

CMMC Level 2 Readiness Checklist

A practitioner walk-through of the 14 NIST SP 800-171 families, SPRS scoring, and the artefacts an assessor will ask for

Published 2026-09-08 · 12 minute read · For Defense contractors and subcontractors preparing a CMMC Level 2 self-assessment

Read it now — the PDF opens either way.

Open the PDF

Leave your e-mail and we'll follow up by hand — the PDF opens either way.

you@company.com

Save my e-mail

☐ I agree to be emailed occasionally about new CMDash resources. See the [privacy policy](#).

No email — download directly

Executive summary

CMMC Level 2 carries all 110 NIST SP 800-171 practices, organized into 14 families — access control through system and information integrity. There is no shortcut through the count; there is a shortcut through knowing which family each open gap sits in.^{[\[1\]](#)}

The SPRS score is arithmetic, not a grade. It starts at 110 and subtracts a fixed point value for every practice not fully implemented — knowing the weight of your open gaps tells you the score before you run the assessment.^{[\[2\]](#)}

Not every gap can go on a POA&M. Level 1 permits none at all. Level 2 permits a narrow set of low-weight gaps, with a strict 180-day closeout — miss it and your Conditional status expires.^{[\[3\]](#)}

Three artefacts, three different places. The target level, the SPRS score, and the official self-assessment PDF are produced by three different parts of

CMDash — section 5 below maps all three, plus the POA&M and OSCAL exports, to the exact page and role required.

1. Which level applies to your program

CMMC 2.0 has three levels of increasing rigor. Picking the wrong one wastes the most expensive resource a compliance programme has: time spent implementing controls for a level you do not need, or worse, an assessment scheduled against a level you have not actually implemented.

CMMC Level 1 (Foundational) — protects Federal Contract Information (FCI). Annual self-assessment. POA&M: Not permitted. Every practice must be fully in place before the self-assessment is submitted.

CMMC Level 2 (Advanced) — protects Controlled Unclassified Information (CUI). Most contractors: triennial third-party (C3PAO) certification. A DoD-designated subset handling non-prioritized CUI may self-assess annually instead — the contracting officer decides which applies.. POA&M: Only 1-point practices (plus SC.L2-3.13.11 at 3 points), and only when the assessment score is at least 88 of 110. Six practices — including the system security plan (3.12.4) and the external-connection controls (3.1.20, 3.1.22) — can never be POA&M'd. Every open item must be closed by a closeout assessment within 180 days of the Conditional CMMC Status date, or that status expires. 32 CFR § 170.21.

CMMC Level 3 (Expert) — protects Prioritized CUI on the DoD's highest-value programs. Triennial government-led assessment by DIBCAC (the Defense Industrial Base Cybersecurity Assessment Center). No commercial C3PAO may perform a Level 3 assessment.. POA&M: Permitted for a narrow set of specific requirements, with the same strict 180-day close-out as Level 2.

A DoD solicitation or your contracting officer names the level — CMDash does not guess it for you. The acquisition rule that puts CMMC clauses into contracts took effect 10 November 2025, establishing a three-year phased structure for later requirements; that later phase-in has been paused since 2026-07-13 with no resumption date announced. (checked as of 2026-09-15)

Check the specific solicitation rather than assume every current contract already requires it.[\[4\]](#)

2. The 14 NIST SP 800-171 families

Level 2's 110 practices are organized into 14 requirement families, each carrying the publisher's own verbatim requirement text where the underlying standard permits it.[\[1\]](#)

- Access Control** — 22 practices
- Awareness & Training** — 3 practices
- Audit & Accountability** — 9 practices
- Configuration Management** — 9 practices
- Identification & Authentication** — 11 practices
- Incident Response** — 3 practices
- Maintenance** — 6 practices
- Media Protection** — 9 practices
- Personnel Security** — 2 practices
- Physical Protection** — 6 practices
- Risk Assessment** — 3 practices
- Security Assessment** — 4 practices
- System & Communications Protection** — 16 practices
- System & Information Integrity** — 7 practices

All 110 of them carry NIST SP 800-171 Rev 2 (NIST CPRT)'s own wording, not a paraphrase — the text an assessor will test your evidence against.

