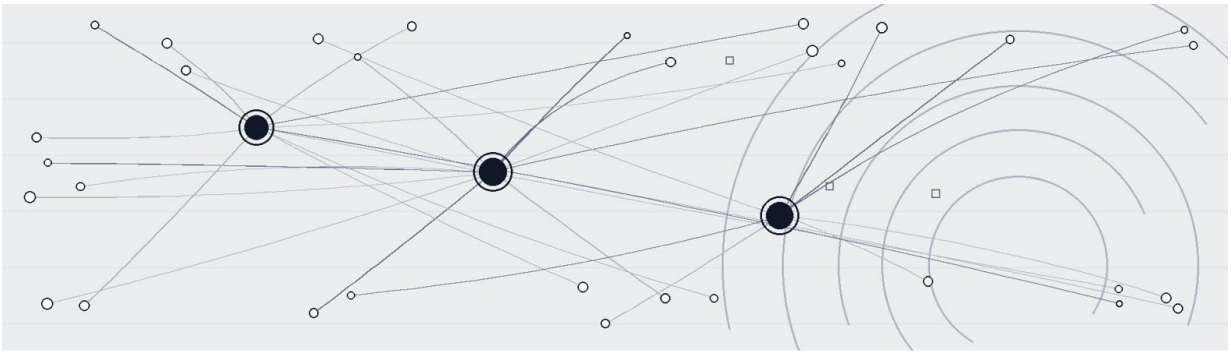
AUGUST 2026

APPLIED QUANTUM

THE APPLIED QUANTUM CCF INSTRUMENT DATA REQUEST SPECIFICATION



What second line asks first line for, and what a complete response looks like

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

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. This work is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). You are free to share and adapt this material for any purpose, including commercial use, provided you give appropriate credit to Steve Vaile, Marin Ivezic and Applied Quantum, link to the licence, and indicate any changes made.

Licence details: https://creativecommons.org/licenses/by/4.0/

The reference implementation and canonical test vectors publish separately under Apache-2.0 on the Applied Quantum GitHub. Neither licence reads onto the other.

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	CCF instrument – data request specification
Parent document	The Cryptographic Concentration Framework – Universal – v1.0-RC (August 2026)
Intended audience	Second-line analysts issuing Phase 2 data requests, and the first-line responders answering them
Assumed knowledge	The Universal Framework’s Phase 2 and its evidence standards
Scope	What second line asks first line for, and what a complete response looks like: request structure, response deadlines, named non-response consequences, and the accountable individual on the coverage statement.

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	CCF-1 certificate row states the CycloneDX 1.7 deprecation of signatureAlgorithmRef.
1.0-RC	8 September 2026	Field tables by level restored; supplier response states aligned to the Profile enumeration; the assessment supplement named. Prose revised throughout. No figure changed.

HOW TO USE THIS DOCUMENT

This instrument executes Phase 2 of the CCF Universal Framework. Issue it as written, state the response deadline and the named non-response consequence, and grade what comes back against the Universal's evidence standards.

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.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

TABLE OF CONTENTS

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Used in Phase 2 of the CCF Universal Framework v1.0-RC. Field definitions are in the Applied Quantum CBOM Profile v1.0-RC or later. Which fields at which level is in the CCF CBOM Conformance Statement.

PURPOSE AND USE

This instrument specifies the evidence an assessment team requests and the conditions under which a response can be used. It is intended to reduce repeated, incomplete requests and make responsibilities clear before collection begins. The response supplies the inputs for concentration, reach, criticality and coverage calculations; it does not itself determine that the service meets its tolerance.

Use it after the Universal Framework's scoping phases, together with the Conformance Statement's field mapping and the Profile's property definitions. Supplier-held provenance is requested through the separate Supplier Lineage Disclosure Request. Material gaps and disputed interpretations pass into the Determination Log rather than disappearing during data preparation.

1. REQUEST OWNERSHIP AND USE

The assessment owner in second line sends this specification to the cryptographic inventory owner in first line after the charter and service boundary have been agreed. It is a specification, not a questionnaire. The inventory owner coordinates the technical response, but does not answer every question alone. Service and key owners provide criticality and operational facts; architecture provides dependency interpretation; third-party risk obtains supplier-held provenance. The request should make that allocation explicit so that missing answers are not mistaken for a discovery-tool limitation.

