National Defense-ISAC

C3PAO Shopping Guide for Small & Medium-Sized Businesses

February 2024

Questionnaire & scoring tool tailored for Defense Industry Base small and medium-sized organizations seeking a C3PAO for a CMMC Assessment.

ND-ISAC
National Defense Information Sharing and Analysis Center

EXECUTIVE SUMMARY

It can be challenging for a small or medium-sized business (SMB) to choose an assessor right for their organization.

In a team effort, SMBs across the Defense Industry Base (DIB), along with feedback from CMMC Third-Party Assessment Organizations (C3PAOs), created this document to address the challenges presented to a SMB when vetting an assessor for Cybersecurity Maturity Model Certification (CMMC).

It is important to note that this document is to be used as guidance and considerations as you, the Organization Seeking Assessment (OSA), tackle the goal of **finding an assessor that best fits is your organization.**

Unfortunately, there is incentive to find the 'easiest' assessor. That should not be the goal. A SMB should seek out an assessor that is knowledgeable in CMMC, willing to understand their unique SMB environment, and provide a reasonable assessment to provide risk mitigation assurances to the DIB.

As you use this guide and scoring tool to identify the C3PAO right for your organization's assessment, we urge you to avoid the extremes. Do not to choose from the "bottom of the barrel," which may have their assessment results nullified if they are not holding to the standard and avoid assessors who draw unreasonable lines during intake and vetting conversations.

How To Use This Tool

When conducting assessments like those under the CMMC framework, there are several areas where subjective judgment might come into play, leading to different assessors having varied opinions or interpretations.

Every small business is different, and with contracts and business on the line, preparation is key and choosing the right assessor is necessary. It is important to find an assessor who not only understands the standard but is familiar with its implementation in an environment like yours. This can be helpful in navigating the determination of organization compliance.

This list is not meant to serve as a method of questioning from start to finish – Many of these questions are likely answered during a C3PAO's intake/quote process that the assessor coordinates. It is highly recommended that you follow a C3PAO's intake/quote process prior to asking questions from this resource[i].

These questions are not exhaustive; a SMB may identify additonal questions pertinent to their environment.

An OSA should review the list below and using their environment as context, select questions to facilitate a conversation with a potential assessor to find the right fit for the organization.

ND-ISAC principal authors of this document include: Allison Giddens, Terry Hebert, and Andy Sauer. ND-ISAC also acknowledges the generous consults and contributions of Amira Armond, Kieri Solutions; and Ozzie Saeed, IntelliGRC.

DISCLAIMER

This content is developed by Member Company participants of the National Defense Information Sharing & Analysis Center (ND-ISAC) to assist and inform small and medium-sized businesses (SMBs). This content is provided at no cost and is based on good faith analyses of best practices in consultation with external resources. The authors and contributors assume no responsibility or liability for any errors or omissions in the content of this product. The information contained in this product is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness or timeliness. Any actions or implementations based on this content are entirely at the user's risk and with no implied warranty or guarantee; or liability to the authors and contributors, or to ND-ISAC as a corporate entity, or to ND-ISAC’s Member Companies or their employees. This report may be excerpted or referenced but should not be appended or incorporated in whole within other products without the prior consent of ND-ISAC (please contact: Info@ndisac.org). Nor may the contents be monetized for any purpose. About the ND-ISAC: ND-ISAC is a non-profit, non-federal entity established and funded by its member companies to support their collective cybersecurity and resilience against all hazards through multiple lines of effort (e.g. secure cyber threat sharing, technical solution working groups, knowledge exchange events). To learn more contact Info@ndisac.org.

TABLE OF CONTENTS

INTRODUCTION

Many of these questions throughout the document are likely to be answered during the assessor's intake/quote preparation coordination. Following the intake exercise, feel free to ask the assessor what you feel is not answered and pertinent to your assessment request.

Use this .pdf, along with the supplied .xls, to input your score to help compare assessors and determine what is best for your OSA.

A. INTAKE/QUOTE PROCESS

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being difficult/unclear, 10 being simple, thorough, clear)

Pay careful attention to the intake questions the C3PAO asks, and what types of follow-up questions they ask. This will show you what type of familiarity and flexibility the assessor has to your environment. **Does the C3PAO ask detailed questions about your scope and boundaries before they accept you as a client?** This is a major key to ensuring both the assessor and the OSA are on the same page in advance of significant work for assessment.