3. How the SPRS score is actually calculated

The Supplier Performance Risk System Basic Assessment score is arithmetic: start at 110, then subtract the point value of every requirement that is not fully

implemented — 5, 3, or 1 points depending on the requirement, per Annex A of the DoD's NIST SP 800-171 Assessment Methodology (v1.2.1). The deductions sum to 313 points, so the score can go well below zero: an organisation with nothing implemented scores **-203**, which is the floor — $110 - 313$. There is no lower number the methodology can produce.[\[2\]](#)

42 practices carry the maximum 5-point deduction — mostly access control, configuration management, and system & communications protection.

14 practices carry a 3-point deduction.

51 practices carry a 1-point deduction.

2 practices are worth 5 points but drop to a 3-point deduction when partially implemented (below).

1 requirement — 3.12.4, the system security plan — carries no point value at all (below).

Two requirements allow partial credit, each with a condition Annex A states explicitly. **3.5.3** (multifactor authentication) deducts 3 instead of 5 when MFA covers remote and privileged access but not general, non-privileged local access. **3.13.11** (FIPS-validated cryptography) deducts 3 instead of 5 when cryptography is in use but the modules are not FIPS-validated. CMDash's scoring engine treats an **In Progress** status on those two requirements as that partial credit automatically. Nothing else on the list earns half marks — half-deployed is a full deduction.

And one requirement is not scored at all: 3.12.4, the system security plan. Annex A assigns it no point value, because the SSP is what defines the assessment's scope. If you do not have one, the assessment cannot be completed and there is no score to report — not a 1-point deduction. CMDash says exactly that instead of showing you a number.

One caution: this weight table is transcribed from Annex A of the DoD's June 2020 methodology (v1.2.1), reconciled requirement by requirement. If you intend to submit a real score to the government, verify the current values with your C3PAO or DoD guidance directly — methodology revisions do happen.

4. What can go on a POA&M — and what can't

A Plan of Action & Milestones lets you track an open gap with a remediation date instead of blocking the assessment on it — but only for a narrow, level-dependent set of gaps.

Level 1: not permitted at all. Every one of the 17 practices must be fully in place before the self-assessment is submitted.

Level 2 and 3: permitted for a narrow set. Only 1-point practices (or SC.L2-3.13.11 at 3 points) qualify, only when your score before those items is at least 80% of the maximum, and a fixed set of six higher-risk requirements — including the system security plan and external-connection controls — can never be POA&M'd regardless of weight.^[3]

The clock is 180 days. A POA&M closeout assessment must confirm every open item resolved within 180 days of your Conditional CMMC Status date, or that status expires — with the standard contractual consequences of losing it mid-contract.^[3]

5. Before the assessment — a readiness checklist

☐ Your CUI boundary is documented, not assumed.

A written system boundary — which systems, networks and third parties are in scope for Controlled Unclassified Information — is what every practice below is scoped against. CMDash tracks this at Security → Program → System Boundary (Command plan and above).

☐ A senior official is identified for the affirmation.

Every CMMC self-assessment ends with a named senior official affirming the results under penalty of the False Claims Act. Decide who that is before you generate the package, not while filling in the form.

☐ Every practice has a status — not just the ones with a tool behind them.

Connected tools (EDR, vulnerability scanner, identity provider) carry data relevant to some practice families, but families like Physical Protection, Awareness & Training, Personnel Security and Maintenance typically need manual evidence: a policy, a signed attestation, a training record.

☐ **Every "Not Applicable" has a written justification.**

Assessors scrutinize N/A designations closely. A practice marked N/A with no justification attached reads as a gap someone tried to hide, not one that genuinely does not apply.

☐ **Open gaps are triaged against the POA&M rules below, before you rely on one.**

Not every gap can go on a Plan of Action & Milestones, and the ones that can carry a hard closeout deadline. Know which of your open items qualify before you build a remediation timeline around them.

