



CMMC Assessment Preparation Guide

*How I Learned To Shut The Fuck Up When
Dealing With DIBCAC / C3PAO Assessors &
Embrace Awkward Silences*

Version 2021.3

Disclaimer: This document is for educational purposes only and does not render professional services - it is not a substitute for dedicated professional services from a competent cybersecurity professional. If you have compliance questions, you really, really, really need to consult a competent cybersecurity professional to discuss your specific needs.

We do not warrant or guarantee that the information will not be offensive to any person. You are hereby put on notice that by accessing and using this document, you assume the risk that the information and documentation contained in the document may be offensive and/or may not meet your needs and requirements. The entire risk as to the use of this document, or its contents, is assumed by you. **If you don't like these terms, then tough shit - don't use the document or any of the content it provides... go do your own research and work, since it will be good for you.**



Understanding Your Goal Of A Successful CMMC Assessment & How To Achieve It

Your goal is to pass a CMMC assessment. It is imperative that you avoid unforced errors. In audits/assessments, unforced errors are primarily due to the assessee lacking the ability to answer a question in a concise and straightforward manner.

How do you prevent unforced assessment errors? It starts with proper, prior planning, but it also involves educating those involved in representing the Organization Seeking Certification (OSC) on how to shut the fuck up and not derail the assessment. That may sound harsh, but it is the simple fact of the matter. Human nature is your enemy with a CMMC assessment since people tend to:

- Talk when they are nervous (with contracts on the line, a CMMC assessment is a great source for anxiety);
- Want to make friends with the assessor;
- Want to impress the assessor(s) with their expertise;
- Feel the need to fill-in periods of awkward silences; and
- Bullshit their way through answers if they are not comfortable or competent with the subject.

Remember That You Are Far Too Pretty For Prison

In October 2021, the Department of Justice (DOJ) launched its Civil Cyber Fraud Initiative (CCFI) and with the explicit mission of going after federal contractors under the False Claims Act (FCA) to prosecute government contractors that “fail to follow required cybersecurity standards.” The CCFI will provide whistleblower protections for those disgruntled cybersecurity practitioners who get fed up with lip service from their management team and report violations. Additionally, the FCA has a “finder's fee” component that incentivizes whistleblowing which can make it financially beneficial for disgruntled cybersecurity practitioners to turn in companies that violate compliance obligations.

Why is this important? If your organization is able to “self-attest” to NIST SP 800-171 and/or CMMC compliance, then any misleading or untruthful submissions are direct violations of the FCA. This means your organization still has to put in the effort and do the work to become and stay compliant, including asking for, receiving and implementing compensating controls, if necessary.

What does this mean for cybersecurity practitioners? With the punitive nature of FCA violations in consideration, there is going to be a significant desire to “pass the buck” for the associated liability.

- Executive management will want to push liability down to the lowest level possible.
- Cybersecurity practitioners should not submit SPRS scores or any other form of attestation, unless there is absolute evidence of due care and due diligence to support that “point in time” attestation of compliance.
- Cybersecurity practitioners should push attestation to senior executives, similar in concept to SOX compliance and its associated attestations.

Key Points To Remember To Avoid Unforced Errors

Those individuals you choose to represent your company during a CMMC assessment need to be trained on the following points, since they are crucial ingredients to having a successful assessment:

- 1) Assessors are not your friends - be polite but understand the relationship. If you want a friend, get a dog!
- 2) Provide well-written and comprehensive documentation to minimize questions the assessor needs to ask.
- 3) Don't offer up any information on your own!! Only answer the specific question being asked - shut the fuck up and do not open up tangents.
- 4) Tell the truth - you are too pretty for prison.
- 5) If you don't know the answer to a question, simply tell the assessor “*I will consult with the subject matter expert on that control and provide you with that answer once I have it.*” Was that so hard?
- 6) Practice a sheepish smile by staring in the mirror to acclimate yourself to sitting into silence while subtly exuding a sense of competence and mystery.
- 7) Know what your POA&M items are, including current status and associated approvals from the DoD CIO.
- 8) If you would not say it in front of your grandmother or the FBI, then don't say it. Shut the fuck up!
- 9) Do not rant about CMMC, the CMMC-AB or DoD. They know it is a shitshow and don't need you reminding them.