Arguably, this is a key piece and possibly the most important step to help determine if this C3PAO is right for your business.

Questions an OSA may choose to ask a potential assessor:

1. What are your individual and organizational credentials with the Cyber-AB?
2. Can you provide proof of your authorization?
3. How many Joint Surveillance Voluntary Audits (JSVA)s and CMMC assessments have you conducted, particularly at our required CMMC level?
    a. What percentage of your certification assessments clients have achieved a conditional or final certification?
    b. What has been the feedback from organizations you have assessed in the past? Can you provide references?
4. Do you screen for potential conflicts of interest in conducting our assessment?
5. How will we securely share information for the assessment?
6. How do you ensure independence and objectivity in your assessment process?
7. Can you show me an example of your assessment planning documents?
    a. Are evidence expectations are discussed in planning?

   b. Does the planning identify-which assets will be assessed against which requirements?

8. How do you handle the discovery of significant cybersecurity issues?
   a. What type of pre-assessment review and acceptance program do you have?
   b. If planning identifies a major issue in our environment, what happens?
   c. If planning identifies a major issue, can we cancel the assessment without a big penalty?

Some assessors will read Systems Security Plan (SSP) descriptions of each implementation during planning to make sure it sounds reasonable and is not misunderstood. This check of readiness helps you secure your investment in an assessment, rather than get halfway through to learn there's a disconnect.

B. COST

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being expensive, 10 being least inexpensive)

Cost is not everything! Small businesses are often resource-constrained and, realistically, one of those constrained resources is cash. However, choosing the assessor that just happens to be the lowest cost may in the long run be more expensive if the small business finds itself having to be re-assessed.

Questions an OSA may choose to ask a potential assessor:

1. What is the estimated cost for the assessment?
2. Can the price change? What conditions will make the price escalate?
3. Is a re-assessment of some practices (if the business almost passed) included in the original price?
4. How many assessors do they plan to assign to the job?

C. AVAILABILITY

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being unavailable/long lead time, 10 being readily available.)

As CMMC nears formal implementation and therefore becomes more and more "real" to businesses, the ecosystem may likely find a bottleneck at the assessment process itself. Consequently, it's important to prioritize your business' needs with an eye toward the availability of an assessor.

It's also wise to recognize that from the time you first interview a C3PAO until the time you are ready to get on their schedule, their availability may differ.

Questions an OSA may choose to ask a potential assessor:

1. What is the expected timeframe for completing the assessment?
2. Do you guarantee any specific schedule or availability?
3. How many Certified CMMC Assessors do you have on-staff?
4. What kind of support do you offer after the completion of the assessment?
5. How do you handle any discrepancies or disagreements that arise post-assessment?
6. Do you provide any tools or guidance for continual improvement post-assessment?
7. How many on-site visits do you project for my assessment?

D. REASONABLENESS

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being unreasonable, 10 being fully reasonable)

Among some observers in the Defense Industrial Base (DIB), there is a perceived "race to the bottom" to find an "easy" assessor. That is not recommended. An assessor's understanding of the standard, consistency of interpretation, and trustworthiness among all stakeholders is key to the success of the Defense Industry Base.

Understanding these areas of potential subjectivity is important for organizations preparing for a CMMC assessment, as it helps them to be thorough in their preparations and mindful of areas where they might need to provide extra clarification or evidence.

Questions an OSA may choose to ask a potential assessor:

1. How involved are you in scoping the assessment?
2. How heavy do you weigh mature procedures? How much historical data do you like to see?
3. When looking for evidence of compliance to a control, what do you believe is sufficient? One example? More than one example? Does it depend on the control?
4. If an OSA uses a cloud application to handle Confidential Unclassified Information (CUI), what type of objective proof are you looking for?
5. Is our Managed Services Provider allowed to lead the OSA's side of the assessment?

6. Do you require the OSA's System Security Plan (SSP) to be numbered/match to NIST SP 800-171 Rev 2 numbering format? What types of information do you require in advance of the assessment? How do you store this data?

