Analog Informatics™ Corporation

C3PAO: Who Assesses CMMC Level 2, and How to Choose One

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

analoginfo.com

Revised 29 October 2026

View this resource online

A CMMC Third-Party Assessment Organization (C3PAO) is the only kind of organization that can perform a Cybersecurity Maturity Model Certification (CMMC) Level 2 certification assessment and issue a Certificate of CMMC Status. No consultant, managed service provider, or compliance tool can produce that certificate, and neither can we.

See Shared responsibility for hosting models and the Customer Responsibility Matrix.

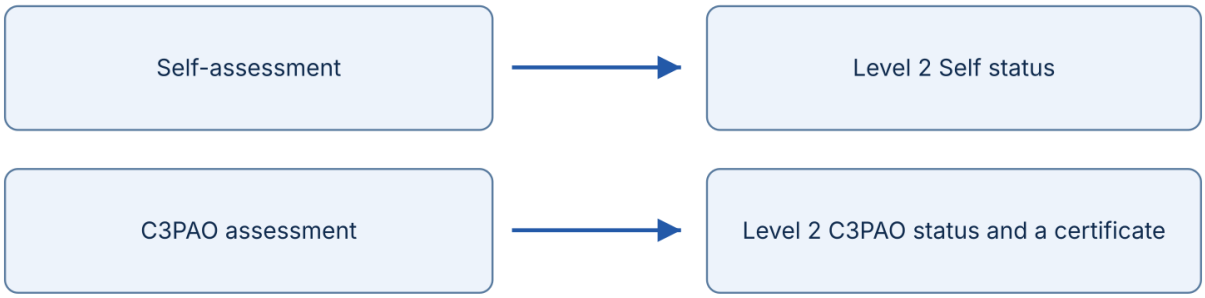
This page explains what a C3PAO is, how to confirm one is authorized, why independence matters, and what to have ready before you engage one.

Check the Contract and Current Phase-In Rules

The Department of War (DoW) suspended the CMMC Phase 2 transition on July 13, 2026. While the suspension holds, a program office or requiring activity may designate only **CMMC Level 1 (Self)** or **CMMC Level 2 (Self)**. It may not designate Level 2 (C3PAO) or Level 3 (DIBCAC), and no waivers are being granted.

Class Deviation 2026-O0025, Revision 3, carried that decision into the clause-insertion rules. DFARS 204.7504(a) now splits at a date: until **November 9, 2028**, clause 252.204-7021 goes into a solicitation only when the program office determines a specific CMMC level is required; on or after **November 10, 2028**, it goes in whenever contractor systems will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI).

What did not change: DFARS 252.204-7012, the 110 requirements of NIST SP 800-171, your SPRS score, and the annual affirmation. Read this page as preparation and as background for a certificate a prime may still ask to see, not as a step to take this quarter. Check your own solicitation, because a class deviation can be revised again.



A self-assessment and a certification assessment produce two different statuses, and only one of them involves a C3PAO.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Self-Assessment and Certification Assessment Are Not the Same Thing

Read your contract before you hire anyone. "Level 2" by itself does not tell you which road you are on.

Path	Who performs it	What it produces
Level 2 (Self)	Your organization	A self-assessment status. No certificate, and no C3PAO involved.
Level 2 (C3PAO)	An authorized or accredited C3PAO	A Certificate of CMMC Status, issued as Conditional or Final.

Both paths assess the same 110 requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The difference is who verifies them and what the contract will accept. See CMMC Level 2.

How to Verify a C3PAO Is Authorized

The Accreditation Body, known as the Cyber AB, authorizes and accredits C3PAOs. Its Marketplace is the live record, and status changes over time.

1. Open the Cyber AB Marketplace and filter by assessor.
2. Confirm the status reads **Authorized C3PAO** or **Accredited C3PAO**. A candidate listing is not authorized to assess you.
3. Confirm the firm lists assessment personnel, including a Lead Certified CMMC Assessor (Lead CCA).
4. Re-check the status immediately before you sign. A listing you confirmed during vendor evaluation may have changed by the time a contract reaches you.

Accreditation is a further step beyond authorization. Under 32 CFR 170.9, a C3PAO must achieve and maintain compliance with ISO/IEC 17020:2012(E), the international standard for bodies performing inspection, within 27 months of authorization.

What a C3PAO Has to Meet

These are federal requirements under 32 CFR 170.9, not vendor marketing claims. They explain why the pool of qualified firms is smaller than the demand.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Requirement	What it means
Assessment team composition	At least two people: a Lead CCA and at least one other Certified CMMC Assessor (CCA). If a firm implies one person can certify you, that is a warning sign.
Separate quality assurance	A quality assurance review of every assessment, performed by a CCA who was not on that assessment team.
Background investigations	Every person taking part in the Level 2 certification assessment process, including the assessment team and the quality assurance individual, completes a Tier 3 background investigation resulting in a determination of national security eligibility. This is not a security clearance.
Foreign ownership review	The firm submits Standard Form 328 and undergoes a national security review for foreign ownership, control, or influence, and reports any change within 15 business days.
Its own assessment	The C3PAO itself undergoes a Level 2 certification assessment, conducted by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center.
Record retention	Assessment records are kept for six years, including records of organizations for which the firm provided consulting services.
Conflict of interest policy	The firm complies with the Accreditation Body's conflict of interest policy, code of professional conduct, and ethics requirements.

