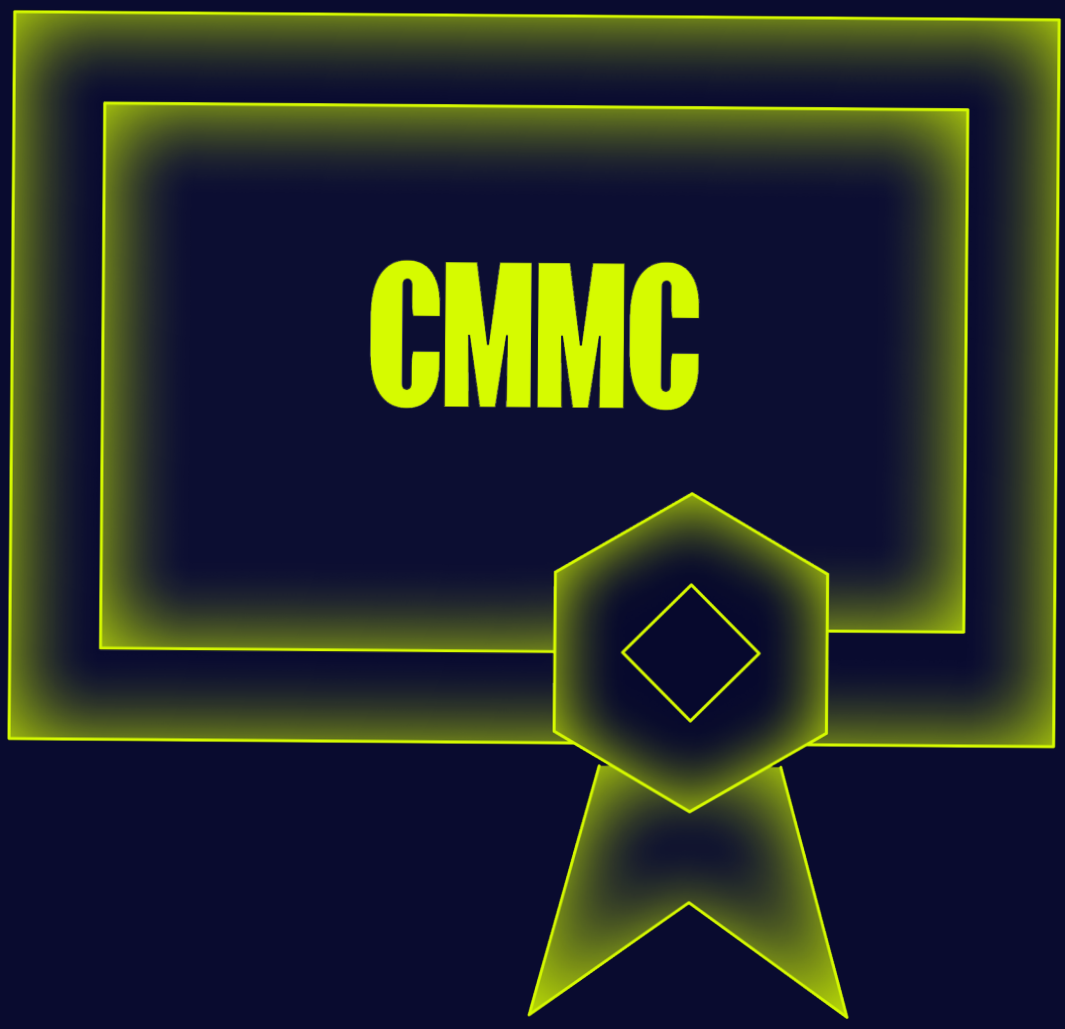
sonatype

TOP 5 CMMC GAPS THAT DELAY CERTIFICATION

And How to Close Them Before Your Assessment



Starting in November 2026, DoD solicitations will increasingly require third-party C3PAO assessments for contractors handling Controlled Unclassified Information (CUI)

C3PAOs are actively conducting CMMC Level 2 assessments. Most Defense Industrial Base contractors won't fail because they lack security controls. They'll fail because they cannot produce the evidence demonstrating that those controls were operating at the right time, in the right scope, across their vendor chain.

Starting in November 2026, DoD solicitations will increasingly require third-party C3PAO assessments for contractors handling Controlled Unclassified Information (CUI). CMMC Level 2 requires either self-assessment or C3PAO certification, depending on the sensitivity of CUI specified in the solicitation, with C3PAO certifications renewed every three years. This shift directly impacts Level 2 and Level 3 contractors — particularly those developing software products bundled into defense systems.

Sonatype wants to help CISOs, Compliance Leads, and Program Managers prepare for assessment, and these are the 5 gaps to identify and close before your assessment.

1. NVD-Only Intake Policy

Your flaw identification process has a two-thirds blind spot

Most vendor intake policies block components based on NVD High/Critical scores. However, in the 2026 State of the Software Supply Chain Report, we found that 65% of open source CVEs lack CVSS scores assigned by the NVD, meaning they pass through NVD-only gates completely undetected.

THE GAP	HOW TO CLOSE IT
Practice 3.14.1 requires identifying and remediating information system flaws. Assessors will examine your flaw identification source and whether your policy provides comprehensive coverage. When your answer is "we block NVD High/Critical," expect C3PAOs to probe whether you've documented the gap and implemented compensating controls.	Implement a policy engine with OSS-native intelligence beyond NVD. Document your coverage rationale. Apply the same standard to every vendor whose artifacts enter your build, because your intake policy is only as strong as its weakest upstream dependency.

2. Undocumented Policy Exceptions

Informal waivers are the leading cause of unmanaged risk findings

Policy exceptions approved through email, Slack, or verbal communication—never formally documented—aren't exceptions under CMMC. They're unapproved deviations. Programs routinely accumulate dozens of these before their first assessment.

