SteelCloud

A Consultant’s Guide To Lower-Level Controls for CMMC

As plans for implementing the Cybersecurity Maturity Model Certification (CMMC) start to slowly roll out, Certified Third-party Assessor Organizations (C3PAOs), Registered Provider Organizations (RPOs), Certified Assessors (CAs), and Registered Practitioners (RPs) are beginning to mobilize.

While the compliance landscape remains in flux, assessors and practitioners are beginning to prepare themselves and their clients to meet the CMMC requirements. With few formalized approaches, finding a way to help clients achieve and document the appropriate level of compliance can be overwhelming.

With too little guidance and too much work to do, compliance professionals are looking for the solutions that help them establish the processes, practices, and documentation their clients need.

Choose Your Own CMMC Adventure – A GUIDE FOR CMMC CONSULTANTS

While all companies need to meet the same set of standardized requirements to achieve CMMC compliance, C3POs and RPOs can take different paths to getting there. The different approaches often lead to different relationships with clients and different client needs.

The Policy Path

Many C3POs and RPOs previously worked in an agency or in the federal space for most of their career. Informed by this experience, they take an approach founded in either the International Organization for Standardization (ISO), National Institute of Standards and Technology Risk Management Framework (NIST RMF), or Command Cyber Readiness Inspection (CCRI).
Leveraging previous work with federal compliance, these practitioners deliver services by organizing documentation and collecting artifacts.

Identifying the problem

Time spent in the highly regulated federal space often meant dealing with an IT organization. However, the move to working with members of the Defense Industrial Base (DIB) changes that. Working with these clients, assessors, professionals, and practitioners may be working with small IT departments or ones that lack the expertise necessary.

Solving the problem

In this case, the consultant needs to offer the IT staff tools that can get the job done. Getting the client to compliant means helping the IT team find technologies that help them overcome some of the barriers they face, including:

- ✓ Technical skills
- ✓ Time
- ✓ Documentation capabilities

The Full-Service Path

This approach almost looks like being a part-time employee, where the assessor or practitioner provides a full suite of services. The consultant becomes the main point of contact internally rather than directing the internal team on best practices, writing policies and processes, then putting them into practice. The services establish an end-to-end CMMC compliance approach.

Identifying the problem

Because these end-to-end consultants manage everything internally, they often find that the organization's current team lacks the tools needed to put the plan into action. Not only are they unable to direct the IT team, but they are also unable to implement the plan themselves.

Solving the problem

In this case, the consultant knows the steps that the IT team needs to take, but the organization lacks the tools that streamline the implementation. After all, the faster the consultant completes the project, the happier their client is. When looking for a technology to enable CMMC compliance, assessors and practitioners need something that:

- ✓ Enables the client to get compliant
- ✓ Enables documentation
- ✓ Reduces the time getting compliant takes

Creating Your Technology Toolset

No matter what path to compliance consultants take, they need a solution for their clients. Whether the consultant or the client implements the solution, the technology needs to be something that gets the job done and gets it done quickly.

One of the most difficult parts of CMMC compliance is configuring lower-level security technical controls and continuously maintaining them. Consultants need proven, tested technologies that can get the right controls in place and provide the necessary audit documentation.

For consultants working with smaller, overburdened IT departments, the chosen technology needs to provide the following benefits:

- ✓ Ability to overcome the cybersecurity skills gap
- ✓ Automate technical configuration baselines
- ✓ Prioritize control remediation activities
- ✓ Automate remediation actions
- ✓ Enable agility

When it comes to lower-level controls, consultants need solutions that enable their clients to document their controls and answer the following questions:

- ✓ How do you describe what controls you have chosen?
- ✓ How do you keep up to date on emerging threats?
- ✓ Who is going to do the research to continually determine what those controls are?
- ✓ How are you going to document the process of hardening, scanning, producing reporting artifacts or doing that kind of thing?

THE STEELCLOUD SOLUTION for C3PAOS and RPOS

Consultants that require a low barrier-to-entry solution for getting their clients CMMC certified can leverage SteelCloud's patented ConfigOS purpose-built technology to solve many problems that DIB member organizations face. Whether consultants want a technology they can suggest or a technology they can use, SteelCloud's technology provides mission critical hardening capabilities that give DIB member organizations the ability to get and stay CMMC compliant.