E. RESPONSIVENESS

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being completely unresponsive, 10 being quickly responsive)

Customer service is important in any industry, and communication is key. There is nothing more frustrating than interviewing for a service and in response experiencing radio silence for an extended period. During your early communications with the C3PAO, you should get an idea of the level of responsiveness that you can expect from working with the assessor.

Questions an OSA may choose to ask a potential assessor:

1. When can I expect a quote from you?
2. Who would be my point of contact if I have questions immediately before, during, or immediately after the assessment?

F. QUALITY

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being poor quality, 10 being highest quality)

The general quality of the conversation you have with the C3PAO is important. Did you feel heard? Do you feel like you'd be a valued client? Was the assessor distracted or seemed to be multitasking during the call, or were you the priority?

Questions an OSA may choose to ask <u>themselves</u> following the conversation:

1. What general feeling did you get from the intake process?
2. Do you feel as though the assessor would provide a high-quality service?
3. Do you feel as though the assessor is detailed and thorough?

Questions an OSA may choose to ask a potential assessor:

1. Can you provide references from previous clients for whom you've conducted CMMC assessments?

G. TECHNICAL APTITUDE & EXPERIENCE

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being no aptitude and experience, 10 being high aptitude and experience)

A key piece of relevant experience to the assessment relates to technical expertise.

You may find some of these answers through conversations with previous clients during a reference check, or these may be questions that are pertinent to your environment that you should specifically ask the assessor.

Questions an OSA may choose to ask a potential assessor:

1. What is your experience assessing an enclave versus a full business enterprise?
2. How do you assess development labs? (or "are you familiar with")?
3. What is your take on legacy software or specialized software ("Specialized Assets" and Operational Technology) that does not easily lend itself to requirement compliance? Are compensating controls acceptable?
4. Are you familiar with assessing software development infrastructures that are built on agile methods such as *Docker*?
5. What experience do you have with Virtual Desktop Infrastructure (VDI)?
6. What type of Security Protection Assets (SPA)s are you familiar with in an environment like mine?

Additional questions an OSA may choose to ask a potential assessor that relate to the OSA's use of Managed Service Providers (MSP), External Service Providers (ESP), and Cloud Service Providers (CSP):

7. Have you assessed an OSA before with an MSP/ESP?
8. Does it hold any value to you if the ESP/MSP has been assessed via DIBCAC?
9. Have you assessed an ESP/MSP? How many? How many clients did the ESP/MSP support? Did the ESP/MSP use a Remote Monitoring & Management (RMM) tool? Was the assessment successful?
10. Do you require any proof of business "need" before assessing an ESP/MSP? Must an ESP/MSP have direct DFARS 204.252-7012 flow down before you will agree to assess them?
11. If I have an ESP/MSP, must they be assessed before I am? Or can they be assessed with me?

H. BUSINESS/GOV CON APTITUDE & EXPERIENCE

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being no aptitude and experience, 10 being high aptitude and experience)

Another piece of relevant experience to the assessment relates to expertise in the business and government contracting (or subcontracting) environments.

You may find some of these answers through conversations with previous clients during a reference check, or these may be questions that are pertinent to your environment that you should specifically ask the assessor.

Questions an OSA may choose to ask a potential assessor:

1. How many years of experience do you have in the field of government contracting or supporting businesses in service-related support?
2. Can you provide examples of projects or contracts that you have managed in the past, prior to your work with CMMC?
3. How do you stay updated with the constantly changing laws and regulations in government contracting?

I. EXPERIENCE IN CMMC

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being no experience, 10 being a lot of experience)

Another piece of relevant experience to the assessment relates to expertise in CMMC itself.

You may find some of these answers through conversations with previous clients during a reference check, on the C3PAO's website or resume, or these may be questions that are pertinent to your environment that you should ask the assessor specifically.

Questions an OSA may choose to ask a potential assessor:

1. Have you participated in any DIBCAC assessments?
2. Have you participated in any Joint Surveillance Audits (JSAs) or Joint Surveillance Voluntary Audits (JSVA)s? If so, how many?
3. What, if any, industry groups do you actively participate in?