☐ **You know which document format your assessor or contracting officer wants.**

A narrative self-assessment PDF, a machine-readable OSCAL system security plan, or both — decide before the deadline, not the week of it.

6. Where CMDash produces each artefact

CMMC Level 1 or Level 2 tracking and SPRS scoring are open on every CMDash plan, and Level 3, like any other framework, on every paid plan — only the export capabilities below are tier-gated.

Target level — Security → Program → CMMC Level (/program/cmmc-level). Owner or Admin picks the level; every other role can see it. Open on every plan.

SPRS score — Compliance → SPRS (/sprs), with a per-practice breakdown and CSV/PDF export. Open on every plan; recording an official submission attempt or editing a weight override is Owner-only.

POA&M — Security → POA&M (/poam). Tracking is open on every plan, and any role can read the register; exporting requires the Starter plan or higher and Owner or Admin.

OSCAL documents — Compliance → OSCAL (/oscal). Validate and Diff work on any plan and role that can reach the page; exporting a system security plan, component definition, or assessment results document is Starter+, Owner or Admin.

Official self-assessment PDF — Reports → Exports (/exports), not the CMMC Level page itself: cover page, senior-official affirmation and signature block, per-family results, and a POA&M summary. Owner or Admin.

7. What CMDash does not automate

Physical Protection, Awareness & Training, Personnel Security, and Maintenance practices typically need manual evidence — a policy document, a signed attestation, a training completion record — because no connected integration observes them directly. CMDash tracks the evidence and its expiration; it does not manufacture it. And, as above, the SPRS weight table is a best-effort transcription your C3PAO or DoD guidance should confirm before a real submission.

Get your own SPRS score this week

See your target level's practice tracker and SPRS score.

30-day free trial of any paid plan (a card is required) — or sign up for Free with no card. No implementation fee.

References

National Institute of Standards and Technology. "SP 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." 2020. <https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>

Cited for: Organizes its security requirements into 14 families (Chapter Three, §3.1–3.14: Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, System and Information Integrity). NIST withdrew Revision 2 on 14 May 2024 in favor of Revision 3, but the CMMC Level 2 practice set and DoD Basic Assessment scoring still reference Revision 2. Checked 2026-09-08.

U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition & Sustainment. "NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1." 2020.

<https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf>

Cited for: A DoD Basic Assessment starts from a maximum score of 110 and subtracts a weighted point value — 5, 3, or 1 — for every NIST SP 800-171 security requirement not fully implemented. Annex A values 42 requirements at 5 points, 14 at 3 and 51 at 1, and allows 3 points instead of 5 on two of them (3.5.3 when multifactor authentication does not cover general local access, 3.13.11 when cryptography is not FIPS-validated), so the deductions total 313 and the lowest possible score is -203. Requirement 3.12.4 (system security plan) carries no point value: if it is absent, the assessment cannot be completed. Checked 2026-09-11.

U.S. Department of Defense (32 CFR Part 170, the CMMC Program rule). "32 CFR § 170.21 — Plan of Action and Milestones requirements." 2025.

<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.21>

Cited for: A CMMC Level 2 POA&M may include only requirements worth 1 point (or SC.L2-3.13.11 at 3 points), only when the assessment score before those items is at least 80% of the maximum, and excludes a fixed set of six higher-risk requirements outright (including the system security plan and external-connection controls); open items must be confirmed closed by a closeout assessment within 180 days of the Conditional CMMC Status date or that status expires. Checked 2026-09-08.

U.S. Department of Defense, Office of the CIO. "Cybersecurity Maturity Model Certification (CMMC) Program." 2025. <https://dodcio.defense.gov/CMMC/>

Cited for: The CMMC acquisition rule (48 CFR) took effect on 10 November 2025, establishing a three-year phased structure for when CMMC requirements can appear in DoD solicitations. Rollout timing for later phases is not fixed and can change — check current DoD CIO guidance before relying on a specific date. Checked 2026-09-06.

Not ready to trial today?

Get the next paper

One email when a new white paper publishes. Nothing else.

you@company.com

☐ I agree to be emailed when a new CMDash white paper publishes. See the

Notify me

privacy
policy .