METHODICAL SECURITY · CMMC LEVEL 2 / NIST SP 800-171 REV 2 · ASSESSMENT READINESS

# Evaluating SSP Implementation Statements

Eight criteria for judging whether an implementation statement would survive a C3PAO's adequacy and sufficiency judgment — with mechanical quality bars, special cases, and a review workflow.

---

For ISSOs, assessment leads, and reviewers · Grounded in NIST SP 800-171A, the CMMC Level 2 Assessment Guide (32 CFR §170.24), and the DoD Assessment Methodology · July 2026

## The Core Standard

An assessor marks a requirement **MET** only when **every applicable assessment objective (determination statement) is satisfied by adequate, sufficient evidence in final form**. One unsatisfied objective fails the whole requirement. An implementation statement is therefore not prose about intent — it is the narrative that connects each objective to what the organization actually does and to the evidence that proves it.

Two terms govern the assessor's judgment (CMMC L2 Assessment Guide):

- **Adequacy** — the evidence actually demonstrates the objective is implemented correctly.
- **Sufficiency** — there is enough evidence, at the right depth and coverage, to support the finding with confidence.

Evaluate every statement against both.

**The most common failure mode is inaccuracy, not omission.** C3PAO experience is consistent on this: an SSP that describes controls as implemented when they are not, or a boundary that doesn't match the actual network, is a direct finding — worse than a gap that is honestly declared. The SSP, the operating procedures, and the real environment are three descriptions of the same system; an assessor will test all three against each other.

## The Stakes

Implementation statements are no longer just assessment inputs — they are the factual basis of the SPRS score a senior official affirms, and the Department of Justice's Civil Cyber-Fraud Initiative treats false affirmations as False Claims Act violations.

> **Enforcement is real.** In 2026, a contractor that self-reported a perfect 110 was scored **–170** by DIBCAC and paid **$507,144** to settle False Claims Act allegations. Evaluate statements as if a government assessor — and, later, a DOJ attorney — will read them against reality, because both may.

The bar is also higher than most organizations assume: when one contractor scored a perfect 110 on its joint-surveillance (DIBCAC-observed) assessment, the industry-average actual score sat around **–15**. Organizations that passed JSVAs consistently report the same surprise — not the requirements themselves, but the *depth of evidence per objective* assessors expected.

## The Eight Evaluation Criteria

### 1. Completeness — does it address every determination statement?

NIST 800-171A decomposes each requirement into lettered objectives (e.g., 3.1.1[a]–[f]) — a CMMC Level 2 assessment evaluates **320 assessment objectives**, not 110 requirements, and the SSP must address that granularity. A statement that answers the requirement's headline but skips an objective leaves that objective **other-than-satisfied** — which fails the requirement.

**Test:** Map each sentence of the statement to the objectives it covers. Any objective with no coverage is a finding.

- ✓ Every lettered objective is visibly addressed (or explicitly N/A'd with rationale).
- ✗ The statement paraphrases the requirement title and stops.

### 2. Specificity — does it name systems, tools, roles, and frequencies?

Generic boilerplate is the most common cause of assessment failure. "We use an EDR tool" tells an assessor nothing; "CrowdStrike Falcon is deployed to all in-scope endpoints" is checkable.

**Test (the first-time-reader test):** Could an assessor seeing this statement for the first time — with no other document open — understand exactly how the control is implemented and where the evidence lives? Could they design an examine/test procedure from the statement alone? If every noun is generic ("appropriate measures", "the organization", "periodically"), it fails. Assessors consistently flag SSPs that force them to cross-reference multiple documents to understand a single control.

- ✓ Named platforms, named policies (by exact title), named responsible roles, stated frequencies.
- ✗ Restated NIST control text; "regulatory mush" ("the organization ensures that appropriate...").

**State parameter values explicitly.** Write the actual frequency, threshold, or timeout ("sessions lock after 15 minutes", "reviews occur quarterly"), not "periodically" or "timely." This is what makes a statement testable today — and it is exactly the shape NIST 800-171 Rev 3 formalizes as organization-defined parameters (ODPs; DoD has published prescribed values for ~50 of Rev 3's 97 controls). Statements that already carry explicit values migrate to Rev 3 cleanly; vague ones must all be rewritten.

### 3. Operational state — does it describe what you *do*, not what you *intend*?

Statements must be present-tense descriptions of current operations, in the organization's own voice. "Access will be reviewed periodically" is an aspiration, not an implementation — and an assessor reads "will" as "doesn't."

**Test:** Search for future tense and intent verbs (*will, plan to, intend, should*). Each instance is either a hidden gap (belongs on a POA&M) or a writing defect.

- ✓ "The IT administrator reviews Active Directory accounts against the HR termination report on the last business day of each quarter."
- ✗ "User accounts will be reviewed on a periodic basis."