J. EXPERIENCE IN OTHER CYBER FRAMEWORKS

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being no experience, 10 being a lot of experience)

As CMMC is an assessment framework built on NIST SP 800-171 and -171A, it is important to consider other cyber framework experiences that the assessor may have.

Expectations by CMMC-specialized assessors are significantly different from NIST SP 800-53 (assessments of government networks and FedRAMP) and CMMI (assessments of software development teams). Assessors who specialize in other frameworks can be found to be unreasonable compared to CMMC-specialized assessors.

You may find some of these answers through conversations with previous clients during a reference check, on the C3PAO's website or resume, or these may be questions that are pertinent to your environment that you should ask the assessor directly.

Questions an OSA may choose to ask a potential assessor:

1. Do you primarily assess other frameworks?
2. Do you have experience in being responsible for implementation and management of frameworks/controls in the past and/or have past career experience?

K. EXPERIENCE IN ASSESSING SIMILAR ENVIRONMENT TO OSA

Consider the following score and add it to the Spreadsheet Tool.
(1-10, 1 being no experience, 10 being a lot of experience)

Regardless of the standard being assessed, familiarity with the environment being assessed is vital to the effectiveness and success of an assessment.

You may find some of these answers through conversations with previous clients during a reference check, on the C3PAO's website or resume, or these may be questions that are pertinent to your environment that you should ask the assessor specifically.

Questions an OSA may choose to ask a potential assessor:

1. Do you have experience with organizations similar to ours in size, industry, and complexity?

2. How familiar are you with the specific regulatory requirements and standards that apply to our industry? (e.g. AS9100, ISO9001)
3. Have you assessed companies that primarily work in a Bring Your Own Device (BYOD) environment?
4. Have you assessed companies with multiple locations, including work-from-home?
5. What is your experience in a manufacturing environment with an on-premise scope? What about with a hybrid environment?
6. What is your experience in a manufacturing environment that incorporates operational technology (OT) into many of its IT systems?
7. What percentage of physical locations will you require to assess? Do you need to assess different types of physical assets such as an operational site and a data center?

[1] As of the initial publication of this document, CMMC as a Proposed Rule suggests that law and standards may evolve over the coming months. Be mindful that this may render some questions irrelevant and also may introduce new questions to business need.

APPENDIX A – ACRONYM & RESOURCE GUIDE

C3PAO: A CMMC Third Party Assessment Organization (C3PAO) is authorized (and in the future accredited) by the Cyber AB to contract and manage CMMC assessments.

CMMC: Cybersecurity Maturity Model Certification

CSP: Cloud Service(s) Provider; a third-party company offering a cloud-based platform, infrastructure, application, or storage services.

CYBER-AB: The Cyber AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. https://cyberab.org/

DIBCAC: Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

ESP: External Service(s) Provider; a third-party company that provides services to a business. These services may include a variety of functions, including supply, IT, consulting, and financial management.

JSA or JSVA: A Joint Surveillance Voluntary Assessment is under the authority of the DOD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). The audit includes a C3PAO and DIBCAC representation. To date, there is no guarantee that DIBCAC Assessment results will translate to CMMC Certifications.

MSP: Managed Service(s) Provider; a third-party company that offers information technology-related support for companies who lack the in-house resources needed to maintain their systems. An MSP delivers services, such as network, application, infrastructure and security, via ongoing and regular support.

OSA: Organization Seeking Assessment; commonly referred to as an "OSC" (Organization Seeking Certification").

OT: Operational technology; hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment.

RMM: Remote Monitoring & Management; a software platform or application that allows Managed Service Providers (MSPs) to manage their clients' IT systems, even when they're not physically on site.

APPENDIX B – SCORING SPREADSHEET

Use this customizable supplied spreadsheet to determine the weight of each of the 11 categories:

https://ndisac.org/wp-content/uploads/2024/03/CMMC-C3PAO-Scoring-Spreadsheet-V3.2024.xlsx

Score the C3PAOs, and use the optional area at the bottom of the sheet to track assessment costs, other offerings, and general notes.

To learn more about the National Defense ISAC go to: www.ndisac.org
Interested in joining our community? Contact info@ndisac.org