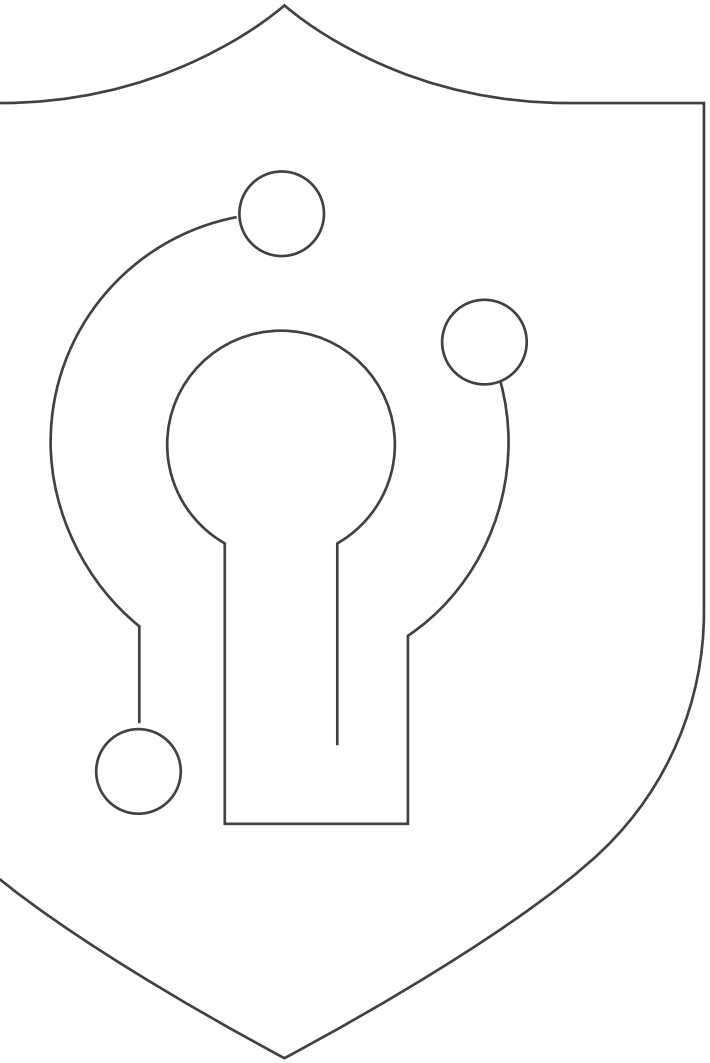
How to Get CMMC Certified

For organizations seeking clarification on the Cybersecurity Maturity Model Certification (CMMC) process, we walk through the 7 steps that can take you end-to-end—from establishing your scope to remediating gaps, this detailed whitepaper will help demystify a complicated and evolving compliance process for those seeking to do business with the Department of Defense.

schellman
Quality, above all.

WHITEPAPER



For those of you considering CMMC, this new certification affecting contractors in the Defense Industrial Base (DIB) defines three levels—your level of certification will depend on the types of DoD information exposed to or handled by your organization:

- **Level 1:** FCI only
- **Level 2:** CUI and FCI
- **Level 3:** Highly sensitive CUI

For those of you who will need to undergo Level 2 or 3 certifications, what can you expect from your CMMC process?

As one of the first authorized C3PAOs, we're going to lay out 7 steps that should take you from initial and crucial preparatory steps through your actual assessment and remediation. As the entire DIB prepares to accommodate the new CMMC requirements, this information will help you get a leg up on how you should proceed.

(As a word of caution, the final rule has not yet been completely defined and further changes and clarifications are anticipated in the interim. Take this into account as you prepare for your assessment.)

