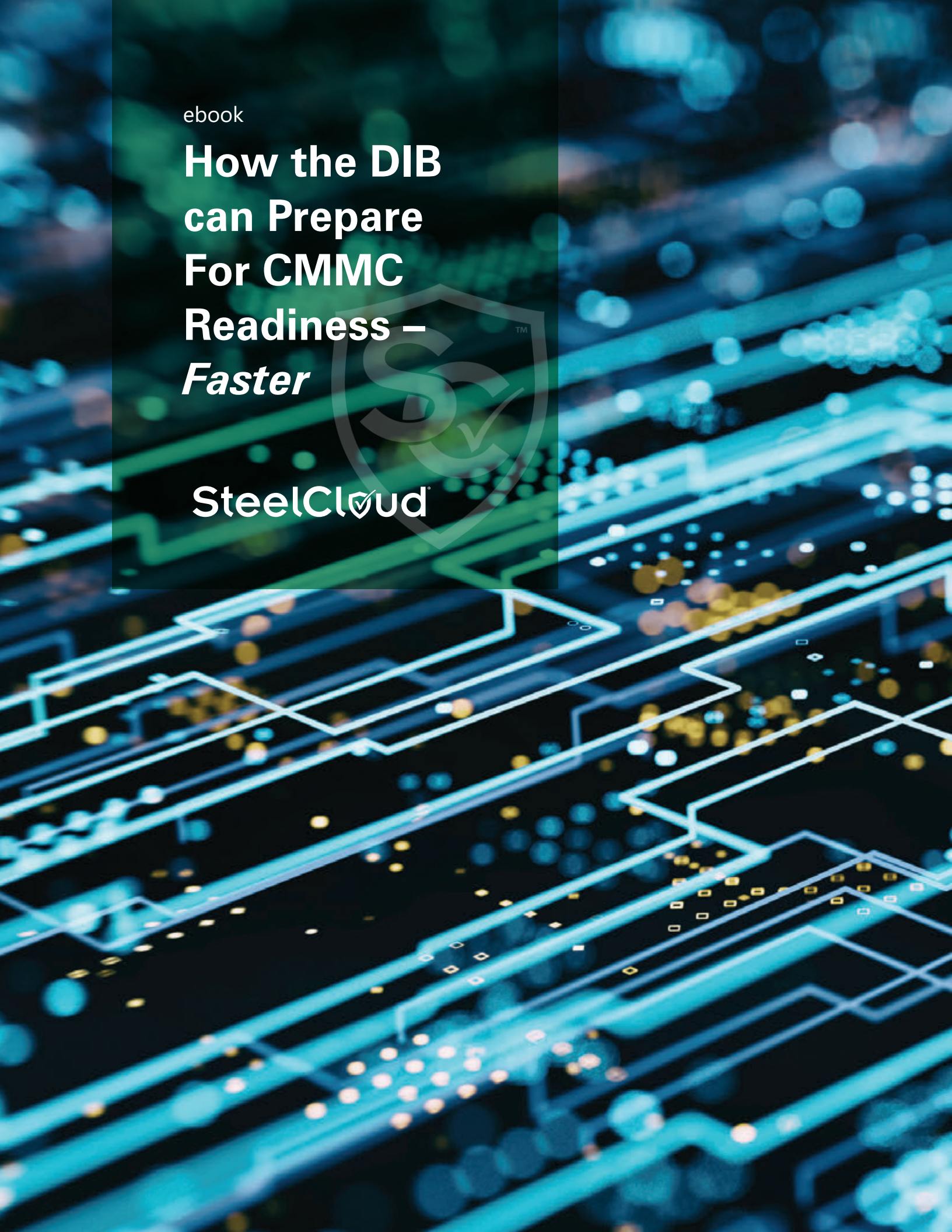

ebook
How the DIB can Prepare For CMMC Readiness – *Faster*
SteelCloud

Each year, hackers and other mal actors grow ever more sophisticated in infiltrating government systems. And the government is keeping pace by issuing security practices and processes to protect our nation's data. For example In February 2020, the Department of Defense (DoD) released Cybersecurity Maturity Model Certification (CMMC) standards. CMMC creates a set of cybersecurity best practices that draw from multiple, proven cybersecurity standards, frameworks, and references. The DoD intends for CMMC to standardize cybersecurity implementations across the Defense Industrial Base (DIB), including those in the commercial and supply chain audience.