Issue one complete baseline request describing the intended output. Repeated partial requests encourage the recipient to supply only the minimum and wait for the next request; a first assessment then takes two quarters instead of one. Prioritise the response into what is already available and what needs engineering or supplier follow-up. The assessment may proceed on supported data, with missing outputs qualified. It must not wait indefinitely for a nominally complete submission or call an incomplete response complete merely to meet a reporting date.

State the deadline and the treatment of late items in the request. An item outstanding at the deadline is recorded as absent, and no missing value improves a reported figure. Name the role informed of outstanding items at the deadline and state that the assessment proceeds and reports the gaps rather than waiting. Further escalation

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

follows the institution's governance. A model escalation path is: items unresolved ten working days past the deadline go to the accountable executive named in the charter.

The authoritative field mapping is the CBOM Conformance Statement; the Profile defines the fields themselves. This request adds delivery, ownership and acceptance requirements. Agree the exact editions and format before extraction rather than asking several teams to produce incompatible versions.

2. STANDARD REQUEST TEXT

Cryptographic Concentration Assessment – Data Request

To: [cryptographic inventory owner]

From: [assessment owner, second line]

Response required by: [date]

Assessment reference: [ref]

This request supports the cryptographic concentration assessment authorised under [charter reference]. It covers [n] important business services, listed in Annex 1.

What is requested. A cryptographic bill of materials per service, conforming to the Applied Quantum CBOM Profile at level [CCF-1 / CCF-2 / CCF-3], together with a coverage statement per Section 4 below and an evidence tier per value per Section 5.

What happens to missing items. Values not supplied by the deadline are recorded as absent. An absent layer is reported as not assessed, never as diversified, and the assessment states which layers could not be computed and why. At the deadline, [named role, per the assessment charter] is informed of outstanding items and the assessment proceeds on what was received. Values supplied without an evidence tier are graded E5 (inferred).

What is not requested. Key material, secrets, or any value whose disclosure would itself create risk. The assessment requires metadata about cryptographic assets, never the assets themselves.

Questions and scope disputes to [assessment owner] before [date minus 2 weeks], not at submission.

3. FIELDS REQUESTED, BY CONFORMANCE LEVEL

3.1 Baseline records

Provide a snapshot identifier, producer, production date, declared CycloneDX version, Profile revision and inventory source references. Retain unique `bom-ref` values and any mapping to enterprise identifiers. The response must allow the assessment to distinguish counted assets from algorithm catalogue entries, implementation components and path-state descriptions.

For each service, provide its owner, boundary, included asset classes, known population, supporting systems and applicable cryptographic functions. State which systems or classes were not examined and which populations remain unquantified. A system-level inventory must be mapped to services before service-level figures are calculated; the first usable mapped subset may be assessed while other mappings are completed.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

The supplement must include the counted-asset record, canonical aliases, layer applicability, cohort cardinality, primary assignments where known, and relationships not fully encoded by the current Profile. Provide generation origin separately from current key custody. Preserve multi-service and multi-path relationships without duplicating the counted asset.

3.2 CCF-1

The following fields are required at CCF-1.

Field	Per
`cryptoProperties.assetType`	asset
`algorithmProperties.primitive`, `.parameterSetIdentifier`, `.ellipticCurve` (`curve` accepted for 1.6), `.mode`	asset
`cryptoProperties.oid`	asset
`certificateProperties.subjectName`, `.issuerName`, `.serialNumber`, `.signatureAlgorithmRef` (deprecated in CycloneDX 1.7; `relatedCryptographicAssets` accepted in its place), `.notValidBefore`, `.notValidAfter`	certificate
`protocolProperties.type`, `.version`, `.cipherSuites`	protocol asset
`appliedquantum:pqc:vulnerabilityStatus`	asset
`appliedquantum:pki:trustAnchorRef`, `:crossSignedBy`, `:trustAnchorOperator`	certificate
`appliedquantum:path:negotiatedOutcome`, `:observationWindow`	path
`appliedquantum:conc:serviceRef`	asset
`appliedquantum:conc:evidenceTier`	value

`oid` is not optional. The same curve appears under three names across tools, and counting those names as distinct dependencies understates concentration. `serviceRef` is the field most likely to be missing because inventories are organised by system and the

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

assessment computes per service. Where that mapping does not exist, build it in Phase 2. Nothing downstream proceeds without it.

