

RESEARCH PAPER

When Evidence Can Be Reused

A decision test for reusing CMMC evidence without detaching it from scope, time, responsibility, or reviewer purpose.

STATUS	LAST REVIEWED	RESEARCH LANES	CLAIM REGISTER
Current	August 13, 2026	Evidence · Mechanism · Principles · Evaluation	V-04 · V-07 · C-05 · C-06 · C-16

Current CMMC 20X reuse proposal as of August 13, 2026. It is a design for public evaluation and does not establish assessment acceptance, contracting eligibility, legal reliance, or a Government-approved reuse rule.

Evidence reuse sounds efficient because the same file often appears relevant to several reviews. Relevance is only the first test. The harder question is: **under which conditions does prior evidence still support the present claim?**

A policy document may support several assessment objectives. A provider report may apply to hundreds of customers. An identity export may populate an SSP, readiness review, and assessment package. Reuse can reduce collection and reconciliation work. Careless reuse can also amplify one stale, partial, or mis-scoped record across many decisions.

CMMC 20X therefore treats reuse as a recorded decision. The evidence remains connected to its source, scope, time, responsibility, limits, and prior review. The receiving party states the new purpose and confirms that the old record is fit for that purpose.

Reuse has several meanings

Policy should distinguish operations that are often grouped under one word.

REUSE OPERATION	EXAMPLE	REQUIRED DECISION
Same evidence, new view	Generate an SSP section and an evidence index from one reviewed implementation record.	Confirm that each view preserves material limits and current data.
Same evidence, new objective	Use an account export for related access-control objectives.	Show how the source supports each distinct objective.
Same evidence, later time	Carry a configuration record into a periodic review.	Confirm freshness and absence of relevant change.
Same evidence, new reviewer	Send a readiness record to an assessor.	Preserve provenance and allow independent testing.
Shared provider evidence	Apply a service-level record across customer environments.	Separate provider facts from customer configuration and duties.
Prior finding	Consider an earlier reviewer's disposition during a new review.	Treat it as review history and establish present applicability.

The first operation is largely presentational. The last five require substantive judgment. Labeling all six “reusable” hides the work that keeps reuse safe.

A six-part decision test

Evidence should be eligible for reuse only when six questions have defensible answers.

1. Is the claim the same?

Compare the exact assertion, requirement version, assessment objectives, and implementation description. Two objectives may cite the same artifact while asking different questions. A policy can show that a process is defined. It may offer little proof that the process operated during the period under review.

Reuse should record the relationship: direct support, corroboration, context, or contrary evidence. Mapping alone should never imply sufficiency.

2. Is the subject the same?

Compare systems, enclaves, assets, accounts, facilities, data flows, services, and organizational units. Evidence collected from a corporate tenant may exclude a production enclave. A scan may omit devices that cannot run an agent. A provider statement may cover one service tier and exclude another.

Population reconciliation is essential when a claim uses words such as all, each, or every. The record should state expected population, observed population, the source for each count, and named exclusions.

3. Is it current enough for this claim?

Freshness is contextual. A network diagram, account inventory, vulnerability scan, policy approval, and recovery exercise age at different rates. A single universal expiration period creates false confidence.

Each evidence type should carry a refresh expectation and change triggers. Reuse requires checking both. A recent artifact can still be obsolete after a material change.

4. Is responsibility unchanged?

Confirm which party implements, operates, configures, monitors, corrects, and attests to each part of the claim. A provider acquisition, service change, contract revision, or customer configuration change can invalidate the old responsibility model even when the technology name remains the same.

Inherited evidence should state the provider's contribution and the customer's remaining work. The contractor retains responsibility for showing how the service is configured and used in its environment.

5. Is provenance intact?

The recipient needs the source, collection method, observation time, transformations, integrity information, and appropriate access. A copied screenshot with a new filename has lost useful lineage. A generated summary without source references cannot be retested.

Transformation is acceptable when it is visible. A normalized record may make comparison easier. It should point back to the source, describe the operation, identify the tool and version, and retain material caveats.

6. Is the new use authorized and fit for purpose?

The same record may be adequate for internal triage and inadequate for an authorized assessment finding. The recipient should identify the decision the evidence will inform, the review method, required independence, access rules, and acceptance authority.

A prior reviewer's conclusion is context. The present authorized reviewer still owns the present finding. Reuse cannot transfer authority that the source party never possessed.

A compact reuse record

The reuse decision should be inspectable. It can point to the original evidence rather than duplicating sensitive content.