The 7 Steps of the CMMC Process

Step 1: Establish Scope

You define the scope of your CMMC environment. It should encompass:

- **Any of your assets that process FCI or CUI**
  - Including (but not limited to) anything that is used to access, enter, edit, generate, manipulate, or print information.
- **Any of your assets that store FCI or CUI while it's inactive or at rest**
  - Includes electronic media, system component memory, and physical formats such as paper documents.
- **Any of your assets that transmit FCI or CUI**
  - These are defined as any means of transferring information from one asset to another asset (e.g., data in transit using physical or digital transport methods).
- **Any assets that support security functions for those mentioned above** (regardless of whether or not the security assets process, store, or transmit CUI themselves)

You'll need to create a detailed inventory of these in-scope assets—you may also need to extend it to include systems or services provided by third parties, depending on if they provide assets that fall into any of these categories. That includes external people, procedures, locations, and technology.

(**An important note:** Should the assets affiliated with supporting organizations be included as part of your CMMC Assessment Scope, those organizations themselves would NOT receive a CMMC Certification during the assessment.)

Step 1: Establish Scope (cont.)

Considerations for the several asset categories to include are outlined below:

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
CUI Assets	Assets that process, store, or transmit CUI.	• Document in the asset inventory. • Document in the System Security Plan (SSP). • Document in the network diagram of the CMMC Assessment Scope. • Prepare to be assessed against CMMC practices.	Assess against CMMC practices.
Security Protection Assets	Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI.		

Contractor Risk Managed Assets	• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place.
	• Assets are not required to be physically or logically separated from CUI assets.
		• Document in the asset inventory.
		• Document in the SSP.
		  • Show these assets are managed using your risk-based security policies, procedures, and practices.
		• Document in the network diagram of the CMMC Assessment Scope.
			• Review the SSP in accordance with practice CA.L2-3.12.4.
			  • If appropriately documented, do not assess against other CMMC practices.
			  • If your risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks.
			  • The limited spot check(s) shall not materially increase the assessment duration or the assessment cost.
			  • The limited spot check(s) will be within the defined assessment scope.

Step 1: Establish Scope (cont.)

Considerations for the several asset categories to include are outlined below:

Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Specialized Assets	• Assets that may or may not process, store, or transmit CUI • Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment	• Document in the asset inventory. • Document in the SSP. • Show these assets are managed using your risk-based security policies, procedures, and practices. • Document in the network diagram of the CMMC Assessment Scope.	Review the SSP in accordance with practice CA.L2-3.12.4 • Do not assess against other CMMC practices
Assets that are not in the CMMC Assessment Scope			
Out-of-Scope Assets	Assets that cannot process, store, or transmit CUI	Assets are required to be physically or logically separated from CUI assets	None

(This table is republished from the OUSD's CUI level 2 scoping guidance document located here.)
For more detailed scoping guidance, the Office of the Under Secretary of Defense (OUSD) has provided that here.
We also wrote on how to use PCI context to further simplify your scoping process.

Step 2: Develop Your SSP and Verify Implementation of Practices

The System Security Plan (SSP) is an integral part of your assessment process. Within it, you'll collect the essential points that will be evaluated in the assessment, including the following:

- Points of contact within your organization who are responsible for the environment and its security.
- A description of the environment with pictorial diagrams identifying the several components that have been determined to be in-scope.
- In-depth details regarding how each practice (and subcomponent practices detailed in the Assessment Procedures or NIST 800-171A) is implemented.

At this point, you must consider how your implemented practices may be evidenced—it's not enough to plan. Your assessment process will require proof that practices stated in the SSP are in place.

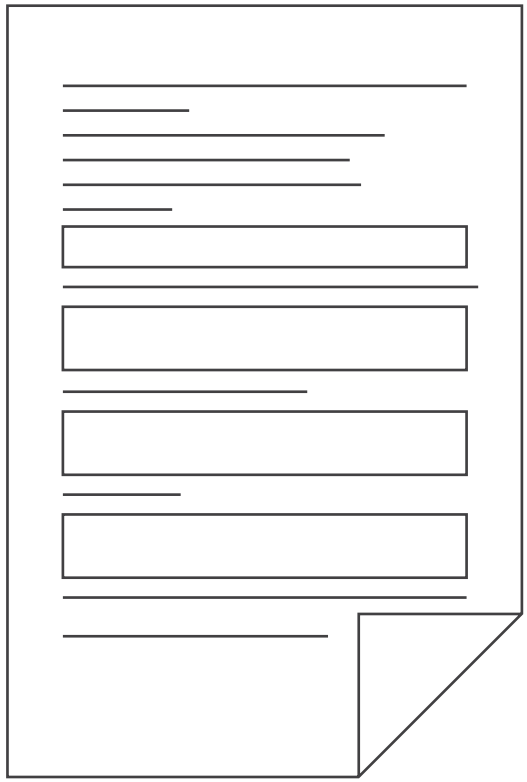
To help expedite that process when the time comes, you should validate the implementation of each practice in advance of your assessment. For further direction here, the OUSD provides a guide that describes each of the assessment objectives for the several practices in detail, including examples of how they may be assessed.