The Independence Rule, and Why It Bites

A C3PAO cannot assess an environment it built, configured, or remediated. That is what the conflict of interest requirement exists to prevent, and the six-year record of consulting engagements is how it is traced.

The practical consequence is a sequencing decision you make early. The firm that helps you get ready is usually not the firm that assesses you. Companies that hire one partner to do both discover the problem late, when the readiness work is finished and the assessor has to be someone else.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Plan for two relationships from the start. A readiness partner and an assessor are different roles with different obligations.

What to Have Ready Before You Engage

Confirm your scope, readiness, and required assessment type before scheduling an assessment. Early discussions can help define timing and the evidence the assessor will need.

1. **A defined assessment scope.** Name the systems, people, and facilities that handle Controlled Unclassified Information (CUI). A narrower, well-defined boundary is easier to assess and easier to maintain. See Secure enclaves.
2. **A current system security plan.** It describes the environment as it actually is, not as you intend it to become.
3. **Evidence for each requirement.** An assessor examines artifacts, interviews people, and tests. A requirement with no artifact is a requirement with no result.
4. **A Plan of Action and Milestones (POA&M) you can defend.** Not every requirement can be deferred, and the ones that can carry a closure deadline.
5. **A current SPRS score that matches all of the above.** See SPRS score.
6. **Named people who can answer.** Assessors interview administrators and users, not only the compliance lead.

How the AIC CMMC Complete™ Kit Prepares the Evidence

Analog Informatics Corporation (AIC) builds **AIC CMMC Complete™** for Level 1, Level 2, and Level 3. The kit runs the controls and keeps the records an assessor asks to see. The assessment decision belongs to the assessor, not the software.

What an assessor asks for	Where it comes from
Current control state against the selected framework and level	**Current State Compliance**
Which requirements have live evidence, and which do not	Control coverage
History showing a control stayed in place, not just that it was in place on assessment day	Control state history

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What an assessor asks for	Where it comes from
Artifacts organized by requirement, for the assessment team to read	**Assessment Binder**
Open items with closure dates	**Assessment Binder** POA&M entries
Records of who accessed which privileged account, when, and why	**Session Recording** and audit records
The certification decision	The C3PAO

An assessment organization, certification body, or regulator decides whether a requirement is satisfied. These pages describe product availability. They are not an assessment result, a certification, or legal advice.

Common Questions

Do I need a C3PAO at all? Only if your contract requires a Level 2 certification assessment. A Level 2 self-assessment does not involve one. Read the clause before you budget for an assessment.

Can my consultant also be my assessor? No. A firm cannot assess an environment it built or remediated. Plan for a readiness partner and a separate assessor.

Can one person assess us? No. The assessment team must include at least a Lead CCA and one other CCA, plus a separate quality assurance review by a CCA who was not on the team.

Who assesses the assessors? The Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center assesses the C3PAO itself, and the Cyber AB handles authorization and accreditation.

What is the difference between Conditional and Final status? A Final status means every applicable requirement was met at assessment. A Conditional status means some requirements remain on a POA&M with a closure deadline.

Does the July 2026 pause remove the need for a C3PAO? For now, a DoW program office may designate only Level 1 (Self) or Level 2 (Self). A new contract should not require a C3PAO assessment. The underlying requirements still apply. Under DFARS 204.7504, starting November 10, 2028, clause 252.204-7021 applies based on the information handled, not only when a level is designated. See CMMC Phase 2 for the full timeline and Why CMMC was paused, and what actually fixes it.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Does AIC perform assessments? No. Analog Informatics builds the software and the training. We are not a C3PAO and we do not issue certificates.

How long do assessment records last? A C3PAO keeps them for six years unless the program office authorizes other disposition.

Related Pages

- CMMC Level 2: all 110 requirements, row by row
- CMMC Level 1 and CMMC Level 3
- SPRS score: the number an assessor and a prime both look at
- DFARS 252.204-7012: the clause behind the requirement
- NIST SP 800-171
- Secure enclaves: narrowing the assessment scope
- **Continuous compliance**
- **AIC CMMC Complete™** and pricing
- Partners and services
- Glossary

Sources

- DFARS 204.7504, solicitation provision and contract clause
- 32 CFR 170.9, CMMC Third-Party Assessment Organizations
- 32 CFR Part 170, CMMC Program
- Cyber AB Marketplace
- Cyber AB R2001, C3PAO Authorization Requirements
- NIST SP 800-171 Rev. 2
- Department of War announcement on the CMMC Phase II pause

Auditor and Readiness Resources

For product orientation, evidence-review exercises, and independent assessor contacts, visit C3PAO Partners and Auditor Resources.

For more information about Analog Informatics Corporation, please go to analoginfo.com.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.