SteelCloud

DATA SHEET

to AUTOMATE Your CMMC 2+ Compliance (with SteelCloud)

It's already on your radar, but you may not have mapped out how you're going to approach it yet: Cybersecurity Maturity Model Certification Level 2+ (CMMC 2+) compliance. If you do (or want to do) business with the DoD as a contractor, and you handle controlled unclassified information (CUI) in the course of that work, you will need to comply with the same 110 NIST 800-171 security controls the DoD complies with. And the way much of the DoD handles cybersecurity compliance is with SteelCloud's ConfigOS cybersecurity automation solution.

ConfigOS helps you save months—if not more than a year—of labor-intensive work to achieve compliance. Getting your compliance infrastructure in place now shows your government clients that you are just as committed to security as they are. Here are the seven benefits of compliance automation that you'll appreciate the most:

1. Reduce the skills gap within your organization.

Finding top security talent is tough—and very costly—if you want to build a Level 2+ program from scratch. Automating CMMC NIST 800-171 requirements reduces talent acquisition costs, increases the return on your CMMC investment, and allows you to become fully compliant using the team you already have.

2. Minimize the cost and effort to comply with CMMC mandates.

Automating your security configurations using NIST-approved checklists reduces compliance costs. Instead of taking the time to figure out the right configurations on your own, you can automate setting and updating them according to recommended configurations. With fewer staff and less time spent on compliance, you can decrease both upfront and ongoing costs.

3. Implement a compliant infrastructure.

The hardest part of compliance isn't getting compliant; it's staying compliant. Sure, you can self-assess and make an attestation, but there's still a question of credibility. Automating security configuration control setting and updating gets you compliant, keeps you compliant and ensures confidence in your compliance for all involved.

4. Provide for continual compliance assurance.

Part of your CMMC assessment is providing a concrete written plan and budget for staying compliant. You can expect new security configurations every 90 days, making configuration management and documentation a heavy lift. Automating compliance lets you regularly remediate your environment against drift and document that you're doing everything CMMC requires.

5. Simplify the ingestion of new control policy updates.

When humans manually handle processes, two things happen. First, they won't improve your security posture at scale. Second, their productivity will decrease as they focus on redundant manual tasks instead of important responsibilities. Using automation to simplify CMMC processes accelerates both organizational and security maturity and maximizes productivity.

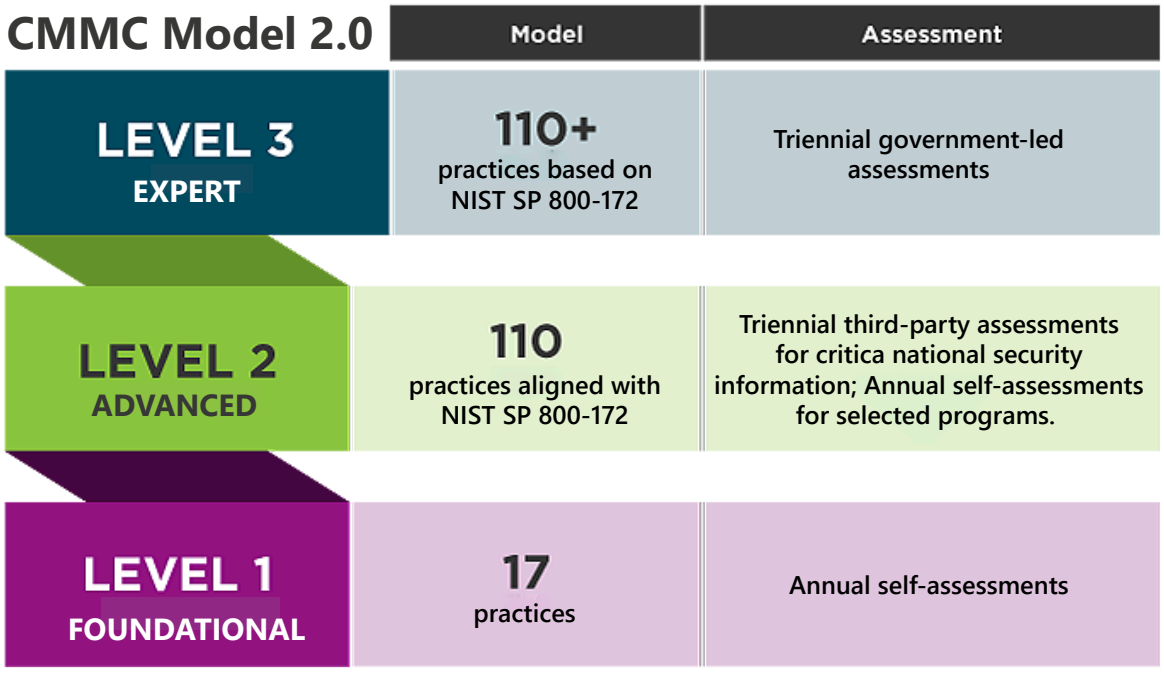
6. Standardize processes for consistency.

Humans make errors and are unpredictable in the delivery of work; systems aren't. Automation removes those risks so you can create consistent, standardized processes over time.

7. Centralize ongoing compliance management.

Managing a security program in silos leads to unnecessary business challenges, including wasteful spending, increased data breach risks, and audit findings. Centralizing operations makes it easier to support your security and compliance posture because it gives you full visibility with continuous assurances for ongoing compliance management.

Key Features of CMMC 2.0



Ensure customers meet their Cyber hygiene expectations.

The DoD's CMMC requirement mandates that DoD contractors obtain certification to ensure appropriate levels of cybersecurity practices are in place to meet "basic cyber hygiene," as well as protect CUI (personally identifiable information, proprietary business information, "For Official Use Only" information, legal information, etc.) that resides on partner systems. This is the first time the DoD will require contractors, subcontractors, and suppliers to be certified to participate in the DoD supply chain.

ConfigOS not only automates the process of securing your systems according to DoD recommendations, it also documents the process for easy reporting. Establishing and maintaining a CMMC-compliant environment using the same automation software the government uses shows the DoD you are serious about cybersecurity, your processes are aligned with theirs and that you prioritize their needs in every detail.

Remain agile in the face of new requirements.

Compliance is not a one-time process. Instead, it is a continuous cycle of assessing the environment, remediating issues, and then reporting and filing. Once the government's first version of CMMC is complete in October 2025, we predict more and more government mandates coming down on industry as we go forward. SteelCloud will be there through all of it, delivering the same solution the DoD uses to address these requirements, protecting both your system and your client relationship.

Trust a proven tool for 800-171 compliance.

You can trust ConfigOS performs and protects the way we say it does because many of your DoD customers have been using it for years to meet 800-171 requirements and beyond. Give them the results they expect with ConfigOS.

Book your free ConfigOS demo at www.steelcloud.com

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**