SteelCloud designed ConfigOS to respond to four primary problems:

✓ Harden systems
✓ Reduce the technical skills gap
✓ Prevent system downtime
✓ Document controls and exceptions

1 Harden Systems and Maintain Secure Configurations

Consultants whose clients need to set baselines and create documentation around security control configurations can streamline this process with ConfigOS automation. ConfigOS can scan 10,000-20,000 endpoints per hour, supporting even the largest infrastructures. With its patented remediation engine, each instance of ConfigOS can remediate 3,000-5,000 endpoints per hour. ConfigOS helps minimize your clientsclient's IT compliance readiness from week or months to days.

2 Reduce Technical Skills Gap with Automation

Consultants can get their clients' IT teams up and running with ConfigOS in less than a day. The easy-to-use automation reduces the time it takes users to manage configurations and reduces the need for deep, technical skills.

3 Prevent System Downtime with Automated Conflict Remediation and Rollback

Consultants can ensure that their clients' environments never experience downtime arising from CMMC compliance. ConfigOS automates all conflict remediation activities to prevent downtime. Additionally, organizations can create rollback points, ensuring continued productivity and uptime.

4 Document controls and exceptions for continuous assurance

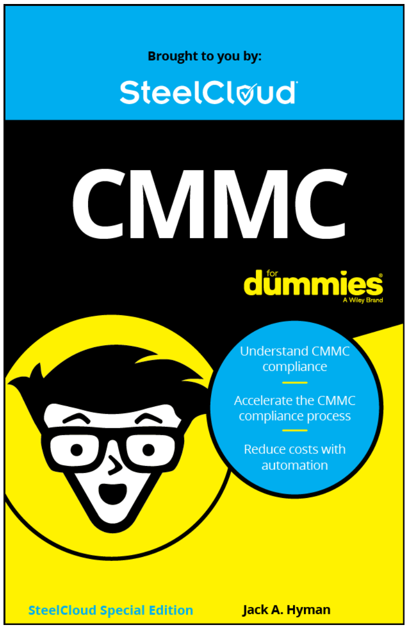
For consultants whose clients need continuous visibility, monitoring, and assurance, ConfigOS's DashView provides IT teams with a single-pane-of-glass for all CMMC compliance documentation and monitoring. The dashboard reduces operational costs arising from cumbersome, time-consuming, manual CMMC reporting processes such as:

✓ Maintaining risk awareness
✓ performing compliance trend analysis
✓ discovering and correcting hardening drift

HOW TO WORK WITH STEELCLOUD

Let SteelCloud help your clients get compliant and get certified. With our patented automation and remediation software, your clients save time, money and manpower as they prepare for CMMC IT related certification requirements.

1. Share our CMMC For Dummies ebook with your clients to help educate them on the process and IT requirements process. It is our CMMC 101 guide that will help your clients get a strong baseline understanding to prepare for the audit, so you don't have to explain it to them.
2. Review our CMMC Control Matrix Crosswalks. To enable NIST compliance readiness, we've created a series of STIG & CMMC Control Crosswalk documents to assist in the Cybersecurity Maturity Model Certification (CMMC) compliance effort, specific to the controls. These documents cross reference the different compliance control sets in relation to the STIG V-IDs .
3. Schedule a demo to see how ConfigOS can help your clients address the IT related STIG/CIS controls for CMMC to prepare for the assessment.
4. Participate in our Partner Referral Program. Call or email us to address any questions you about how we are enabling CMMC readiness today and learn how you can earn by recommending and reselling our offering.


Brought to you by:
SteelCloud
CMMC
for dummies
A Wiley Brand
Understand CMMC compliance
Accelerate the CMMC compliance process
Reduce costs with automation
SteelCloud Special Edition
Jack A. Hyman

**SteelCloud is here to help you help your clients…
get compliant and stay compliant.**

> *DoD contractors required to achieve CMMC Level 2+ are finding the process of getting and staying compliant to be a daunting proposition without automation. For more than a decade, SteelCloud compliance software has been implemented across the DoD, and we are glad to assist Defense Industrial Base contractors with their CMMC compliance requirements. - Brian Hajost, SteelCloud President and CEO*

SteelCloud
20110 Ashbrook Place, Suite 170
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**