This directive enhances security procedures for controlled unclassified information (CUI) in all unclassified networks. Without a standard for protecting these networks, many DIB member companies often have fewer controls safeguarding CUI. This makes unclassified networks a path of least resistance for adversaries — if an unauthorized attacker gained control of the identity capabilities at one agency, the access could be used to compromise other federal networks.

The CMMC directive changes how DIB members secure data and document their activities.
On November 4, 2021, as part of an update to the CMMC program, dubbed CMMC 2.0 was announced.

CMMC 2.0 makes compliance easier for the DIB.

Initially, CMMC required contractors to adhere to one of five levels of security and gain third-party verification of their compliance. CMMC 2.0 eases some of that burden by:

✓ Changing the number of CMMC Levels.

The number of levels in CMMC 2.0 was reduced from 5 to 3, streamlining and clarifying the effort. Levels 2 and 4 are now gone. Old Level 1 becomes CMMC 2.0 Level 1, and it covers those contractors who deal with Federal Contract Information (FCI). Old Level 3 becomes CMMC 2.0 Level 2 and covers those who deal with CUI. And Old Level 5 becomes CMMC 2.0 Level 3 and covers those who deal with CUI on critical programs.

✓ Simplifying processes.

CMMC 2.0 removes some controls and the "CMMC unique" processes from the mandate, aligning CMMC 2.0 more closely with existing NIST 800-171 or CIS practices at Levels 1 and 2, though this part is not entirely clear yet. Level 3 will now comply with NIST-172 practices. This change allows companies to rely on tools that have been in use in the government for years, such as automated scanning, remediation and continuous monitoring of controls. In addition, the requirement to manage policies, procedures, and resource plans were also eliminated.

✓ Enabling self-assessments.

The new rules allow for self-assessment at Level 1, saving small and mid-size businesses the costs of independent certification through the CMMC Accreditation Body. At Level 2, some may self-assess, while others require independent assessment, depending on the data you handle. The exact criteria for that has yet to be determined. Prior to CMMC 2.0, all DIB businesses had to obtain and pay for the third-party assessment.

✓ Issuing POAMs and waivers.

2.0 provides additional flexibility to organizations by allowing plan of actions and milestones (POAMs) and a waiver process that can waive certification on a limited basis and in mission-critical instances.

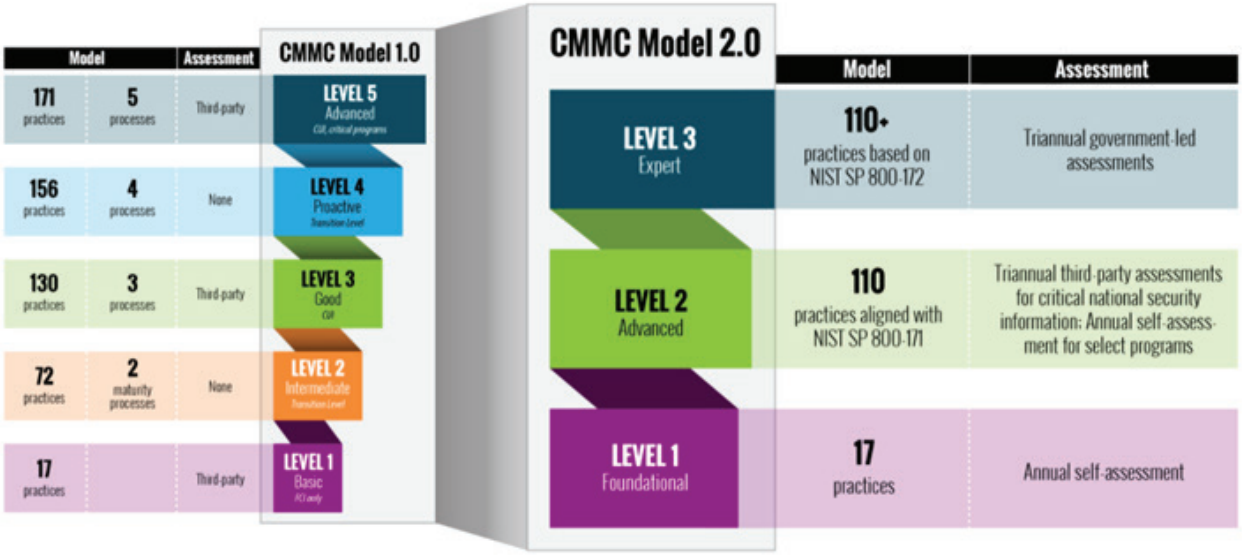
One big word of caution here is that these new changes are what we know of the DoD's intent. The exact rules and how they apply are not yet carved in stone. The final rulemaking process is expected to take 9-24 months, meaning the final determination will come between September 2022 and November 23. Until then, it is recommended to act as if the rules were final and begin aligning your organization to the practices required at your level (see graphic next page).

