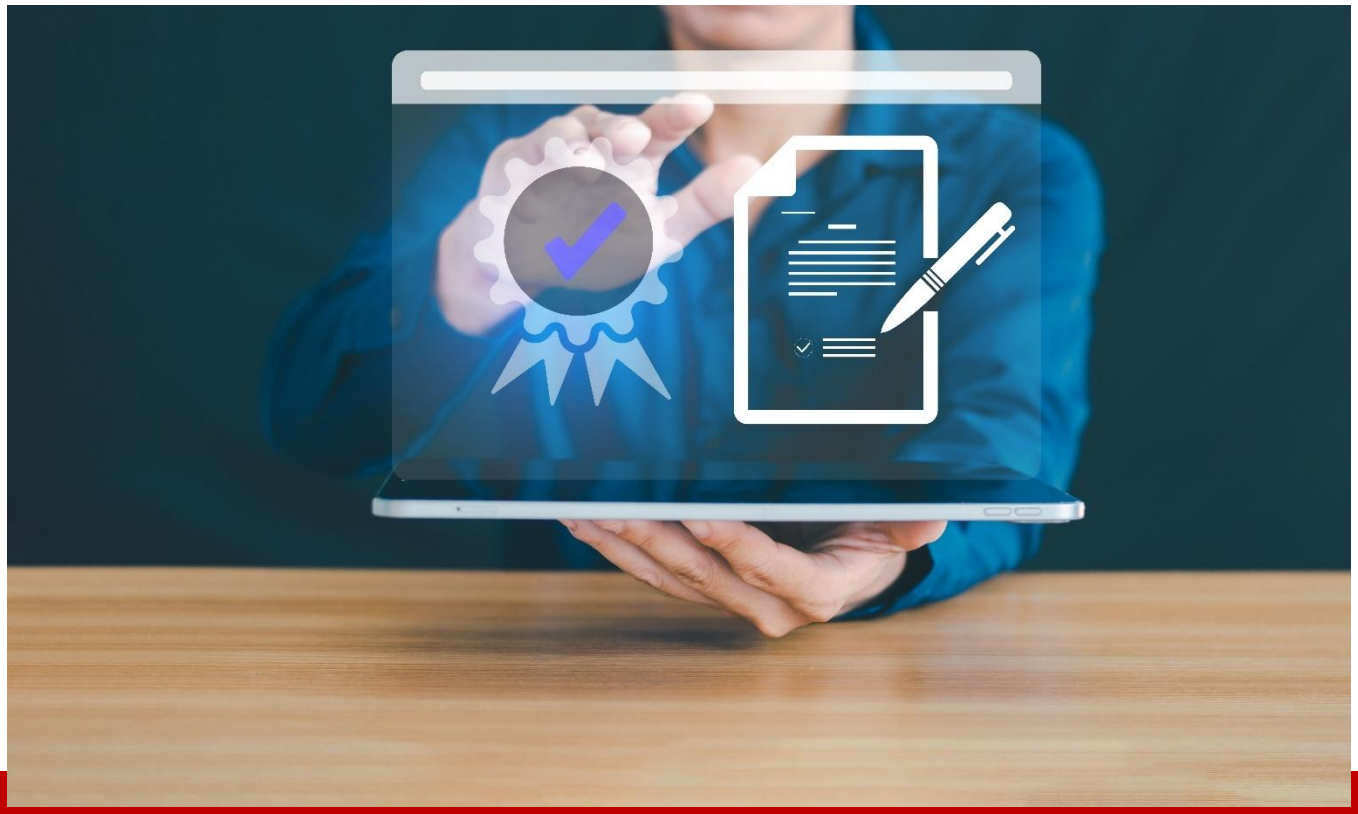


Choosing the Right C3PAO for Your CMMC Level 2 Certification

Here's what you need to know—broken down simply and clearly.

By Claire Kelley, Marketing Writer, AXIOTROP

If you're aiming for CMMC Level 2 certification, choosing the right C3PAO (Certified Third-Party Assessment Organization) is one of the most important decisions you'll make. Here's what you need to know—broken down simply and clearly.

What Is CMMC and Why Does It Matter?

The Cybersecurity Maturity Model Certification (CMMC) is a U.S. Department of Defense (DoD) program. It ensures that companies working with the DoD protect sensitive data like Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

If your company handles this kind of data, you'll need to pass a CMMC Level 2 assessment—conducted by an authorized C3PAO.

What's a C3PAO?

A C3PAO is a company approved by The Cyber AB (the official accreditation body) to perform CMMC assessments. Only C3PAOs listed in The Cyber AB Marketplace can certify you for Level 2.

What Makes a Good C3PAO?

Not all C3PAOs are the same. Here's what to look for:

- Experience in Your Industry: Do they understand your sector's unique needs?

- Team Qualifications: Do they have Certified Assessors and a Lead Certified CMMC Assessor (CCA)?

The size and internal capacity of the C3PAO also matter. Only a small number have full- time Lead Assessors on staff, and most operate with lean teams. You will want to ensure the C3PAO can provide a well-qualified assessment team that includes Certified Assessors and Professionals and is led by a formally designated Lead CCA who is equipped to interpret NIST SP 800-171A methods effectively.

- Assessment Style: Are they hands-on and educational (great for small businesses) or built for large, complex organizations?