THE GAP	HOW TO CLOSE IT
Practices 3.14.1, 3.4.1, and 3.11.3 all address exception management. Assessors will request your exception register and examine whether each entry includes: approver identity, scope, rationale, expiration date, compensating controls, and a remediation plan. Missing any one of these six elements constitutes a finding.	Establish a formal waiver workflow before assessment preparation begins. Every open exception requires all six fields to be documented. End-of-life software isn't a waiver situation—it's a migration event that must appear in your program plan with schedule and budget attached.

3. Static SBOM Submitted as Compliance Evidence

A snapshot proves nothing about what your software looks like today

The State of the Software Supply Chain Report also found that in 2025, nearly 1.8 billion downloads of components with known fixes still occurred, because nothing was watching after the initial scan ran green. A PDF SBOM generated at contract award is not compliance evidence for an assessment that happens 18 months later.

THE GAP	HOW TO CLOSE IT
Practices 3.14.1, 3.11.1, and 3.11.3 collectively require continuous monitoring, documented impact analysis, and evidence of ongoing risk management. Assessors will ask: when was this SBOM generated, how is it maintained, and how would you identify if a new CVE affected a component in production today?	Shift from SBOM-as-document to SBOM-as-operational-signal. Use machine-readable formats (CycloneDX or SPDX consistent with NTIA minimum elements guidance under EO 14028). Update with each release. Continuously monitor against new disclosures. Retain version history and produce on demand.

4. Vendor Attestation Accepted as Evidence

Self-reported compliance status is not demonstrable compliance

Prime contractors routinely accept vendor attestation letters—statements like “we are CMMC compliant” or “we follow secure software practices”—as sufficient documentation of supply chain risk management. Assessors do not.

THE GAP	HOW TO CLOSE IT
DFARS 252.204-7012 clause (m) requires primes to flow CUI protection requirements down to subcontractors. Practices 3.11.3 (vulnerability remediation in accordance with risk assessments) and 3.4.1 (configuration baselines) require demonstrable evidence that your own controls are operating effectively—and that means you need evidence from your vendors, not just their word. An attestation letter is a self-reported status. Assessors will request the artifact behind the claim: the policy document, the exception register, the SBOM, the tool configuration. If you don’t have it, neither does your vendor—and that becomes your finding.	Replace attestation language in subcontracts with evidence requirements: documented intake policy enforcement, traceable exception management, and a continuously monitored machine-readable SBOM. Require these artifacts to be producible during any assessment period.

5. Undefined CUI Enclave Scope

If you haven't declared your boundary, assessors will draw it for you

The most common reason CMMC scoping conversations become expensive is that contractors never formally declared a CUI enclave boundary. Without it, every system touching the program is potentially in scope—which is exactly how assessors will treat it.

THE GAP	HOW TO CLOSE IT
CMMC scoping determines which systems, networks, and tools fall under assessment. Assessors will trace CUI flows. If your source code, build environment, artifact repository, and SBOM are all CUI-adjacent, and you have no documented boundary decision, expect the scope argument to go against you.	Declare the enclave boundary now. Document which systems are in scope, where CUI is created and stored, and which vendor environments touch CUI-designated deliverables. The Army's contract designation of the deliverable as CUI is the triggering event—your boundary declaration is the response to it.

What Assessors Actually Look For

C3PAOs aren't looking for perfect security; they're looking for demonstrable governance across three dimensions:

ARTIFACTS	BEHAVIORS	SCOPE
• Written policies with version history • Exception register (all 6 fields per entry) • Machine-readable SBOM in CycloneDX/SPDX • CI/CD gate evaluation reports • Access and download logs from artifact repos	• Continuous monitoring — not point-in-time scans • Policy enforcement in the developer workflow • Traceable exception lifecycle (open -> closed) • EOL treated as migration events, not waivers • Vendor evidence requirements in subcontracts	• Declared CUI enclave boundary (documented) • Flow-down to all vendors touching CUI deliverables • Artifact repo in scope if it stores CUI derivatives • SBOM treated as CUI-derived controlled artifact • Evidence chain from intake through delivery

Don't wait for your assessor to find the gaps; let Sonatype help you uncover them first.

Certification is an Evidence Exercise: Where Sonatype Fits

The five gaps share a common theme: informal practices do not translate into evidence. NVD-only intake policies, undocumented exceptions, static SBOMs, vendor attestations, and undefined enclave boundaries all create ambiguity. During an assessment, ambiguity becomes scope expansion, additional artifact requests, and ultimately findings.

Preparation should begin with one guiding question: If a C3PAO asked for proof today, could we produce it on demand, with version history and traceability?

Closing these gaps before your assessment accomplishes three things:

- Reduces the risk of costly remediation cycles.
- Prevents scope expansion during the scoping review.
- Changes compliance from a point-in-time scramble into a repeatable operating model.

This is where Sonatype can help. We make it possible for organizations to operationalize CMMC requirements inside the software lifecycle itself, not as a parallel compliance exercise. From OSS-native vulnerability intelligence beyond NVD, to policy enforcement in CI/CD pipelines, to continuously monitored, machine-readable SBOMs, to traceable exception workflows and artifact-level governance, Sonatype helps teams generate the exact evidence C3PAOs request at the moment they request it.

CMMC requires demonstrating disciplined, continuous governance across your software supply chain. Organizations that operationalize SBOMs, formalize exception management, enforce comprehensive intake policies, require vendor evidence, and clearly declare their CUI boundary will move through assessment with confidence rather than friction.

Do not wait for your assessor to discover what your program cannot prove. Close the gaps now and enter your C3PAO assessment with evidence, not assumptions. With Sonatype, compliance becomes operational, defensible, and sustainable.