Defense contractors will need to achieve one of three levels of cybersecurity.

Depending on what you do for the government and the sensitivity of the DoD information you'll need to protect, you'll have to conform to one or more of three levels of cybersecurity. At the low end, you'll need to implement 17 basic cyber hygiene practices to protect Federal Contract Information (FCI)—data every government contractor has that is not open to the public.

Once you deal with CUI, your requirements will increase to meet Level 2 compliance using NIST SP 800-171 or Level 3 compliance using NIST SP 100-172. These NIST requirements consist of the same controls and checklists the DoD uses internally to protect data, aligning your products and services with their existing mandates.

KEY FEATURES OF CMMC 2.0

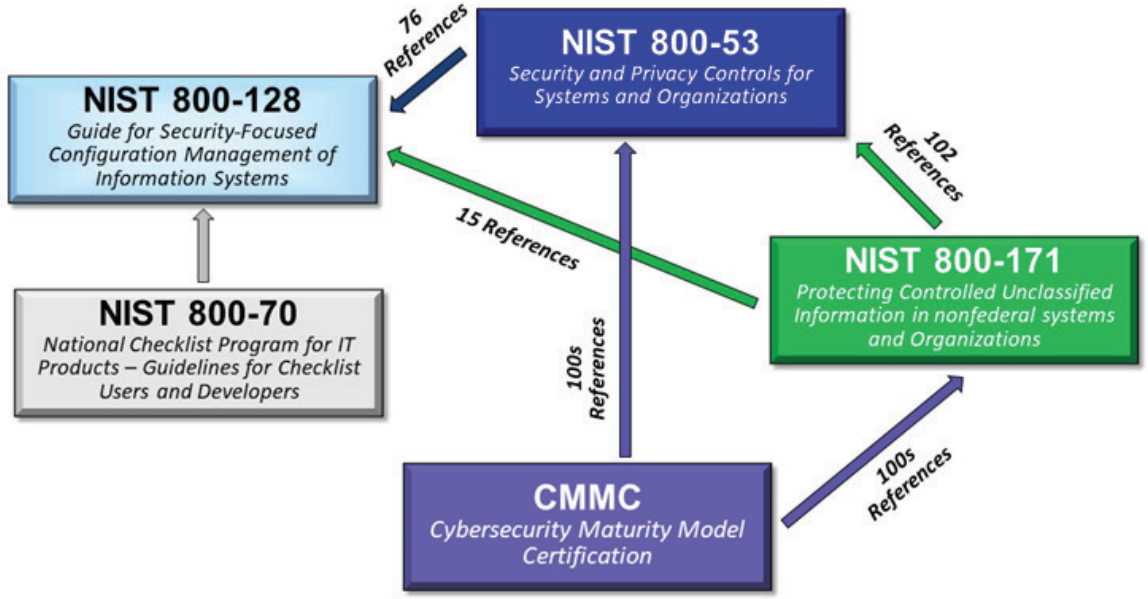


https://www.acq.osd.mil/cmmc/about-us.html

Before you can comply with CMMC 2.0 at Levels 2 and 3, you'll need to know about NIST.

As you start building out your CMMC compliance program at Levels 2 and 3, you might find yourself mired in the cross-referencing built into the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. NIST publications like 800-171 contain vital details and instructions to meet CMMC requirements. But there's a catch: It's all very confusing. CMMC references NIST 800-171, which references NIST 800-53, and NIST 800-128. NIST 800-53 further references NIST 800-128. NIST 800-128 relies on NIST 800-70 to set secure configurations. Clear as mud, eh?