### 4. Traceability — does it anchor to evidence that exists?

Every governing document cited must exist, be producible on demand, and be in **final, approved form** — drafts, working papers, and unapproved policies are ineligible as evidence (CMMC L2 Assessment Guide). And a policy alone proves intent, not operation: for objectives that require the control to be *operating*, expect an operational artifact (config export, log sample, review record, screenshot, report).

**Test:** For each cited artifact: (a) does it exist, (b) is it final, (c) is it current (stale evidence signals an unmaintained control), and (d) does at least one artifact show the control *running*, not just mandated?

- ✓ "...as defined in the *Access Control Policy v3.2* §4; quarterly review records are retained in the Access Review SharePoint library."
- ✗ Citations to documents nobody can produce; policy-only support for an operational objective.

**Benchmark: two artifacts per requirement, findable by reference.** Teams that passed report assessors expecting roughly **two pieces of evidence per requirement (~220 across the 110)** — typically one governing document plus one operational artifact — and that assessments go fastest when the SSP is written to 800-171A structure so the assessor can verify a claim "by referencing a page number" rather than hunting. Statements should cite not just the artifact but the *location in it* (section, page, library path).

### 5. Scope accuracy — does it say where the control applies?

The statement must identify the systems, locations, and user populations within the assessment boundary that the control covers — and match the SSP's CUI scoping. A control described without scope invites the assessor to assume the broadest scope and find the gaps.

**Test:** Does the statement bound itself ("all in-scope Windows endpoints", "the CUI enclave", "remote and on-site staff")? Does that boundary agree with the SSP's system description and asset inventory?

A right-sized boundary is also the cheapest quality lever: successful assessments consistently trace back to aggressive scoping (one JSVA participant cut in-scope users from 150 to 15). Every system and population inside the boundary is one more thing every statement must accurately describe — an over-broad scope multiplies the surface on which statements can be wrong.

### 6. Responsibility — does it name who, including inherited controls?

Name the accountable role (not a person's name — a role that survives turnover). Where implementation is inherited from an enterprise service or an External Service Provider (cloud, MSP, MSSP), say so explicitly and record the shared-responsibility split; inherited requirements are MET only with adequate evidence that the provider implements the objectives.

**Test:** Exactly one accountable role identifiable per control activity; inherited/shared controls flagged with the provider named and the customer-side responsibilities stated.

**Outsourcing has limits.** Even where an MSSP runs the control day-to-day, successful assessments name an *internal* accountable owner — practitioner experience puts the floor at two to three knowledgeable internal people who administer and enforce policy. A statement whose only named party is the vendor reads as abdication, not implementation; and the vendor itself must meet equivalent standards, which the SRM and provider evidence should demonstrate.

**Shared Responsibility Matrix at the objective level.** Where any ESP (CSP, MSP, MSSP) touches CUI or security functions, assessors routinely request an SRM/CRM that maps responsibility per assessment objective — not per requirement — with no unassigned gaps. The implementation statement should agree with the SRM: "inherited from provider" in the statement with no corresponding SRM row (or vice versa) is an inconsistency finding. Verify the provider-side claims are backed by the provider's own documentation (e.g., FedRAMP authorization, provider SRM, contract terms).

### 7. Honesty — are gaps declared, not papered over?

A candid statement that flags a gap (with its POA&M reference) is assessment-ready; an embellished statement that implies tooling or process the organization doesn't have is a finding

waiting to happen — assessors test. Never fabricate; use explicit placeholders during drafting and resolve them before submission.

**Test:** Spot-check claims against the actual environment. Any unresolved `[placeholder]` text, or claims of capability the org can't demonstrate, fail.

✓ "Log aggregation to a SIEM is not yet implemented; see POA&M item PM-014 (target: Q3)."

✗ Claiming a SIEM because the requirement expects one.

**Document compensating controls in advance.** C3PAO joint-surveillance experience: for anything partially implemented or planned, the statement (or its POA&M pairing) should record the compensating controls and mitigating factors *before* the assessor arrives — a declared gap with documented mitigation is defensible; the same gap discovered by the assessor with no mitigation narrative is just a finding.

### 8. Consistency — do statement, findings, and status agree?

The implementation statement, the per-objective findings, the requirement status, and the linked evidence must tell one story. A requirement marked MET whose statement describes a partial implementation — or whose evidence was withdrawn — is internally contradictory and undermines the whole SSP's credibility.

**Test:** Requirement status equals the rollup of its objective findings; the statement doesn't contradict any recorded finding; no cited/linked evidence has been withdrawn or superseded.

## Special Cases

**Not Applicable.** N/A requires a documented rationale — NIST 800-171A requires it, and an unexplained N/A is treated as a gap. (A properly justified N/A objective counts as MET.)

