FIELD GUIDE

From CMMC to ISO 27001:

What You've Already Built and What's Missing

SENTINELBLUE

SUMMARY

Who This Guide Is For

- Organizations that have passed Level 2 CMMC asssessment and are considering ISO 27001 certification
- Federal contractors in the DIB

What This Guide Contains

- Comparisons between CMMC and ISO 27001 requirements
- Tips for what work can carry over from CMMC and what can't

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!

From CMMC to ISO 27001: What You've Already Built and What's Missing

If your company has done the work for CMMC Level 2, you've probably heard that ISO 27001 should be the easy next step. That's partly correct, since the technical controls overlap substantially. But ISO 27001 asks for more than controls; it asks for a management system that runs your security program over time.

We created this guide to help you sort what you already have from CMMC into three categories for ISO 27001: what can be reused, what needs rework, and what you'll have to build from scratch.

What Carries Over from CMMC

The good news is that a significant portion of your CMMC work will transfer to ISO 27001 with few or no changes.

1. Your commitment to protecting sensitive information. First and foremost, CMMC and ISO 27001 share the same fundamental aim of keeping sensitive information secure. If your team built its CMMC program around real security and not checkbox compliance, you'll have a solid foundation to begin with ISO 27001.

2. Many of your technical controls. Both standards expect you to control access, manage configurations, protect physical spaces, monitor for threats, and respond to incidents. The controls you put in place for CMMC cover much of the same territory as ISO 27001 Annex A, which means less rework for your IT team in general.

(You also don't have to work out the control mapping on your own. Appendix D of NIST SP 800-171 Rev 2 pairs each of the 110 CMMC requirements with the related controls in ISO/IEC 27001:2013 Annex A. Under Rev 3, NIST's online Cybersecurity and Privacy Reference Tool will take over the job.)

3. Your assessment experience. A team that has been through a demanding CMMC Level 2 assessment already knows what it takes to prepare for outside evaluation, and that experience leaves you ready for ISO's recurring audits.

What Needs Rework

Some of what you've built will be relevant to ISO 27001, but only after it's been reframed or adjusted. Your existing CMMC documentation gives you a substantial head start here, but many pieces need to be adapted before they'll hold up in an ISO audit.

1. Your scope. CMMC scope is drawn around CUI (which is why so many contractors build enclaves). ISO 27001 scope, on the other hand, is drawn around the business: the units, locations, processes, and systems your customers and partners need the certificate to cover. Your specific scope will ultimately appear on your ISO certificate, so only including an enclave can undercut the credibility you're trying to achieve.

2. Which controls you implement. Under CMMC, all 110 requirements apply. Under ISO 27001, you should only choose controls that trace back to a specific risk, legal requirement, or contractual obligation identified through your risk assessment. We explain more about that process in this related ISO 27001 resource.

3. Your evidence. CMMC evidence shows that controls are in place at the time of assessment, while ISO 27001 evidence needs to show your management system operating over time. In other words, it can't be thrown together the night (or more realistically, the weeks) before the auditor arrives.

What You'll Build from Scratch

There's one key part of ISO 27001 with no CMMC equivalent: the information security management system (ISMS), a set of recurring business processes for running your security program. Your ISMS will require:

- Defined roles delineating who is responsible for information security at your organization
- A risk assessment process that determines which controls you implement
- A Statement of Applicability (SoA) that justifies which Annex A controls you're including
- Security objectives your organization is working toward
- An internal audit program
- A process for identifying and correcting problems
- And more

You'll also need time. ISO auditors need to see the ISMS in operation before your Stage 2 audit, including at least one internal audit and one management review on record. As we noted above, that means you can't finish building your program the day before your audit; a full operating period has to be built into your project timeline.

Where to Start

With many of your controls already in place from CMMC, most of your effort in achieving ISO 27001 certification will go toward building your ISMS and giving it time to run. If you'd like help making the shift, Sentinel Blue can assess your readiness, help define a scope that supports your business goals, and prepare you for certification.



Is pursuing ISO 27001 after CMMC the right move for your organization? Let's find out.

Contact Us Now