Native algorithm fields apply only to the relevant asset type. A mode or curve is not required for every algorithm. Inventory and cryptography engineering provide the applicable `cryptoProperties`, normalised algorithm and parameter identifiers, and vulnerability classification.

Application and platform engineering provide native component identity, version, supplier/build information and dependency/provision links sufficient to resolve the executing implementation family. PKI and the service owner provide the certificate-signature and subject-key roles, primary accepted anchor, cross-signing and verifier-policy context. Network and application engineering identify the affected endpoint/configuration population for the observed protocol outcome. The inventory owner and source contributors provide service mapping, evidence defaults and per-claim exceptions, source dates and deployment scope.

For CycloneDX 1.7 certificate relationships, use the correct `relatedCryptographicAssets` relation-object structure or the supported legacy mapping. Preserve certificate-signature and subject-key roles. A reference to an algorithm is not a reference to the HSM that stores its key.

3.3 CCF-2

CCF-2 adds the following fields.

Field	Per
`appliedquantum:custody:platform`, `:firmwareFamily`, `:oemOrigin`, `:certificate`	custody platform
`appliedquantum:conc:criticalityDerivesKeys`	asset
`appliedquantum:conc:criticalityAuthorizesIrreversible`	asset
`appliedquantum:conc:criticalityNotRevocable`	asset
`appliedquantum:conc:criticalityPastHorizon`	asset
`appliedquantum:conc:criticalityNoEquivalent`	asset

`firmwareFamily` and `oemOrigin` usually require supplier contact. Recording the product name does not answer the request for family and origin. Two products in one firmware family are one dependency, and rebadging is not visible without the manufacturer. Provide custody component identity and the source of each firmware-family and

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

manufacturer claim. If a managed service conceals the underlying module, identify the visible service and leave unknown sublayer identities unresolved rather than filling them with the provider's name. Supply the certificate reference where applicable.

The five criticality tests are determinations, not discoveries. The service or key owner answers them, not a tool. Retain the applicable tolerance, migration horizon and reasoning. Unknown criticality is not false; retain unresolved counts. Where an asset supports several services with different answers, supply asset-by-service records in the supplement.

The same routing applies to the failure-impact facts consumed in Phase 6. The service owner supplies affected functions, service effect, recovery options and times, operational evidence, and relevant confidentiality/integrity consequence thresholds. The assessment owner challenges those facts. A numerical concentration score does not supply them.

3.4 CCF-3

CCF-3 adds the following fields.

Field	Per
`pedigree.ancestors`	implementation component
`appliedquantum:lineage:evidence`, `:disclosureStatus`, `:cmvpCertificate`	implementation component
`appliedquantum:entropy:sourceDesign`, `:generationDesign`, `:drbgSpecification`, `:esvCertificate`, `:evidence`	key generation point

No additional data is collected specifically for reach. Lineage and design responses graded through the Supplier Lineage Disclosure Request populate the reach edges of Universal C.3.2 directly. Both depend on supplier disclosure, so issue the Supplier Lineage Disclosure Request in the same week as this request. Supplier replies take weeks, and the disclosure response rate is itself a reported figure.

Provide known implementation ancestry in `pedigree.ancestors` on implementation components, preserving nested chains, genuine multi-parent derivation and evidence of relevant divergence. Use dependencies for components merely bundled or called. Include the ancestry evidence, disclosure status and applicable certificate references.

Provide the identified generation point for each applicable key or homogeneous key cohort and the link to its generation origin, together with the available entropy and generation-design fields. A current custody location is not sufficient. A broad class or

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

common certification profile must be labelled as class/profile evidence, not as a shared design identity.

Supplier-held gaps should be routed through the Supplier Lineage Disclosure Request. Supply the response register, including requests not yet issued, pending deadlines, usable disclosures, explicit refusals, deflections and silence. Do not substitute the number of questionnaires sent for the number of dependencies resolved.

Use the Profile's `lineage:disclosureStatus` values: `disclosed`, `declined`, `pending`, `no-response` and `not-requested`. Silence after the deadline is `no-response`. Explicit refusal and a deflected reply are `declined`, with "deflected" recorded in the response register's reason field, not as a new enumeration value.