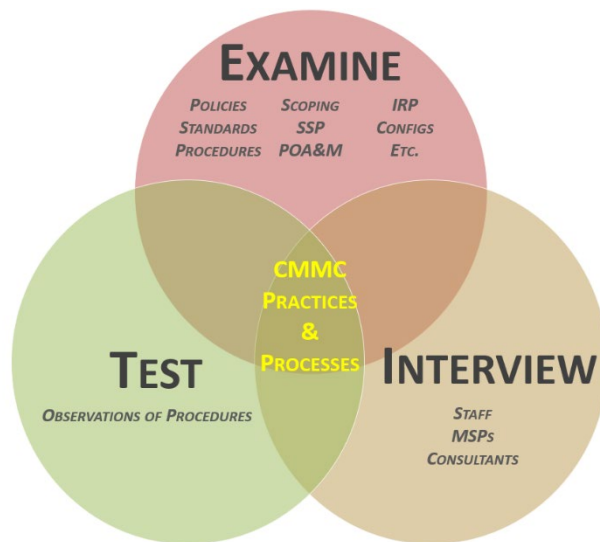


Frontload Your Efforts To Minimize Questions From An Assessor

The best way to avoid unforced errors is to minimize questions that your assessor will ask during the assessment! This is achieved through providing quality documentation that is comprehensive enough to address the questions your assessor needs to answer. From the CMMC Assessment Guide, your assessor has guidelines they must follow to:

- 1) Examine
- 2) Interview and/or
- 3) Test

Your assessor must evaluate certain criteria to ensure your practices and processes are sufficient. If you fail to prepare and frontload “examine” then you will have to answer those questions through testing and interviewing.



Examine

This is your money-maker to avoid unforced errors! If you can frontload the assessment by providing the assessor with answers to their questions, prior to them asking the question then that is a win!

- The better the documentation, the less questions you can expect.
- The inverse is also correct, where if your documentation sucks then expect a shit ton of questions to fill in the gaps.

You should view this as doing the assessment for them - your System Security Plan (SSP) shouldn't ramble on, but should specifically address each assessment criteria and map to specific documentation that you can immediately provide. You're essentially "leading the witness" to a specific conclusion by being upfront and providing an accurate implementation statement and corresponding evidence.

In most cases, your assessors are going to be busy and really don't want to be there in the first place, so if you do their work for them (e.g., structure your evidence and SSP to make it easy for them to fill out what they need to), you will likely get brownie points and hopefully that means your assessor will be more willing to work with you on the tough stuff.

If you don't like your documentation and find it hard to read, your assessor will be in the same boat. As a public service to keep your assessor from day drinking, please be kind by having documentation that is well-written and professional. It benefits both the OSC and the CMMC Third-Party Assessor Organization (C3PAO) by having documentation that doesn't suck.

Interview

This is your mine field! If you are the designated “cat herder” for your CMMC assessment, you should plan to be in the room with the assessor the entire time to help ensure those interviewed do not screw things up for your company. You need to focus your “shut the fuck up training” with those stakeholders who will likely be interviewed:

- Staff internal to your organization who are stakeholders (they affect controls in some manner);
- Managed Service Provider (MSP), if you outsource IT services to a third-party; and
- Consultants who may have helped you implement CMMC controls that you want to help represent your company during the assessment, if applicable.

If your pre-game work is done properly ahead of time, you shouldn't need to bring in additional stakeholders and increase their potential to fuck things up.





Test

Testing can be a mixed bag. It is a blend of “examine” and “interview” where you can expect your assessor to ask you to perform certain CMMC practices/processes while they observe your procedures in action:

- If your documentation is solid, you need to focus on enjoying awkward silences while you perform the procedure. Just repeat the “shut the fuck up” mantra in your head so that you do not open up additional questions by your incessant rambling.
- If your documentation is a steaming pile of crap, you can fully expect a lot of questions during the testing process, since the documentation is insufficient. If you are in this category, focus on succinctly answering the question(s) asked by the assessor and nothing else.

Nothing that is being asked for at this stage should be a surprise. The assessment objectives are publicly accessible information and realistically you’ve already gone through this exercise at least once with the internal audit. If not, consider yourself screwed, but that is a longer conversation.





Objective Evidence: The Documentation You Should Expect To Provide An Assessor

The following table lists reasonable evidence that you should be prepared to present to your assessor. Not only can this help avoid in-person questions during the assessment, it can:

- Demonstrate that your organization is professional and knows what it is doing; and
- Potentially decrease assessment-related costs since time is money and the less time it takes for an assessor to perform the assessment, that should equate to cost savings for your organization.