**Enduring exceptions & temporary deficiencies.** Document enduring exceptions in the SSP with their mitigations; track temporary deficiencies in an operational POA&M. Both are assessed as MET when properly documented — the documentation *is* the control.

**POA&M discipline.** Every other-than-satisfied requirement needs a paired POA&M entry, and know your weights: under the DoD Assessment Methodology, **5-point requirements cannot remain on a POA&M at assessment time** — they must be fully implemented before the C3PAO arrives. A requirement with no statement and no POA&M entry is treated as not implemented (full point deduction; no partial credit).

**High-risk requirements deserve double scrutiny.** DIBCAC's published top-failed list is dominated by "misunderstood requirements" — where the implementation is often easy but the statement claims the wrong thing. The canonical example is **3.13.11**: "we encrypt CUI" is not the requirement — the cryptographic *module* must be **FIPS-validated** (named certificate number,

validated module, approved mode), and it is the single most-failed requirement in DIBCAC assessments. When reviewing statements for the top-failed requirements (FIPS validation, multifactor authentication, audit review, vulnerability scanning, CUI encryption at rest/in transit), verify the statement demonstrates the *precise* obligation, not a paraphrase of it.

## Mechanical Quality Bars

Cheap checks that catch weak statements before a human review:

| Check | Threshold | Signal |
|---|---|---|
| Length | < 25 words | Too brief to demonstrate a control; flag for expansion |
| Length | 80–180 words | Healthy range: long enough to demonstrate, short enough to read |
| Future tense | any *will / plan to / intend* | Hidden gap or writing defect |
| Control-text echo | statement ≈ requirement text | Boilerplate; says nothing about actual implementation |
| Unresolved placeholders | any `[…]` | Not submission-ready |
| Uncited evidence | no named policy/artifact | Untraceable; assessor must hunt |

## Review Workflow

1. **Screen** with the mechanical bars above.
2. **Map** the statement's claims onto every determination statement — mark each covered / weak / missing. Where available, compare against DIBCAC's published objective-evidence lists for the requirement — the most authoritative statement of what assessors expect to see.
3. **Verify** each cited artifact: exists, final, current, and (for operational objectives) shows the control running. Confirm artifacts are retained in a form that survives the assessment record (CMMC assessments hash submitted artifacts with SHA-256 and the record is kept for six years — an artifact you can't reproduce is an artifact you didn't have).
4. **Cross-check** consistency: findings rollup, scope claims vs. system description, statement vs. SRM rows, inheritance claims vs. provider documentation (e.g., FedRAMP status).
5. **Grade** each objective as a skeptical assessor would — *covered* only when a linked artifact clearly and directly addresses it; policy-only support for an operational objective is *weak*, not covered.

6. **Disposition**: fully covered → ready; gaps → POA&M (checking 5-point eligibility) or fix before assessment.

## Quick Reference — the One-Line Versions

1. **Complete** — every lettered objective, no exceptions.
2. **Specific** — named tools, roles, documents, frequencies, explicit parameter values.
3. **Present-tense** — what you do, not what you intend.
4. **Traceable** — cites real, final, current evidence that shows operation.
5. **Scoped** — says where it applies, matching the boundary.
6. **Owned** — a named role; inheritance made explicit and SRM-backed.
7. **Honest** — gaps declared with POA&M references, nothing invented.
8. **Consistent** — statement, findings, status, and evidence agree.

## Sources

**Primary:** NIST SP 800-171A (assessment procedures, determination statements, methods, depth & coverage); NIST SP 800-171 Rev 2/Rev 3; CMMC Level 2 Assessment Guide v2 (32 CFR §170.24); DoD Assessment Methodology; 32 CFR Part 170, including the final rule's responses-to-comments preamble.

**Successful-assessment experience:** DCMA DIBCAC objective-evidence lists and published top-failed-requirements data; Microsoft's JSVA lessons-learned; Schellman's JSVA program insight; CyberSheath's perfect-JSVA retrospective; Washington Technology's preparation lessons.

**Practitioner and regulatory:** Fortreum and Secureframe on C3PAO-observed SSP failures; CMMCAudit.org and Summit 7 on DIBCAC top-failed requirements; DoD CIO ODP values for Rev 3; DefenseScoop and Holland & Knight on False Claims Act enforcement; the CMMC Assessment Process (CAP); Summit 7 on shared responsibility matrices.

## About Methodical Security

Methodical Security provides resources and tooling to support Defense Industrial Base organizations through CMMC / NIST SP 800-171 assessments. Its platform, **Certalo**, works at the determination-statement level: it maps your existing documentation to each objective, flags where evidence is thin, and compresses the path to a submission-ready SSP, Assessment Report, and SPRS package. The result turns a one-time compliance scramble into a repeatable process — protecting current revenue and opening new contract eligibility.

---