3.5 Effective Coverage

The following fields are required at any level where coverage is in scope.

Field	Per
`appliedquantum:path:pathId`, `:counterpartyRef`, `:counterpartyClass`, `:counterpartyTargetState`; `:populationTargetPct` where the class is `population`	path

Coverage data is marked EC-0, EC-1 or EC-2 per the Conformance Statement, independently of the CCF level. Concentration is computable without these coverage fields; Effective Coverage is not.

For each service/function in the coverage scope, provide the approved target definition, own-state facts, relevant asset-to-path mappings, observed outcomes and counterparty states. For multi-hop or multi-path cases, include the required hop relationships and relevant fallback paths. `pathId` remains single-valued per carrier; use native links or the relationship supplement for several paths.

Use the Profile's path properties for the state records: `pathId`, `negotiatedOutcome`, `observationWindow`, `counterpartyRef`, `counterpartyClass`, `counterpartyTargetState`, `counterpartyStateReason`, and `populationTargetPct` where applicable. These require the `appliedquantum:path:` prefix in the actual CBOM. Preserve service context with `conc:serviceRef`.

For populations, state the denominator, date, segmentation, measurement method and overlap evidence across required conditions. Several marginal percentages cannot be assumed to identify the same ready devices or users. Supply joint observations or the information needed to calculate explicit bounds.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Where a service's target state accepts hybrid constructions, assess its paths against Universal C.6's soundness test. Supply the combiner, binding and fallback evidence needed for that determination. A path whose combiner or fallback behaviour cannot be established is recorded `hybrid-unverified` and counts below target. An unsupported "hybrid deployed" status is not an end-to-end coverage result.

Internal-only functions have no external counterparty entries. Their coverage depends on their own relevant cryptographic state and paths. Unknown or unquantified coverage scope must not be reported as 0% readiness; zero is a supported numerical finding only on an identified population.

4. THE COVERAGE STATEMENT

The statement qualifies every subsequent result. It describes what the data represents, not simply what a tool returned. Each service requires:

1. **Coverage figure.** The fraction of the service's cryptographic estate the submission represents.
2. **Enumeration method.** How the estate denominator was established.
3. **Observable perimeter.** Which asset classes the discovery method can and cannot see.
4. **Unobserved classes.** Named individually, not aggregated into a residual.
5. **Accountable individual.** The named owner of the coverage claim, who answers for it in Phase 6 challenge.

Report two quantities: coverage of the enumerated estate and completeness by asset class. A figure scoped to one tool's observable classes is never labelled whole-estate coverage.

Challenge the method behind the claim, not the percentage alone. A 92% figure derived from certificate lifecycle tooling is a claim about certificates. Application-embedded keys, key material inside custody platforms and firmware-resident cryptography are outside that tool's perimeter; they are not part of the remaining 8%.

For classes the method cannot observe, record coverage as unknown, not zero. "We cannot see application-embedded keys" states the method's perimeter. "We found none" asserts a finding the method could not make.

Standard response format:

```
Service: [name]
Coverage: [n]% of enumerated estate
Enumeration method: [how the denominator was built]
Observable: [asset classes the method sees]
Not observable: [asset classes it does not – named]
```

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

```
Coverage for unobservable classes: unknown
Accountable for this statement: [name, role]
```

Retain the supporting detail with the statement: service identifier and boundary, included functions, enumeration sources, observed numerator and enumerated denominator with their unit, observable but unobserved counts where independently known, reasons for unobservable or unquantified classes, whole-estate completeness, enumeration and observation dates, known exclusions and aliases, and evidence references to the retained snapshot.

A response observing 920 of 1,000 enumerated certificate/configuration assets supports a scoped 92% figure. It does not establish the size of an embedded-key estate that was never enumerated. A known population with no observations has zero observed coverage; an unknown population does not have zero assets.

The assessment owner challenges the enumeration method, source completeness and treatment of inaccessible classes. Improving the method can change a result in either direction. The response should preserve the previous scope where available so the next assessment can distinguish discovery from deployment change.

5. EVIDENCE TIERS AND HANDLING

Every supplied value is graded. Untiered supplied values default to E5; a missing field remains absent rather than acquiring an invented value.

