CMMC Assessment Preparation Guide

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

Version 2024.1

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

Your goal is to pass a CMMC assessment. To reach that goal, 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.

Preventing Unforced Errors

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 Assessment (OSA) / Organization Seeking Certification (OSC) on how to shut the fuck up and not derail the assessment. That may sound harsh, but it is a simple matter of fact. Human nature is your enemy with a CMMC assessment since people being assessed 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.

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) Stare in a mirror to perfect a sheepish smile while acclimating yourself to sitting into silence while subtlety 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 Cyber-AB or DoD. They know it is a shitshow and don't need you reminding them.

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? Any misleading or untruthful submissions about NIST SP 800-171 and/or CMMC to the US Government (or to a prime) are 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.

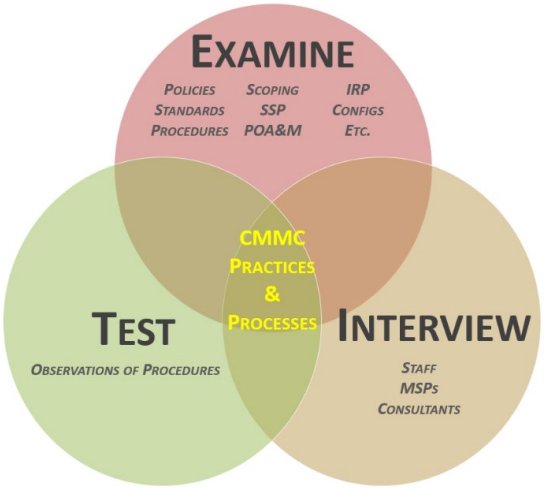
What does this mean for cybersecurity practitioners? With the punitive nature of FCA violations in consideration, there is going to be a significant desire to "pass the buck" for the associated liability.

- 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.

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 addresses 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 OSA/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) Managed Security Service Provider (MSSP), 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.

Do Your Research & Pick A Reasonable C3PAO

It is unfortunate that this has to be said, but there are unqualified and incompetent people/companies in the CMMC ecosystem. This can include anyone waiving one of the following badges, as though that somehow magically makes them competent:

- Registered Provider (RP)
- Registered Provider Organization (RPO)
- CMMC Certified Professional (CCP)
- Certified CMMC Assessor (CCA)
- CMMC 3rd Party Assessment Organization (C3PAO)

Why this is important is that you are potentially inviting an idiot with an irrational view of cybersecurity compliance into your organization to perform an assessment. While that has all the makings of a funny sitcom episode, it is a potential disaster for an OSA/OSC.

To prevent this issue from materializing, you need to do research:

- **Find out who the CCAs will be on the assessment team:**
  - Are those CCAs employees or contractors?
  - How many times has the C3PAO used those CCAs?
- **Go to LinkedIn and read posts/articles that the CCAs authored:**
  - Are they rational or are they spouting idiotic interpretations?
  - Do they appear to have respect from their peers?
  - How much audit/assessment experience do they have? Did they just wake up one morning and decide it would be good to get into cybersecurity assessments?
- **Read the fucking contract with the C3PAO:**
  - In writing, how are disagreements on control/AO interpretations between the CCAs and OSA/OSC handled? This is a big issue, since an illogical CCA can be your worst nightmare in CMMC.
  - Is there a Non-Disclosure Agreement (NDA) that precludes the OSA/OSC from making a public complaint about the C3PAO's processes? Seriously. This could affect your rights to push back on a rogue C3PAO/CCA.
  - Thoroughly go over what is and is not included in the Statement of Work (SOW) (e.g., what would be an additional item, out-of-scope for the quoted assessment cost?).
- **Understand your rights to go "scorched earth" on a wayward C3PAO:**
  - Filing a complaint about a C3PAO / CCA through the Cyber AB is likely a useless endeavor, based on the "black hole" reporting of RPs/RPOs for misconduct with no follow up and no RP/RPO credentials revoked. Given that history, the process for removing bad players in the CMMC ecosystem is apparently not a priority for the Cyber AB and OSA/OSC should not expect any meaningful help from the Cyber AB or DoD.
  - For misguided interpretations of controls / AOs that negatively affect your assessment, you may want to seek an enforcement action (civil penalties) against the C3PAO through the Federal Trade Commission Act (FTC Act) Section 5 that deals with "unfair or deceptive acts or practices in or affecting commerce."[1]
    - In 2022, the FTC considers Business To Business (B2B) customers are "consumers."[2]
    - Per the FTC, an act or practice is "unfair" if it *"causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."* 15 U.S.C. Sec. 45(n).
    - You can learn more about submitting a complaint to the FTC here - https://consumer.ftc.gov/media/video-0054-how-file-complaint-federal-trade-commission
  - While not exactly "scorched earth," you may also want to pursue a complaint through the Better Business Bureau (BBB) against the C3PAO for their business practices.

[1] FTC Act Section 5 - https://www.ftc.gov/about-ftc/mission/enforcement-authority
[2] Bloomberg Law - https://news.bloomberglaw.com/us-law-week/the-ftc-thinks-b2b-customers-are-consumers

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.