- **Here's an extra tip from us:** As encryption that is implemented in support of CMMC practices must be supported by FIPS 140-2 validated encryption mechanisms, compile a catalog of the "Cryptographic Module Validation Program" (CMVP) numbers for all of your encryption mechanisms in advance.

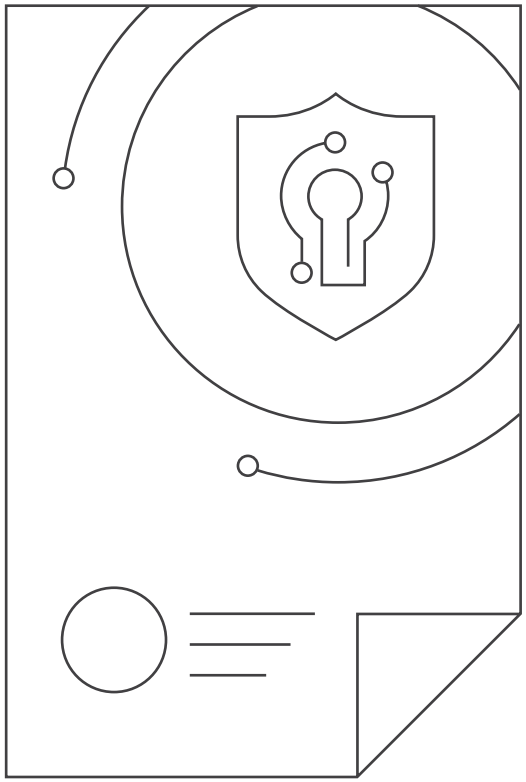
Step 2: Develop Your SSP and Verify Implementation of Practices (cont.)

Helpful Tools to Develop Your SSP:

Example Template
for the SSP



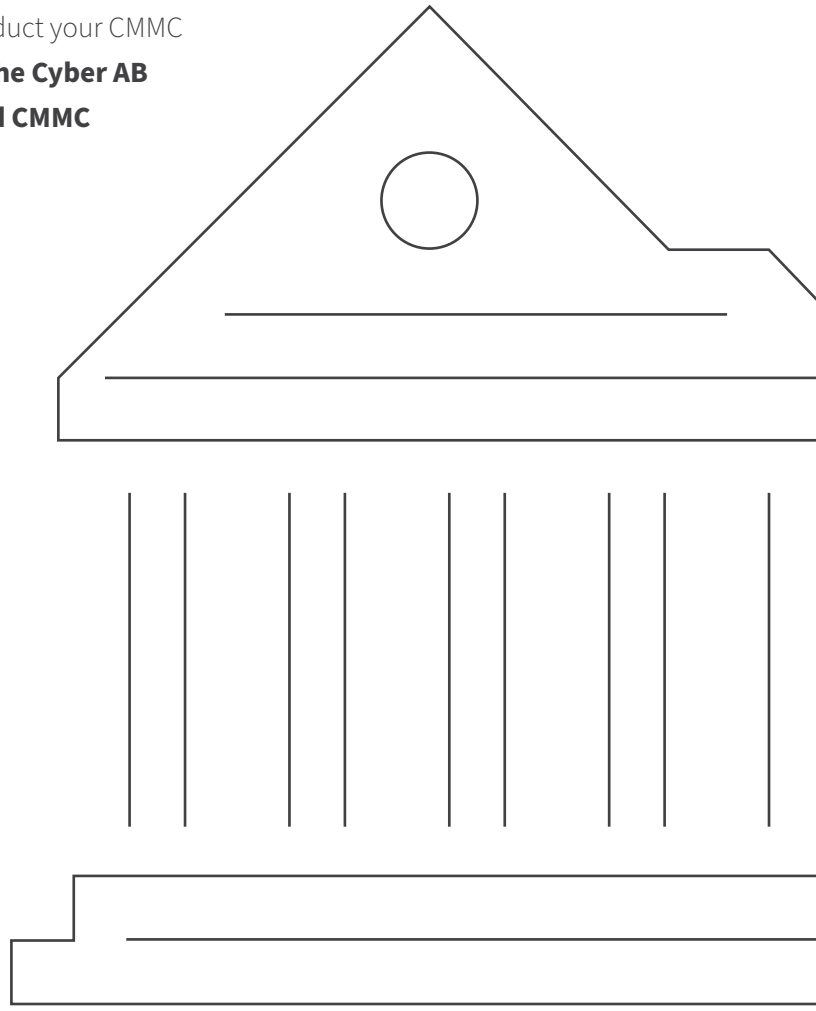
Details on the Intent of Each Practice and
Examples of How They May Be Addressed



