FIELD GUIDE

After the Assessment: A C3PAO's Guide to Continuous Compliance

SENTINELBLUE

SUMMARY

Who This Guide Is For

- Organizations that have passed their Level 2 CMMC asssessment
- Federal contractors in the DIB
- Anyone with an interest in CMMC

What This Guide Contains

- Advice on maintaining continuous compliance
- Tips for preventing drift after your Level 2 certification

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!

After the Assessment: A C3PAO's Guide to Continuous Compliance

Passing your CMMC Level 2 assessment is a major achievement, but the work doesn't stop there. Your certification is valid for three years, and every one of those years requires an SPRS score submission and the expectation that you're still meeting all 110 controls.

As a C3PAO, we know how easy it is to unintentionally let your posture drift once your certificate is in hand. Here are our top tips to maintain continuous compliance after the assessment.

1. Run Gap Assessments on a Schedule

Most compliance policies call for quarterly gap assessments, and there's a practical way to make that manageable: split the 320 assessment objectives into roughly four batches and work through one batch per quarter. However, make sure that ongoing obligations like vulnerability management and access controls are still assessed on a timeline based on your own organization-defined parameters (ODPs).

2. Let Your Quarterly Work Cover the Annual Risk Assessment

If you're running disciplined quarterly gap assessments and you're confident all 110 controls are still met, that work can do most of the heavy lifting on your annual risk assessment, since four quarters of findings, re-verified controls, and documented changes will give you the raw material to build from. Risk assessment adds an important analysis of threats, costs, and business decisions, and assessors will still expect to see both... but it's worth knowing where your quarterly work can carry over so you can save yourself time and effort.

3. Keep Up with Employee Training

CUI training is a mandatory and ongoing requirement, not a one-time event. It's important to keep up not only the training itself but also (and this is where people get tripped up) the record-keeping of the training. If you can't produce documentation showing who completed what training and when, it doesn't count.

4. Document Every Change, Even the Small Ones

It's all too easy to let change records slip, particularly at small companies. An admin pushes a software update. An outside contractor gets elevated access to finish a project. These changes tend to happen outside any formal process, without any documentation, and then there's no record of them down the line. Regardless of how mundane or routine it may seem, every change to your environment needs a paper trail.

5. Maintain Strict Access Controls

This is one of the most important elements of continuous compliance: limiting insider risk by implementing strict physical and technological access controls. It's particularly easy to miss when legitimate access continues after it should have ended. For example, someone gets promoted off a project and their credentials stay active, or a supplier retains access long after their engagement ends. To avoid unnecessary insider risk, build a habit of revoking access at every one of these transition points, not just the final offboarding.

6. Don’t Ignore Your Low and Medium Vulnerabilities

Critical and high vulnerabilities are relatively easy to stay on top of because they’re loud and important. Low and medium vulnerabilities aren’t, and enough of them can add up to the same real-world risk as a single critical one. An information disclosure finding, a weak configuration, and an unpatched service are each minor on their own, but together they can give an attacker the same path a single critical vulnerability would have. Making sure your ongoing vulnerability management program accounts for the aggregate is key.

Your Level 2 certificate covers three years. What you do in those three years is what determines how the next assessment goes. Pick the suggestion above that’s slipped the furthest at your organization and start there.

Additional Guidance

Staying Level 2 certified is different than getting certified, but it doesn't have to be a burden if you build it into your routine. For more CMMC guidance tailored to your unique environment, Sentinel Blue is available to help.

Contact Us Now