:entropy:evidence` plus design/point relationships and candidate exclusions	Use evidenced or bounded reach; identify a bounded design and the basis for its bound

Native ancestry and design fields do not automatically determine reach. Reach also needs the applicable asset population, relationship relevance to the failure mode, evidence of retained components and a reasoned treatment of possible membership. These facts are retained in the assessment supplement.

5. SERVICE MAPPING, CUSTODY AND NEGOTIATED OUTCOMES

`conc:serviceRef` is the field most likely to prevent a first assessment from proceeding. Bills of materials are organised by system, while CCF computes per important business

service. The mapping exists in the operational resilience function but not in the inventory. It must therefore be included in the assessment input.

`custody:firmwareFamily` and `custody:oemOrigin` are the resolution step most often omitted. A product name is not sufficient. Two products in one firmware family are one dependency, and rebadging is invisible without the manufacturer's origin.

`path:negotiatedOutcome` must not be substituted with `cipherSuites`. Capability and negotiated outcome differ on most cross-institutional paths, and layer 5 measures the outcome. Substituting capability reports a materially better position than the institution holds.

6. EFFECTIVE COVERAGE DATA MARKERS

EC markers describe the coverage data supplied. They do not certify that the percentage is high or that the deployment is secure. CCF indices may be available without a computable EC result. EC-0 reports "not computable", never 0%; an exact 0% over a mapped population is a computed result.

Marker	Data position	Permitted coverage reporting
EC-0	Target state, population or required path/counterparty relationships are insufficient	EC is not computable for that scope; report known observations and gaps separately, not a fabricated 0%
EC-1	A supported asset-to-path population, target definition, own-state and bilateral counterparty state for the declared function	Bilateral or wholly internal coverage for that scope; qualify any unobserved states or excluded topology
EC-2	EC-1 plus the required multi-hop, multi-path and population relationships, segment/cardinality and joint-state evidence or bounds	End-to-end coverage across the declared topology, with explicit treatment of unknown states and population overlap

EC-2 is not mandatory for a service whose complete relevant architecture is genuinely bilateral or internal. Do not invent hops or populations to obtain a higher marker. Conversely, a service requiring several hops cannot be described as end-to-end covered solely because its first bilateral connection is at target.

The applicable Profile fields are `path:pathId`, `:negotiatedOutcome`, `:observationWindow`, `:counterpartyRef`, `:counterpartyClass`, `:counterpartyTargetState`, `:counterpartyStateReason`, `:populationTargetPct` and `conc:serviceRef`, with the full `appliedquantum` prefix. Target definitions, own-state, required hop ordering, all-path asset mapping, population denominators and overlap evidence are supplementary records. Internal paths omit external counterparty fields rather than using invalid placeholder values.

`pathId` is single-valued per carrier. Assets with several paths use appropriate native dependency references or the relationship ledger. Distinct state records have unique `bom-ref` values even when their logical path ID is the same. A single scalar path ID is not a complete topology model.

When a hybrid is accepted by the target, retain the three-condition determination in Universal C.6. An unverified combiner or fallback policy receives no confirmed target-state credit. Do not write `hybrid-unverified` into `migrationStatus` or a boolean property: it is an assessment state, not one of those Profile enumerations.

7. MISSING DATA AND VALIDATION

Condition	CCF treatment
`pedigree.ancestors` absent, `lineage:disclosureStatus` is `declined`, `pending` or `no-response`	Layer-2 index unchanged – it computes over the institution's own executing families at CCF-1. The affected unit widens every reach bound it can't be excluded from, and the spread is reported and put to the supplier.
`entropy:*` absent	Layer 6 not computed. Recorded as not assessed, never as diversified.
Target state undefined for a service	Effective Coverage not computable. Never computed against an implicit definition.
Recoverability or consequence-threshold facts absent	Tolerance result recorded Not assessable, never Pass. The failure-impact determination cannot run without them.
`conc:criticality*` absent	Flagged-only indices not computed. The asset-count weighting bias is then declared without a compensating view, which weakens but does not invalidate the assessment.

Condition	CCF treatment
`path:*` absent	Effective Coverage not computed. Concentration remains computable.
`conc:serviceRef` absent	Nothing is computable. The assessment cannot proceed.
`conc:discoveryCoverage` absent	The assessment proceeds; every figure is published as coverage-unknown, which a reviewer should treat as a material limitation.
Hybrid combiner or fallback behaviour not establishable for a path	Path recorded `hybrid-unverified` and counted below target state, per Universal Framework C.6. Never read as sound.