Please note that the format and content of your SSP are wholly at your discretion.
The template provided should be considered as an example of what is commonly adopted.

Step 3: Identify a C3PAO

At this stage, you'll need to find a C3PAO to work with—this independent organization will conduct your CMMC assessment and provide the results to the appropriate governing bodies. **To make it easier, the Cyber AB (formerly The CMMC Accreditation Body) maintains a marketplace where all approved CMMC organizations and individuals are identified (including Schellman).**



That marketplace can also be a source for other approved CMMC resources, including:

- Registered Practitioners & Organizations (RPs and RPOs)
- Licensed Training Partners (LTPs)
- Certified Professionals and Assessors (CCPs and CCAs), among others

These organizations and professionals provide different services to various entities within the CMMC ecosystem depending on their role:

- **RPs and RPOs:** Typically aid in CMMC preparation
- **LTPs:** Provide authorized training regarding the ecosystem
- **C3PAOs and CCAs:** Perform assessment activities

Step 4: Define Your Internal Assessment Team

While your C3PAO will be performing the actual assessment procedures, your organization will still need to play a critical part. **You'll need to field a team who will interact with the C3PAO in the following roles:**

- **Assessment Official (AO):** This will be your most senior representative who is directly and actively responsible for leading and managing your engagement in the assessment, including decision-making authority. Your AO must be an employee (i.e., not outsourced).
- **Point of Contact (PoC):** This person will be responsible for daily coordination and liaison support between you and the C3PAO assessors. Unlike the AO, the PoC doesn't necessarily have to be an employee—you could choose to put a contractor, consultant, or advisor, such as a CMMC Registered Practitioner (RP), in the role.
- **Subject Matter Experts (SME):** SMEs should be your employees or consultants who are responsible for the assets, practices, or procedures to be assessed.

