Cybersecurity Services Provider | Authorized C3PAO | Service-Disabled Veteran Owned Small Business

Steps For Preparing For A CMMC Assessment From a C3PAO

Preparing for an official CMMC Assessment can be a time-consuming and frustrating experience if you are taking a Do-It-Yourself approach. However, working with experts who have been through this before can help you speed up the process, reduce the cost, and lower your frustration level from ready to hit your head on the wall, to at least snapping your wrist with a rubber band.

Below are the steps that we advise our clients and Organizations Seeking Certification (OSC) to follow when they are preparing for a CMMC assessment, and the criteria to complete in order to be ready to have an assessment done:

- **Conduct a CUI inventory, lifecycle determination, and document it**
  - You have to first know what you have to protect, where you have it, how much you have, and then log the lifecycle of the CUI you possess, from first receipt to final destruction

- **Determine your assessment scope**
  - Identify all hardware, software, firmware, users, facilities, and documentation that make up your assessment scope, and document/inventory it.

- **Develop your Network topology and FCI / CUI data flow diagrams**
  - Conduct a data flow exercise where you trace how and where CUI flows through your organization, capture it in a flow chart
  - Create a network topology diagram from the assets within your assessment scope

- **Conduct a self-assessment using the DoD Assessment Methodology to calculate your initial or updated SPRS score**
  - Prior to scheduling your actual CMMC assessment, you should be at a full score of 110, but at least be at a score of 88 with no L1 (FAR 17), and no 3 or 5 point deficient controls

- **Create a document traceability matrix that consists of at least two forms of compelling evidence (CE) identified and cited in the System Security Plan (SSP) for each control**
  - This creates a map for you and the assessor
  - Assessors will choose from the three following types of evidence:
    - List of the documents or procedures to examine
    - List of the responsible personnel to interview
    - List of the processes, procedures, or systems to demonstrate

- **Controls matter. Assessment Objectives matter more.**
  - Every Assessment Objective should be covered by at least one of the forms of compelling evidence identified above

- **Identify all in-scope cloud services**
  - Get a NIST 800-171 based Shared Responsibility Matrix (SRM) from every cloud service that is within your assessment scope, referenced from or included in the SSP
  - The SRM must show any consumer-shared responsibilities addressed in the SSP
  - Know what you can and cannot inherit from them

KNC Strategic Services
701 Palomar Airport Rd Suite 300, Carlsbad, CA 92011
(833) 562-7700
www.kncss.com

- **For any Cloud Services Provider identified, determine if they are authorized at a FedRAMP Moderate ATO level or equivalent**
  - If not listed on the FedRamp marketplace, and they are a CSP, then they have to meet the FedRamp equivalency requirements
  - The assessors will be reviewing the Body of Evidence (BOE) from the CSP

- **Develop an Incident Response Plan (IRP), and procedures, and test them at least annually**
  - Run tabletop exercises, test your team, and document the lessons learned

- **Setup and test your DIBNET incident reporting portal access**
  - If an incident happens, and you are on a tight timeframe, you do not want to then learn your login isn't working

- **Gather all of your artifacts in a structured repository, and have them controlled and approved by a Information Security Officer (or designate)**
  - A great tip is to name your documents with the applicable control # that it applies to first, e.g. "3.1.1-Access Control Policy". This helps organize and structure your evidence

- **You must have a senior official sign off on the SSP**
  - This is an easy-to-miss step, especially on a revised version. Make sure that the

- **Review all cybersecurity-related plans (SSP), policies, and artifacts checked for contradictions, e.g. differing password policies in SSP vs Account Management procedures**
  - If you say you do it in your SSP, then make sure you do it, and make sure you don't contradict yourself in your policies, procedures, forms, etc.
  - We are assessing you against your SSP. Scrub it at least 1-2 more times than you think you should.

- **Do not procrastinate!**
  - Do not wait until the month of your actual assessment to try to get everything updated and ready. You will have plenty to do, and time goes fast. The more you have ready and done, the easier it will be for you, the fewer grey hairs you will acquire, and the better you will sleep before and during the assessment.