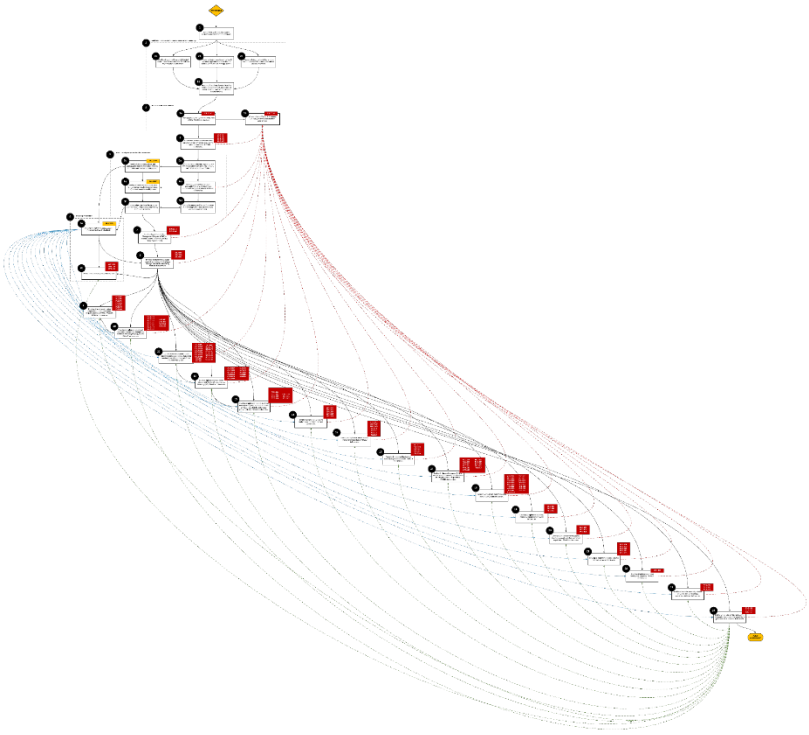
Item #	Documentation Artifact	Pertinent Corresponding Requirement(s)	Description
1	Policies, Standards & Procedures	NIST SP 800-171 Appendix E Non-Federal Organization (NFO) Controls	Policies, standards and procedures are needed to establish a cybersecurity program. NIST documents these requirements as Non-Federal Organization (NFO) controls that are deemed basic enough expectations that they do not have to be further specified as CUI controls. If you do not understand that fundamental requirement for documenting cybersecurity practices, then please do not do business with the Defense Industrial Base (DIB). If you still do not get it, you fail the "reasonable expectations" consideration for negligent behavior for willfully ignoring due diligence expectations.
2	Network Diagram	No Direct Requirement [general artifact]	The "CUI environment" cannot be scoped without an accurate network diagram.
3	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.
4	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).
5	"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.
6	Data Classification & Handling	AC.L2-3.1.9	There needs to be evidence of how CUI (and other types of data) are classified and identified, including acceptable data handling practices.
7	SSP	CA.L2-3.12.4	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.
8	POA&M	CA.L2-3.12.2 RA.L2-3.11.3 SI.L1-3.14.1	The POA&M need to document the "risk register" of activities from identification through remediation.
9	Asset Inventories	CM.L2-3.4.1	Systems, applications and services need to be documented.
10	Roles & Responsibilities	AT.L2-3.2.2	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.
11	SPRS Score	DFARS 252.204-7019 DFARS 252.204-7020	Supplier Performance Risk System (SRPS) score.
12	Vulnerability Scan Results	RA.L2-3.11.2	Vulnerability scans that cover the CUI environment.
13	Change Control & Maintenance Documentation	AC.L1-3.1.20 CM.L2-3.4.3 MA.L2-3.7.1 RA.L2-3.11.3 SI.L1-3.14.1	There needs to be evidence of change control, such as meeting notes from the Change Control Board (CCB).

14	Security Awareness Training	AT.L2-3.2.1 AT.L2-3.2.2 AT.L2-3.2.3	Appropriate, relevant security training for personnel who interact with or protect CUI.
15	Incident Response Plan (IRP)	IR.L2-3.6.1 IR.L2-3.6.2 DFARS 252.204-7012	Documented Incident Response Plan (IRP). If applicable, evidence of incidents reported to the DoD.
16	Secure Baseline Configurations (SBC)	CM.L2-3.4.1	Documented Secure Baseline Configurations (SBC) for all technology platforms within the CUI environment.
17	Access Permission Review	AC.L2-3.1.5	There needs to be documentation that shows periodic access permission reviews are performed.
18	Risk Assessment	RA.L2-3.11.1	There needs to be documentation that shows periodic risk assessments are performed.
19	Threat Intelligence Feeds	SI.L2-3.14.3	There needs to be documentation that shows the OSC receives threat intelligence feeds.
20	Rules of Behavior	AT.L2-3.2.2	Users with access to CUI must have documented acknowledgement of acceptable rules of behavior.
21	Non-Disclosure Agreement (NDA)	AC.L2-3.1.3	Non-Disclosure Agreement (NDA) that restricts unauthorized sharing of CUI.
22	Log Review Process	AU.L2-3.3.2 AU.L2-3.3.3 AU.L2-3.3.5 AU.L2-3.3.6 SI.L2-3.14.3	Centralized collection and review/analysis of security event logs.
23	Background Checks	PS.L2-3.9.1	HR needs to provide evidence of personnel screening practices, which centers around some form of formalized background check process.
24	Visitor Logbook	PE.L1-3.10.3 PE.L1-3.10.4	Evidence of visitor management and logging visitor activities.
25	Work From Home (WFH) Security	PE.L2-3.10.6	Be prepared to describe how safeguarding measures for CUI are enforced at "alternate work sites" which includes working from home.
26	Data Backups & Reconstitution	MP.L2-3.8.9	Evidence of backups being performed and reconstitution of material from backups.
27	Control Assessments	CA.L2-3.12.1 CA.L2-3.12.3	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 24 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