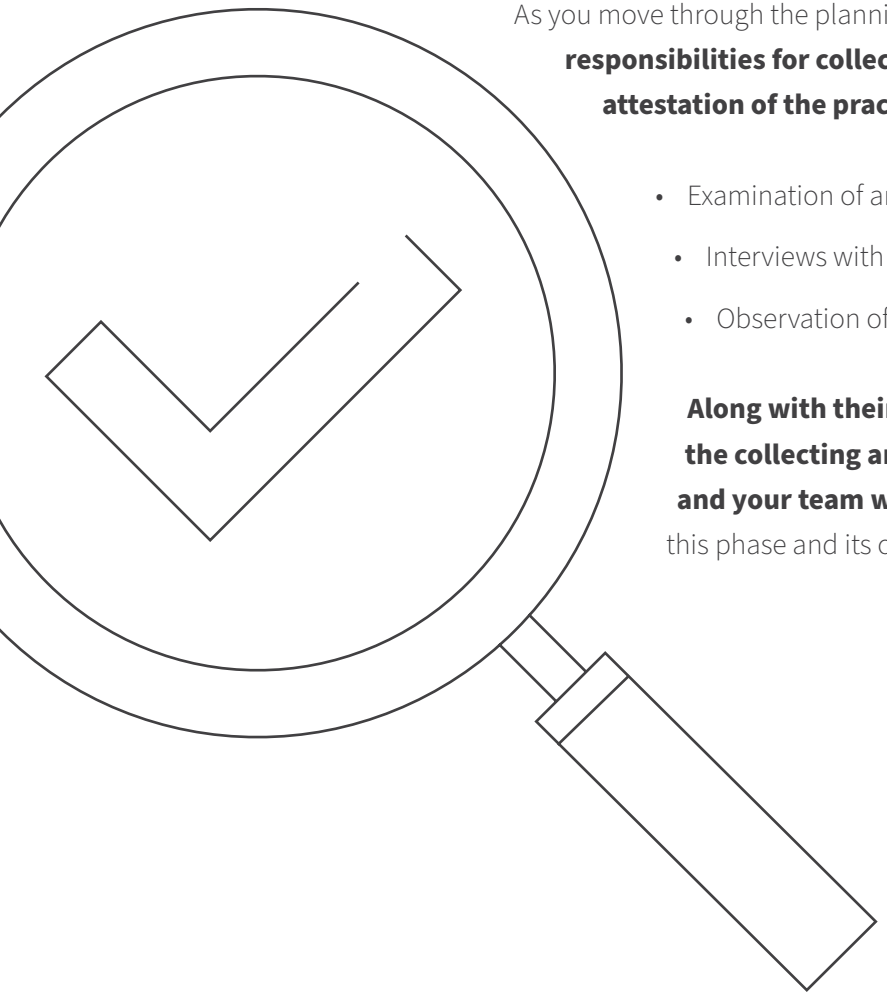
Together, the AO and POC will coordinate all assessment activities with your C3PAO. If you do choose to go outside your organization to fill the PoC role, remember that you must avoid any conflict of interest with your C3PAO to ensure the integrity and validity of the assessment (e.g., don't put someone from your C3PAO in that role).

Step 5: Plan Your Assessment with Your C3PAO

In getting started planning your assessment process, you should communicate the general parameters of your requirements, including:

- Any previous self-assessments you've done.
- Your estimated timeframe for beginning the assessment.
- Information system architecture, boundary, and inventory.
- The physical location of your in-scope assets.
    - As previously mentioned, you'll initially determine the assessment scope, but it will then be validated by the C3PAO, who may request you extend it to ensure that all assets supporting FCI and CUI are included as appropriate.
- Any inheritance or shared responsibility with a managed service provider, cloud service provider, or other. Be prepared to discuss how your organization has implemented any customer responsibilities as indicated by the service provider in their Customer Responsibility Matrix (CRM).
    - **Inheritance** refers to your compliance by virtue of another organization's status.
        - For example, if AWS GovCloud or Microsoft GCC High, or any other Infrastructure-as-a-Service (IaaS) hosts your infrastructure, then the IaaS would be responsible for controlling physical access to the data center and you could inherit the practice implementation from the IaaS for CMMC Practice PE.L1-3.10.1 concerning physical access to facilities.
    - Your customers or partners may also be required to **share responsibility** for complying with certain CMMC practices.
        - For example, a customer may connect a workstation that they manage to your system, giving them access to CUI. You may not have direct responsibility for the protection of CUI on their workstation, so the responsibility would be shared between you and your customer/partner for CMMC practice SC.L2-3.13.16 concerning the protection of data at rest.

Step 5: Plan Your Assessment with Your C3PAO (cont.)