- Support Services: Some offer pre-assessment help—but make sure your assessor isn't your consultant (conflict of interest!).

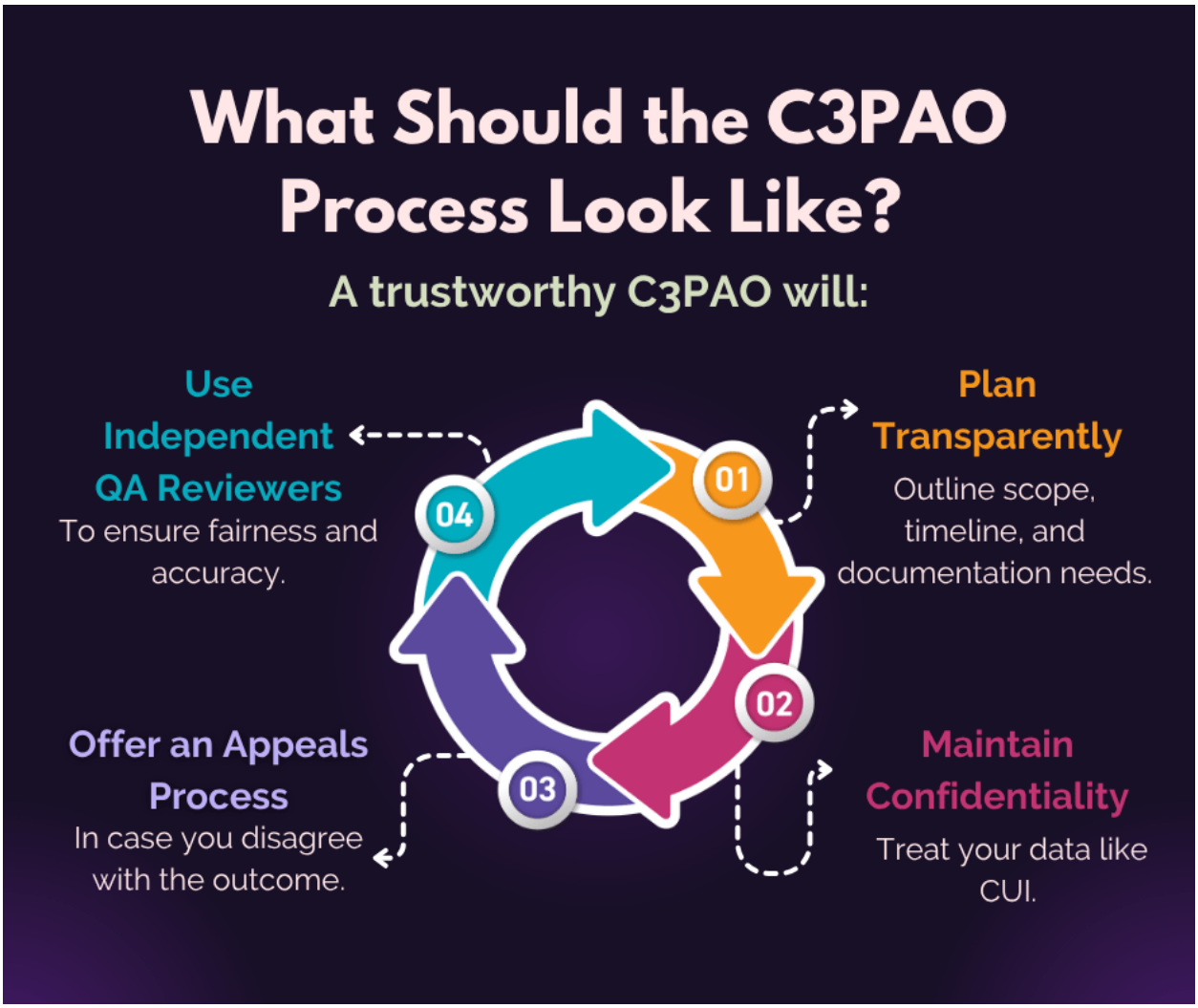
Small Business vs. Large Enterprise: Choose Accordingly

- Small Businesses: Look for C3PAOs that offer guidance, flexibility, and a streamlined process.

- Large Enterprises: You'll need a C3PAO with a bigger team and deep technical expertise across areas like cloud security and network architecture.

Impartiality Is Non-Negotiable

C3PAOs must follow strict rules to stay unbiased. They can't offer guarantees or remediation advice tied to your certification outcome. They must also follow ISO/IEC 17020:2012 and the CMMC Code of Professional Conduct.



Final Thought

Getting CMMC Level 2 certified is a big step—but the right C3PAO will make it smoother, clearer, and more secure. Take your time, ask questions, and choose a partner who aligns with your goals.

About the Author

Claire Kelley is a Marketing Writer at AXIOTROP, a cybersecurity firm that offers clients leading services in assessment, remediation, and validation to protect the confidentiality, integrity, and availability of their regulated information. She has worked in the Rhode Island Department of Administration where she was recognized by the Rhode Island General Assembly for her work there. Claire has contributed to cybersecurity-focused content and outreach AXIOTROP, where she handles related public relations and marketing efforts. Claire can be reached online at claire.kelley@axiotrop.com and at our company website www.axiotrop.com.