Tier	Basis
E1	Runtime observed
E2	Binary confirmed
E3	Inventory declared
E4	Vendor attested
E5	Inferred

Tier is recorded per value, not per document. A submission may carry E2 algorithm data and E5 entropy data. Record the specific source and its relevance, date and deployment scope, and identify ungraded supplied claims for review.

Component-level `conc:evidenceTier` and namespace overrides are defaults. Provide material claim-level exceptions in the supplement. Where a supplier attestation is

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

corroborated against a certification record, record the corroboration as a separate attribute; the evidence basis stays E4. A supplier's engineering answer corroborated by its own security policy is not upgraded to E3. Contradictory sources must be preserved for determination.

Do not supply private keys, symmetric secret values, random-generation seeds or other operational secrets. Public certificate records, permitted public fingerprints and metadata are acceptable where authorised. Detailed topology and supplier provenance must still follow the institution's information-handling rules.

Store the response in an approved access-controlled location, retain its integrity/snapshot identifier, and apply an appropriate retention period. Evidence references should remain accessible to authorised reviewers without copying unnecessary sensitive detail into the board report. Unexpected secret material must be handled through the institution's incident and secure-deletion procedures; a public certificate is not, merely by being a certificate, an incident.

6. RECEIPT AND ACCEPTANCE

The assessment owner records receipt, format checks, reference checks, coverage qualifications and unresolved items. A complete response meets all six conditions:

1. Every scoped service has a submission or a stated reason why it does not.
2. Every asset carries `serviceRef`.
3. Every value has an evidence tier, or the assessment owner has knowingly graded it E5.
4. A coverage statement per Section 4 is present, with the enumeration method, named unobservable classes and accountable individual.
5. Fields required at the requested level are present or recorded as unavailable, with the reason.
6. No key material or secrets have been supplied.

Anything short of these conditions is accepted with the gaps recorded, not rejected. Preserve missing applicable fields and their owners in the gap register. A submission containing key material is a security incident. State the prohibition in the request and check for it on receipt; Section 5 specifies handling requirements.

Acceptance means the response can be used with its stated limitations. It does not mean the requested CCF level has been achieved. Record the achieved scope and EC marker only after the consumer-sufficiency checks. Obtain corrected files without destroying the original submitted snapshot or the history of material changes.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

7. COMMON RESPONSE FAILURES

Failure	How to handle
Coverage supplied as a bare percentage	Return for method and perimeter. Do not proceed on an unqualified figure.
Product name supplied where firmware family was requested	Record as unresolved at layer 4 and route to supplier contact. Do not accept as resolution.
Supported cipher suites supplied where negotiated outcome was requested	Record layer 5 as capability-only. It cannot support a coverage figure.
`serviceRef` absent	Assessment cannot proceed. Escalate to the accountable executive rather than substituting a system-level mapping.
Criticality tests answered by the inventory team	Re-route to the service or key owner. These are determinations, and the inventory team lacks the facts.
Response arrives without tiers	Grade everything E5 and state that the confidence is a consequence of the submission, not of the estate.
Default false values in unanswered fields	Restore unknown status and investigate the effect on flags or coverage
Repeated single-valued `pathId` or duplicate assets per path	Replace with proper relation records and re-run de-duplication
Certification cited as proof of lineage	Extract any actual provenance claim; otherwise retain the ancestry gap
A received deflection recorded as supplier silence	Correct the response register; preserve the reply and its actual content

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

ANNEX 1 – REQUEST SCOPE RECORD

Service	Owner	Functions and asset classes	Included systems/issued estates	Target CCF / EC scope	Tolerance/target references	Response owner
[service]	[owner]	[scope]	[systems]	[target]	[references]	[owner]

The completed scope record is part of the assessment charter or its controlled annex. Changes during collection require approval and a recorded effect on comparability, rather than an unrecorded reduction of the denominator.

The records listed in this request form the assessment supplement.

RESOLVED AT V1.0-RC

Two questions carried from v0.9 review, closed August 2026.

1. The request names its deadline and its non-response consequence in its own text, per Sections 1 and 2. Escalation mechanics beyond that naming stay with the institution's governance, with a one-line model path offered and nothing more.
2. The coverage statement names an accountable individual, per Section 4. That figure is challenged in validation more often than any other, and someone has to answer for it.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.