As you move through the planning phase, **your C3PAO will identify methods, techniques, and responsibilities for collecting, managing, and reviewing evidence necessary to support the attestation of the practices, which may include the following:**

- Examination of artifacts (such as policies, procedures, reports, inventories, configurations, etc.)
- Interviews with SMEs (either virtually or in person)
- Observation of tests/demonstrations of evidence (either virtually or in person)

Along with their chosen approach to testing, how the C3PAO decides to proceed with the collecting and compiling of evidence will affect the amount of time and effort you and your team will need to allow for preparation activities. As such, you should consider this phase and its outcome when determining the scheduling and budgeting of the assessment.

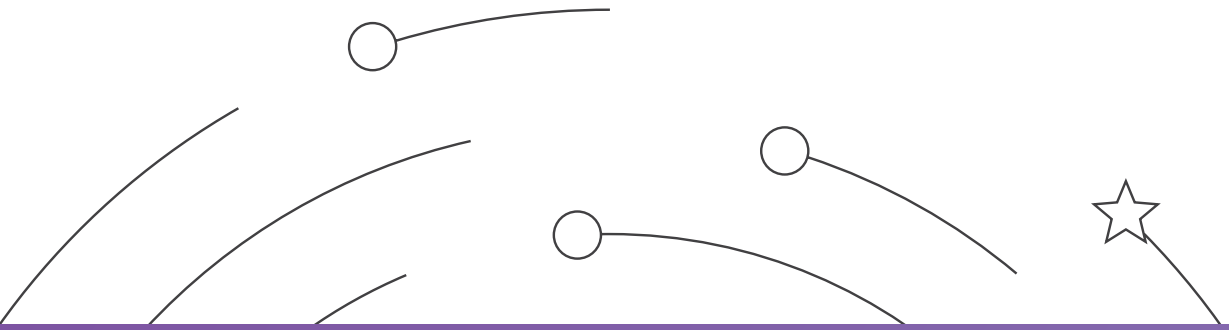
Step 6: Conduct the Assessment

After 5 phases, we've finally arrived at the CMMC assessment, which consists of the actual review of the evidence you'll have previously collected, interviews with the assessors, and demonstration of practices in place, as well as the addressing of any questions that come up.

During the assessment, your C3PAO will verify the "adequacy" and "sufficiency" of evidence to determine whether your practices have "met" or "not met" the CMMC standard. As they identify, describe, and record any gaps in procedures, they will present these to you daily.

- **For evidence to be "adequate"**—i.e., whether a given artifact, interview response, demonstration, or test meets the CMMC practice—it must answer this question: "Does the team have the right evidence?"
- **For evidence to be "sufficient"**—i.e., whether it provides the support necessary to verify coverage by domain, practice, or operating units—it must answer this question: "Does the team have enough of the right evidence?" (as per section 2.2.5 and page 25 of CMMC Assessment Process (CAP) v1.0)

(If you disagree with a judgement of "not met" made on a practice and there is substantial evidence showing that all the objectives of that practice have been met, Cyber AB is expected to develop an appeals process to dispute adverse findings.)



Step 7: Remediate Gaps

Aside from appealing the assessment results, **CMMC will allow the conditional use of plans and designations on practices that are not fully or successfully implemented. The CAP's guidance for these situations is summarized below:**