Item #	Documentation Artifact	Pertinent Corresponding Requirement(s)	Description
1	Network Diagram	No Direct Requirement [general artifact]	The "CUI environment" cannot be scoped without an accurate network diagram.
2	Data Flow Diagram (DFD)	No Direct Requirement [general artifact]	The "CUI environment" cannot be scoped without an accurate Data Flow Diagram (DFD) that identifies where CUI is stored, transmitted and/or processed.
3	Controls Responsibility Matrix (CRM)	No Direct Requirement [general artifact]	There needs to be a clearly documented Controls Responsibility Matrix (CRM) that identifies the stakeholder involved in executing the practices and processes (e.g., controls).
4	"Flow Down" Contracts	No Direct Requirement [general artifact]	There needs to be documentation that shows Third-Party Service Providers (TSP), contractors, vendors, etc. are contractually-obligated to protect CUI where it is stored, transmitted and/or processed, if applicable.
5	Data Classification & Handling	AC.2.005	There needs to be evidence of how CUI (and other types of data) are classified and identified, including acceptable data handling practices.
6	SSP	CA.2.157	There needs to be at least one (1) System Security Plan (SSP) that covers the CUI environment, but the OSC may have multiple SSPs, based on applicable contracts.
7	POA&M	CA.2.159 RM.2.143 SI.1.210	The POA&M need to document the "risk register" of activities from identification through remediation.
8	Asset Inventories	CM.2.061	Systems, applications and services need to be documented.
9	Roles & Responsibilities	AT.2.057	Personnel need to be assigned discrete roles and responsibilities to ensure they are both educated on the role and are responsible for the associated control execution.
10	SPRS Score	DFARS 252.204-7019 DFARS 252.204-7020	Supplier Performance Risk System (SRPS) score.
11	Vulnerability Scan Results	RM.2.142	Vulnerability scans that cover the CUI environment.
12	Change Control & Maintenance Documentation	AC.1.003 CM.2.065 MA.2.111 RM.2.143 RM.3.146 SI.1.210	There needs to be evidence of change control, such as meeting notes from the Change Control Board (CCB).
13	Security Awareness Training	AT.2.056 AT.2.057 AT.3.058	Appropriate, relevant security training for personnel who interact with or protect CUI.
14	Incident Response Plan (IRP)	IR.2.092 IR.3.098 DFARS 252.204-7012	Documented Incident Response Plan (IRP). If applicable, evidence of incidents reported to the DoD.





15	Secure Baseline Configurations (SBC)	CM.2.061	Documented Secure Baseline Configurations (SBC) for all technology platforms within the CUI environment.
16	Access Permission Review	AC.4.025	There needs to be documentation that shows periodic access permission reviews are performed.
17	Risk Assessment	RM.2.141 RM.3.144	There needs to be documentation that shows periodic risk assessments are performed.
18	Threat Intelligence Feeds	SI.2.214	There needs to be documentation that shows the OSC receives threat intelligence feeds.
19	Rules of Behavior	AT.2.057	Users with access to CUI must have documented acknowledgement of acceptable rules of behavior.
20	Non-Disclosure Agreement (NDA)	AC.2.016	Non-Disclosure Agreement (NDA) that restricts unauthorized sharing of CUI.
21	Log Review Process	AU.2.041 AU.3.045 AU.3.051 AU.3.052 SI.2.214	Centralized collection and review/analysis of security event logs.
22	Background Checks	PS.2.127	HR needs to provide evidence of personnel screening practices, which centers around some form of formalized background check process.
23	Visitor Logbook	PE.1.132 PE.1.133	Evidence of visitor management and logging visitor activities.
24	Work From Home (WFH) Security	PE.3.136	Be prepared to describe how safeguarding measures for CUI are enforced at "alternate work sites" which includes working from home.
25	Data Backups & Reconstitution	RE.2.138	Evidence of backups being performed and reconstitution of material from backups.
26	Control Assessments	CA.2.158 CA.3.161	Evidence of "gap assessments" to provide governance of the security controls.





Project Plan To Prepare For A CMMC Assessment

If you are early-on in the process of preparing for a CMMC assessment, then you might want to take a look at the CMMC Kill Chain.

The premise of the CMMC Kill Chain is to build a viable project plan from the perspective of a prioritized listing of tasks in order to successfully prepare for and pass a CMMC assessment. This helps establish your Critical Resource & Acquisition Path (CRAP), since errors or misguided adventures with people, processes and technology earlier in CMMC practice/process implementation activities will have cascading effects, so the CMMC Kill Chain is meant to provide a model for prioritizing CMMC-related pre-assessment activities.

The CMMC Kill Chain breaks down CMMC into 23 major steps, which can then be translated into a project plan.

You can download the CMMC Kill Chain at:

<https://www.cmmc-coa.com/cmmc-kill-chain>