Cyber Hygiene Document Relationships



Each NIST document contains controls, checklists, and processes you need to meet to comply with CMMC. In essence, they are the "what" that you are trying to achieve. Here is what each of the interrelated and cross-referenced guides covers:

NIST 800-171—Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST 800-53—Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-128—Guide for Security-Focused Configuration Management of Information Systems

NIST SP 800-70—National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

NIST SP 800-128 and NIST SP 800-70 provide the technical foundation for creating a security-focused configuration management program. You can then use documentation of these controls to prove compliance with CMMC.

But wait, you also need to know about STIGs.

NIST 800-70 explains that the first place to look for configuration controls is NIST-produced checklists. However, it also points out that agency-produced checklists from the Defense Information Systems Agency (DISA) should be used where no NIST checklist exists.

If you're looking to meet Level 2 or 3 CMMC compliance, DISA Security Technical Implementation Guides (STIGs) are the security configuration checklists that meet Department of Defense (DoD) requirements. Each technology product that your environment uses will have a STIG associated with it. Getting compliant means implementing these secure configurations and maintaining them.

However, getting compliant can be a struggle. Often, the STIG for one technology breaks another one. Often, companies choose to set waivers, or exceptions, to these controls because finding a way to account for them becomes overwhelming.

If getting compliant is hard, staying compliant is even more difficult. Every 90 days, DISA updates STIGs, meaning that you have to implement the changes and prevent additional downtime from conflicts.

Add it all up and it's a LOT of work.

To give you an idea of how cumbersome and complex CMMC compliance can be, here is an example. NIST 800-53 outlines the security and privacy controls for information systems and organizations. There are 20 control families:

- ✓ Access Control
- ✓ Awareness and Training
- ✓ Audit and Accountability
- ✓ Assessment, Authorization, and Monitoring
- ✓ Configuration Management
- ✓ Contingency Planning
- ✓ Identification and Authorization
- ✓ Incident Response
- ✓ Maintenance
- ✓ Media Protection
- ✓ Physical and Environmental Protection
- ✓ Planning
- ✓ Program Management
- ✓ Personnel Security
- ✓ Personally Identifiable Information Processing and Transparency
- ✓ Risk Assessment
- ✓ System and Services Acquisition
- ✓ System and Communications Protection
- ✓ System and Information Integrity
- ✓ Supply Chain Risk Management

Companies trying to meet NIST 800-53 baselines often find section 5, "Configuration Management," the most challenging. This control family consists of 14 categories of controls, totaling 56 controls.

While NIST 800-171 only lists 9 security requirements for this control family, embedded in those 9 are 800-53's 14 control categories and 56 controls. In other words, NIST 800-171, which is CMMC 2.0 Level 2 compliance, squashes many requirements into a tiny, not-so-neat package covering everything from registry settings and access controls to data processing preferences and permissions across every system and device. So, organizations that need to meet compliance have to put a great deal of work into each of these 56 controls, and that's still only one control family out of twenty!

3 steps to setting CMMC security baseline configurations

Now that you know where all the checklists and controls come from, you can start getting into the exact details of setting your security configurations. We have narrowed your task list down to three action items.

1. **Determine local requirements.** Before you can start putting controls in place, you need to know your security risks and define threats you need to mitigate. According to NIST, the risk mitigation methodology should include:

    a) Identify functional needs: understanding how end-users will use the product helps define the security needs

    b) Identify threats and vulnerabilities: identifying the potential threat sources that apply to a specific IT product or system helps set baseline controls

    c) Identify security needs: determining security controls that minimize or eliminate threats better secures systems, networks, and software

2. **Browse and retrieve checklists.** Once you determine the local requirements, you can start collecting information about securing your environment. The National Security Checklist Program Repository contains all the checklists available for download. You can process these checklists with Security Content Automation Protocol (SCAP) validated products. NIST categorizes checklists based on content type, like:

    a) Prose: narrative descriptions for manually configuring a product

    b) Automated: documented in machine-readable format but do not fully match SCAP requirements

    c) SCAP Content: machine-readable standardized SCAP format that SCAP-validated product can process

    Although you can use any of these three content types to set your baselines, SCAP-expressed checklists make it easier to consistently and efficiently maintain low-level security controls.