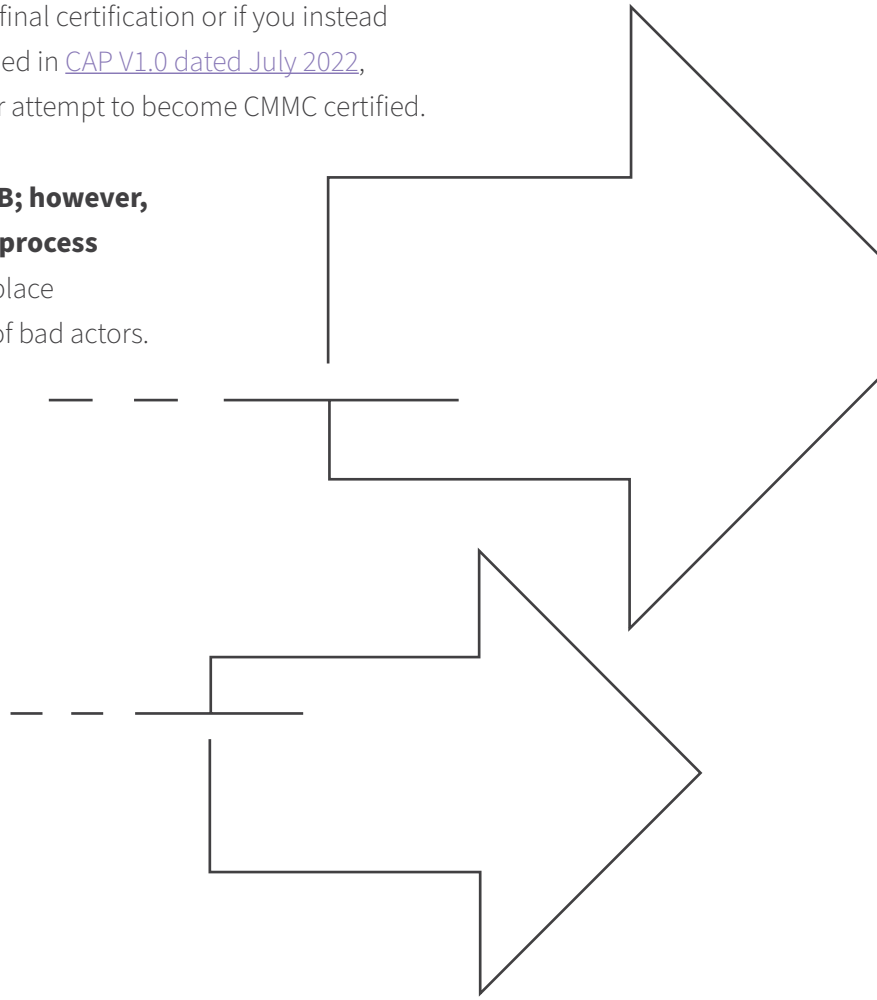
- **Plans of Action and Milestones (POA&M)**
  - These are strictly time-bound with a validity period of no more than 180 days from the completion of the assessment.
  - The most sensitive or critical requirements cannot be remediated, as per section 2.4.1.1 and page 28 of CAP v1.0.
    - Cyber AB and DoD are expected to deliver further clarification on what will be considered acceptable deficiencies as the final rule is decided upon.
- **Limited Practice Deficiency Correction Designation**
  - For practices that may have been effectively implemented, but not necessarily documented correctly, or are missing minor updates—e.g., updates to policy signatures, procedural documentation that exists but is outdated, etc.
  - Practices that could lead to significant exploitation of the network or exfiltration of CUI are not eligible for this designation, as per section 2.3.2.2 and page 27 of CAP v1.0.
    - Again, Cyber AB and DoD are expected to deliver further clarification on what will be considered acceptable deficiencies as the final rule is decided upon.
  - **To upgrade a practice under this designation to a status of "met," you must provide evidence within five (5) calendar days from the final findings briefing or within a timeframe deemed acceptable by the C3PAO.** For any practices where evidence still shows the deficiencies, the score will remain "not met" and be placed under a POAM.

Moving Forward with CMMC

Your level of compliance with CMMC practices will determine whether or not you achieve final certification or if you instead will be awarded conditional or interim certification with more work to be done (as identified in CAP V1.0 dated July 2022, sections 2.4.1 and 4.1). Regardless of the outcome, these are the 7 steps you'll take in your attempt to become CMMC certified.

The implementation of CMMC will pose challenges for many contractors in the DIB; however, with the proper preparation and support, you'll be able to progress through this process to achieve certification. In the end, ensuring that strong cybersecurity practices are in place across the board will help keep our nation's most sensitive information out of the hands of bad actors.

If you find you have any further or more specific questions, please reach out to us today to learn more about how we can support your organization in both CMMC training and assessments.



CLICK FOR MORE INFO

www.schellman.com
4010 W Boy Scout Blvd
Suite 600
Tampa, FL 33607
1.866.254.0000
Outside of the United States,
please dial: +1.813.288.8833