FIELD GUIDE

Why You're Procrastinating Your CMMC Preparation (and What To Do About It Today)

SENTINELBLUE

SUMMARY

Who This Guide Is For

- Organizations Seeking Certification (OSCs)
- Federal contractors in the Defense Industrial Base

What This Guide Contains

- Explanations of the common reasons that organizations put off their CMMC prep and assessment
- Suggestions for what to do about it

About Sentinel Blue Field Guides

Security is a team sport. We believe the Defense Industrial Base is stronger when knowledge and expertise are shared openly. That's why we've created free educational resources for federal contractors navigating cybersecurity and compliance challenges.

If you find this guide helpful, please share it with your community. Shields up!

Why You're Procrastinating Your CMMC Preparation (and What To Do About It Today)

Let's be real: CMMC prep is no one's idea of a good time. It's expensive, it's time-consuming, and it involves more interpretative nuance than a tarot reading. So it's not difficult to understand why contractors put it off.

We've helped over 50 companies get CMMC Level 2 certified, and what we've found is that people usually procrastinate for specific reasons, from budget uncertainty to confusion around where to start. Here's how to diagnose what's actually holding you back (and what to do about it before it's too late).

1. If You're Waiting on Leadership Buy-In or Budget...

... frame it in terms of costs to your business.

There's no getting around the fact that Level 2 certification is expensive. The DoD estimated first-year costs for a small contractor to be around $150K for an enclave-only approach (and that assumes your organization is already operating in compliance with DFARS 252.204-7012, which many aren't). The assessment alone typically runs $50K or more.

But the question really isn't whether your business can afford to get certified. It's whether you can afford to lose your government contracts. The unavoidable fact is that you stop getting paid if you don't have your Level 2 certification in place when your contracts require it. If your leadership is still hesitating, ask them which cost is higher.

Also: If you're budgeting for external help with your certification, remember that not all CMMC service providers are created equal. The market is crowded with MSPs and consultants who address pieces of the problem, but you need comprehensive coverage from your initial baseline all the way through a successful assessment. Make sure you understand exactly what's included before you commit to a provider.

2. If You Think CMMC Is Mainly About Checking Boxes...

... think again.

Compliance is the byproduct of good cybersecurity, not the goal. Organizations that treat CMMC certification as a transaction, i.e. something to get through so they can keep selling to the government, tend to end up with neither good security nor a smooth assessment.

The reality is that good cybersecurity doesn't just serve your government contracts; it serves your whole business. A ransomware event can shut down operations entirely. An undetected intrusion can reroute payments or compromise confidential data for months before anyone notices. The reputational damage alone can end a business.

If you've never experienced a serious breach, the risk can feel abstract, like riding a bike without a helmet. Nothing bad has happened yet, so the helmet feels optional. But research shows that the median cost of a single data breach is $83,000 in insurable claims alone (and growing every year). That makes the cost of good cybersecurity and compliance seem a lot more reasonable.

3. If You're Planning to Handle It Internally...

... make sure you're as prepared as you think you are.

Start with your SPRS score. It runs from –203 to 110, and if you haven't calculated yours yet, you should know that you're running out of time.

Next: do you have an SSP? A POA&M? Are all your technical controls mapped to your policies and procedures? If the answer to any of these is no, you're not going to make it through an assessment without significant rework. (And if you're making all your technical improvements before your policies and procedures are written, you're also in trouble.)

If your in-house team has the expertise to do this right, great. Just make sure they're actually doing it in the right order, with the right artifacts, against the right assessment objectives.

4. If You Think You're Ready But You're Hesitating...

...it's time for a gap assessment.

If your controls are in place, your documentation is done, and you think you're close to the finish line, get a gap assessment conducted by an experienced CMMC consultant or C3PAO. This gives you an objective read on where you stand, surfaces the things you've missed, validates the things you've done right, and gives you confidence going into your official assessment.

5. If You've Run Out of Time or Hit Your Limits...

... it's time to bring in the experts.

If you've exhausted your in-house resources and the clock is running out (a common experience for small- and medium-sized defense contractors), the answer isn't to keep pushing harder. It's to bring in a CMMC consultant or full-service provider who can tell you exactly where you stand.

You want someone who can assess your current posture, close the gaps that matter most, and map a realistic path to certification in the time you have left. Look for someone who holds active credentials (e.g. Certified CMMC Professional or Certified CMMC Assessor) and who has hands-on assessment experience. (They should be able to provide references from companies they've helped achieve Level 2 certification.) They should also be able to speak plainly about what's achievable and when, without resorting to jargon.

At this stage, what you need most is clarity. Find your expert, nail down your timeline, and get moving. We promise it's worth it.

Additional Guidance

CMMC preparation is complex, but it doesn't have to be paralyzing.

For more free resources on DIB cybersecurity and compliance, explore our other field guides here.

If you'd like more specific advice tailored to your environment, Sentinel Blue is available to help. Contact us now.