

The Hardest CMMC Client: Level 2 for a Solo Defense Technology Consultant

A one-person defense consultancy carried the same 110-control burden as a 200-person manufacturer, with none of the capacity. InterSec redesigned its delivery model around a sole operator's reality: shorter documents, self-execution, manual monitoring, and an honest timeline.

<p>CLIENT A solo defense technology consultancy</p>	<p>PROFILE Signal-processing and embedded-systems expert, 30+ years, no IT staff</p>	<p>STATUS ● In progress</p>
--	---	--

<p>110 Controls, same as a 200-person firm</p>	<p>1 Operator, no IT support</p>	<p>120 → 50 Page controls guide, condensed</p>	<p>30+ Years in independent practice</p>
---	---	---	---

<p>STANDARD CMMC Level 2, self-assessment</p>	<p>FOOTPRINT 2 laptops, no MSP</p>	<p>MONITORING Manual, quarterly POA&M review</p>	<p>MODEL Client-autonomy delivery</p>
--	---	---	--

— THE CHALLENGE

This is the most constrained profile in the CMMC small-business landscape: a leading expert in a one-person practice, with genuine DoD contracts and real CUI obligations, but no IT support and limited bandwidth alongside active delivery. The standard model, sustained biweekly sessions and parallel workstreams, was not executable. Yet the requirements were identical: the same 110 controls, the same November 2026 deadline.

— THE APPROACH

InterSec redesigned its delivery around the operator's reality. The pivot, from a simultaneous build-out of all 110 controls to a prioritized, client-autonomy model, accepted a longer path in exchange for a sustainable one. The most impactful, least disruptive controls came first, with InterSec in a review role. Every choice minimized the time burden: shorter documents, self-executed steps with review, and asynchronous feedback.

When you are the entire company, a program only works if you can run it without help.

— THE SOLUTION IN PRACTICE

The standard 120-page technical workbook was condensed to a 50-page guide for a two-laptop environment with no managed services. Live sessions walked the owner through scanning, full-disk encryption, password policy, and CIS hardening. Documentation followed the same logic: a single consolidated operational-procedures document with annual updates. Phones and tablets were removed from the CUI boundary, and manual log review was documented as the right-sized control.

— RESULTS & IMPACT

- ✓ The CUI architecture is defined, with phones and tablets removed and disk encryption and CIS hardening applied.
- ✓ The policy framework is simplified to a single operational-procedures document.
- ✓ Technical controls are documented through the condensed guide, with screenshot-based evidence underway.
- ✓ Manual monitoring is formalized in the SSP, with a quarterly POA&M cadence.

— KEY TAKEAWAYS

The CMMC burden does not scale down with size.

A sole proprietor with two laptops faces the same 110 controls as a 200-person manufacturer. A model that ignores that tension will stall.

Client-autonomy delivery fits constrained operators.

Putting the owner in the execution seat, with the consultant validating, produces evidence he can actually explain to an assessor.

Documentation must match operational reality.

A well-documented manual process for a two-laptop environment is more defensible than a SIEM that never gets read.

Scope reduction is a legitimate strategy.

Removing devices from the CUI boundary and keeping CUI off local servers shrinks the assessment surface defensibly.

CAPABILITIES DEMONSTRATED

CMMC Level 2 Readiness

CUI Scope Reduction

Right-Sized Technical Controls

Consolidated Policy Development

Client-Autonomy Delivery

Compliance does not get easier when you are the only person in the company.

InterSec prepares the smallest defense contractors for CMMC assessment with programs they can own and sustain.

Let's talk →