Reuse decision

original evidence: ev-identity-0042
original claim: privileged MFA in tenant A
proposed use: support objective X in quarterly self-review
baseline/profile versions: recorded
scope comparison: same tenant; emergency account added to expected population
time check: collected 8 days ago; no listed trigger since collection
responsibility check: unchanged provider and customer duties
provenance check: source export and integrity value available
unresolved condition: emergency account enforcement needs direct test
disposition: partial support; human review required
reviewer, method, date: recorded

This record does not make the evidence sufficient. It shows why someone chose to use it and which condition remains open.

Provider evidence is the hardest useful case

Provider evidence offers large potential savings because shared services perform common functions for many contractors. It also creates concentrated risk: one ambiguous statement can spread across a large customer population.

A reusable provider assertion should name the legal entity, service and version, architecture or operating scope, applicable period, functions performed, evidence available, subservice dependencies, known exceptions, customer responsibilities, change triggers, and contact or correction path.

Each customer then supplies the connecting evidence: tenant configuration, identity integration, data flows, monitoring, and completion of customer duties. A provider's encryption capability does not show that a customer enabled it for every relevant data store. A provider's logging service does not show that required sources are connected or reviewed.

Government or an authorized assessor may decide which provider records can be accepted for a particular purpose. The profile should preserve the material needed for that decision without inventing acceptance authority.

Events that should stop or reopen reuse

Reuse should pause when a material event makes applicability uncertain. Useful triggers include:

- change to CUI flow, boundary, enclave, or asset population;
- addition or removal of a provider or subservice;
- identity, network, logging, backup, endpoint, or security architecture change;
- change in requirement, objective, guidance, profile, or assessment method;

- collection failure, integrity failure, unexplained population change, or conflicting source;
- security incident, failed test, newly exploited weakness, or corrective action affecting the claim;
- expiration of an evidence-specific refresh period; and
- discovery that the original reviewer lacked information material to the conclusion.

A trigger does not automatically prove failure. It changes the state to uncertain and routes the affected claim for collection, correction, or review.

Failure patterns to design against

Artifact laundering. A source moves through several tools and emerges with its gaps omitted. Require immutable source references and propagation of material limits.

Scope drift. A record created for one enclave is copied into an enterprise claim. Require explicit subject comparison and population reconciliation.

Evergreen provider claims. A service statement remains in use after a major version or responsibility change. Require provider-issued versions, effective periods, triggers, and withdrawal mechanisms.

Finding inheritance. A prior passing conclusion is treated as proof for a new period or purpose. Preserve prior findings as history and require a new disposition by the current authority.

Automation complacency. A rule sees valid dates and identifiers and labels the evidence reusable. Structural checks should produce eligibility signals and exceptions. Human judgment remains necessary wherever sufficiency, applicability, or authority is at issue.

An inspectable reuse trial

Government could test reuse policy with synthetic provider and contractor cases before granting operational reliance.

Create a base case with valid service evidence and several customer configurations. Introduce controlled changes: an excluded asset class, an added emergency account, a service-version change, a stale report, an unfulfilled customer duty, and a conflicting log source. Give reviewers the original packages and proposed reuse records.

Measure whether each method identifies when reuse is permitted, partial, or requires fresh evidence. Record missed changes, unsupported acceptance, excessive rejection, reviewer disagreement, labor, elapsed time, and correction behavior. Publish cases and expected structural results where security permits.

The trial should set failure thresholds before execution. A method that saves time while increasing unsafe reliance should be narrowed or stopped. A method that rejects every reusable record may be safe yet operationally pointless.

Reuse is a conclusion with an expiration condition

Safe reuse depends on sameness of claim and subject, current applicability, stable responsibility, intact provenance, and fitness for the new purpose. The decision must identify who made it and which events reopen it.

That standard is stricter than copying a file and more useful than rebuilding every package. It turns reuse into something a contractor can defend, a provider can maintain, an assessor can challenge, and Government can test.

TRACE THE CLAIM

Sources and revision history.

PRIMARY AND GOVERNING SOURCES

01 **Cybersecurity Maturity Model Certification Program, 32 CFR part 170**

Electronic Code of Federal Regulations



02 **CMMC Assessment Guide — Level 2, Version 2.13**

Department of War Chief Information Officer



03 **NIST SP 800-171A Revision 2**

National Institute of Standards and Technology



04 **Open Security Controls Assessment Language**

National Institute of Standards and Technology



05 **CMMC 20X Common Evidence Profile**

Deep Fathom



CORRECTIONS AND MATERIAL REVISIONS

No material corrections recorded.

See an error or a source we missed? [Send a correction](#). Material changes are recorded here rather than silently overwritten.