3. **Apply checklists to IT products.** Finally, you apply the checklists by either modifying the product's setting or verifying existing settings. Some best practices include:

    a) Modification:

        1. Test in a non-operational environment to minimize any conflicts that can lead to downtime.
        2. Review the Rollback Capability field to determine whether you can revert to the original configuration.
        3. Back up the original configuration before making any changes.
        4. Back up all critical data files in case you need to restore the system to pre-checklist configurations

    b) Verification: after reviewing and testing, ensure that product settings are not inadvertently altered.

3 tips for managing CMMC security configurations.

Understanding CMMC 2.0 Level 2 and 3 security configurations gives you a better visualization of how to organize your approach and prioritize your activities. NIST SP 800-128 is the "Guide for Security-Focused Configuration Management of Information Systems." Although security configurations themselves live in the repository, 800-128 guides you through the steps to create a configuration management process.

Here are three tips for managing security configurations:

1. **Break systems into configuration items (CIs).** A configuration item is a group of system components treated as a single entity for the Security-focused Configuration Management (SecCM). Examples of CIs include:

   a) Specific system components: servers, workstations, routers, or applications

   b) Group of system components: grouping together servers that have the same operating system, similar network components like routers and switches, or a suite of applications

   c) Non-component object: firmware, documentation

   By breaking systems into CIs, you can take a more granular approach to configuration management, giving you more control over managing the system's security configurations.

2. **Set baseline configurations.** Baseline configurations are the formally reviewed and agreed-upon set of specifications for a system or CI within a system that you use as the basis for future builds, releases, or changes. After setting these, changes can only be made according to your organization's formal change control procedures.

   When you change the configuration baseline, you agree that anything different from the previous baseline is now the new approved configuration. However, as a best practice, you should maintain older versions of the baseline configurations so that you can "roll back" or revert to those configurations. This practice protects you in case the new configurations create a problem for your systems.

3. **Do a security impact analysis.** Before you change a baseline configuration, you should analyze how it could impact your overall security. Systems tend to be in a constant state of flux. A robust security posture requires analyzing how functionality changes can impact security controls or impact your data breach risk.

   It is essential to keep your organization's risk tolerance in mind. Before implementing a configuration change, you should make sure to review NIST 800-53's Configuration Management impact analysis best practices, including:

   a) Ensure anyone engaging in the impact analysis has the appropriate skills and technical experience

   b) Review security and privacy plans, policies, and procedures to understand control requirements

   c) Review system design documentation and operational procedures to understand how changes might impact controls

   d) Review potential impact on supply chain partners

   e) Determine potential to create new risks to people's privacy

   f) Review how to mitigate potential risks

   g) Create a separate test environment that is physically or logically separate from the operational environment

   h) Verify controls are implemented correctly and operate as intended without negatively impacting security and privacy

Your one saving grace: automation.

As you start to figure out how to get your company CMMC compliant, you probably noticed that establishing low-level controls that meet the high-level requirements is far more complicated than you realized. Setting CMMC security baselines is a fundamental step to getting compliant, and automating continuous control compliance is the way to stay that way.

While you can find all the controls and STIGS, you need to meet online, making sure you've found them all is a challenge. Then ensuring you're up to date is a struggle. The process of scanning and remediating issues is cumbersome and highly specialized. Then there's the element of human error to consider. It's a lot. And considering your government contract and relationships hang in the balance, it's a heaping helping of a lot.

The good news is that automation support enables currency, completeness, accuracy, and availability of your system's baseline configurations. SteelCloud's ConfigOS automates STIG compliance so you can meet NIST 800-171 and 172 compliance requirements faster for Level 2 and 3 compliance. Our unique patented technologies remove the barriers associated with maintaining STIG compliance while reducing the staffing and time costs associated with system hardening.

Our automated tool scans your systems against the Security Technical Implementation Guide (STIGs), tells you the number of compliant controls you have in place, remediates any non-compliant configurations, allows you to document your waivers for easier review in the future, and enables continuous maintenance of controls. ConfigOS provides easy-to-use automation that not only gets you compliant but keeps you compliant.

Dealing with complex controls and checklists is not your core competency but it is essential to your customer. Automating the process will save costs and allow you to maintain compliance so you can focus on more critical initiatives. Contact us for a demo today for more information about how SteelCloud's ConfigOS can harden systems, keep you compliant and maintain your trusted relationship with the government.

https://www.steelcloud.com/cmmcfordummies/

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