The Universal Framework's A.7 names eight status states: not assessed, not applicable, excluded, bounded, unresolved boundary, hybrid-unverified, unknown coverage and not assessable. Each condition above maps to one of these states. An assessment reports the marker beside the figure it qualifies.

Absence is never treated as a favourable value. A layer recorded as not assessed is never counted as diversified, and that rule is what prevents thin discovery from producing a flattering result.

Accept incomplete submissions with a gap register so the assessment can proceed on supported evidence. Acceptance of a submission is not acceptance of an unqualified conformance claim. A missing applicable input prevents the unsupported output or requires an explicitly qualified scope or bounded reach.

Distinguish non-applicability, unobserved state, unresolved identity, supplier non-disclosure and an unknown population. These have different implications. A missing certificate reference may be legitimate where no validation exists; a missing generation point cannot be replaced by a fictional certificate; an unobserved population cannot be entered as a count of zero.

The validation record must separately state: base-schema result; Profile property/structure result; reference and carrier checks; and output-specific consumer sufficiency. Do not report a single "valid" label as proof that all four have passed. Record the exact validators, revisions, tests not run and manual review needed.

8. DISCOVERY COVERAGE STATEMENT

Each assessed service must carry a coverage statement identifying the independently enumerated scope, counted classes, numerator, denominator, unquantified classes, discovery methods, observation dates and accountable owner. The native service record may carry `appliedquantum:conc:discoveryCoverage` as a decimal fraction, while the detailed statement preserves its meaning.

Report the coverage of the enumerated perimeter and the completeness limitation separately. For example, "920 of 1,000 enumerated certificate/configuration assets observed; embedded firmware keys unquantified" supports 92% coverage of that perimeter. It does not support 92% of the full cryptographic estate. Where an independently counted population has no observations, its observed coverage is zero; where the population is unknown, no numerical completeness percentage is asserted.

Discovery coverage and Effective Coverage are different quantities. The former concerns what was inventoried; the latter concerns which assessed assets meet the service target across their paths. A 100% EC result over an incompletely discovered subset is not a claim that the whole service is protected.

9. REPORTING

Every CCF output states the conformance level, the discovery coverage and the evidence-tier distribution across the assets over which it was computed.

The disclosure response rate is a required figure wherever lineage disclosure requests were issued, and its absence at CCF-2 or above is itself reported. Full plus partial disclosures over requests issued, per the Supplier Lineage Disclosure Request's grading, Sections A to C only.

The response rate distinguishes an institution held below CCF-3 by supplier refusal from one that never issued a request.

A figure computed at CCF-1 over 40% of an estate is a different result from one computed at CCF-3 over 95%. Reporting both in the same format without those qualifiers misstates the position and prevents comparison between institutions.

10. RE-PERFORMANCE AND AUDIT EVIDENCE

Retain the original input snapshots and all transformations needed to reproduce the result: canonical identity aliases, asset weights, applicable populations, primary assignments, relationship edges, candidate exclusions, evidence references, criticality flags, target definitions, state windows, calculation version and determinations. Do not reconstruct these records only after a finding is challenged.

For each quoted CCI, a reviewer must be able to recover its denominator and primary-unit counts. For reach, the reviewer must be able to identify the named domain or bounded node and its known/possible members. For EC, the reviewer must be able to trace counted assets to required paths and functions, including joint population state. For a tolerance conclusion, the reviewer must recover the operational assumptions and threshold rather than infer them from the numerical score.

The Model Documentation Pack records validation and review. The Determination Log preserves judgement and reversals. A conformance statement is complete only when its qualifications survive into the corresponding heat map and board report.

For audit purposes, the conformance level is a population-completeness claim about which data classes exist for the estate under audit. Per-value evidence tiers form the basis-quality record: they state whether values were observed, confirmed, declared, attested or inferred, so reliance can be graded accordingly. The determination log provides the judgement trail needed for re-performance. Per-service coverage fractions and the named uncertainty states disclose the scope limitations.

As PQC migration enters SOX ITGC scope, audit teams can consume a conformant bill of materials as an ITGC or SOC 2 evidence structure. The framework certifies nothing. It makes the institution's claims testable.

RESOLVED AT V1.0-RC

1. Resolved in the prior edition: Effective Coverage has a separate EC-0/1/2 marker, stated in Section 3 and mirrored in the Data Request.
2. The disclosure response rate is a required reported figure wherever lineage disclosure requests were issued, with its absence at CCF-2 or above itself reported, per Section 9 – mirroring the Universal Framework's rule.