**CMMC Assessment Method**

**Version 1.0**

**June 8, 2020**

Table of Contents

[1.0 Phase I: Plan and Prepare Assessment 5](#_Toc42693315)

[1.1 Analyze Requirements 5](#_Toc42693316)

[1.1.1 Assessment Request Received by C3PAO from OSC 5](#_Toc42693317)

[1.1.2 Identify Lead Assessor 5](#_Toc42693318)

[1.1.3 Identify OSC Sponsor and OSC POC 5](#_Toc42693319)

[1.1.4 High-Level Scoping Discussion 5](#_Toc42693320)

[1.1.5 Determine, Record & Review Assessment Scope and Assessment Objectives 5](#_Toc42693321)

[1.1.6 Negotiate and provide Rough Order of Magnitude (ROM) 5](#_Toc42693322)

[1.1.7 Identify/map OSC Processes and Process Roles 5](#_Toc42693323)

[1.1.8 Verify and Record Objective Evidence (OE) Adequacy and Sufficiency Criteria 5](#_Toc42693324)

[1.1.9 Determine and Confirm Assessment Outputs 5](#_Toc42693325)

[1.2 Development Assessment Plan 5](#_Toc42693326)

[1.2.1 Identify Allowable Tailoring of Assessment Method 5](#_Toc42693327)

[1.2.2 Develop OE Collection Approach 5](#_Toc42693328)

[1.2.3 Select Assessment Team Members, if applicable 5](#_Toc42693329)

[1.2.4 Identify Resources and Schedule 5](#_Toc42693330)

[1.2.5 Identify and Manage Conflicts of Interest 5](#_Toc42693331)

[1.2.6 Identify and Manage Assessment Risks and Their Mitigation & Contingency Plans 5](#_Toc42693332)

[1.2.7 Obtain and Record Commitment to the Assessment Plan 5](#_Toc42693333)

[1.3 Verify Readiness to Conduct Assessment 6](#_Toc42693334)

[1.3.1 Prepare and Train assessment team 6](#_Toc42693335)

[1.3.2 Identify, Obtain, Inventory, and Verify OE 6](#_Toc42693336)

[1.3.3 Perform Certification Assessment Readiness Review (CA-RR) 6](#_Toc42693337)

[1.3.4: Update the Assessment Plan and Schedule as Needed, Based on CA-RR 6](#_Toc42693338)

[Phase 2 – Conduct Assessment 6](#_Toc42693339)

[2.1 Collect and Examine Objective Evidence 6](#_Toc42693340)

[2.1.1 Assessment Kickoff – Opening Briefing 6](#_Toc42693341)

[2.1.2 Collect and Examine Artifacts 6](#_Toc42693342)

[2.1.3 Collect and Examine Affirmations 6](#_Toc42693343)

[2.1.4 Observe Control and Procedural Demos 6](#_Toc42693344)

[2.1.5 Verify OE and Record Gaps 6](#_Toc42693345)

[2.1.6 Update OE Collection Approach 6](#_Toc42693346)

[2.2 Rate Practices and Validate Preliminary Results 6](#_Toc42693347)

[2.2.1 Determine and Record Initial Model Practice Ratings 6](#_Toc42693348)

[2.2.2 Generate Preliminary Findings 6](#_Toc42693349)

[2.2.3 Validate Preliminary Findings 6](#_Toc42693350)

[2.3 Generate Final Assessment Results 6](#_Toc42693351)

[2.3.1 Determine Final Practice Pass/Fail Results 6](#_Toc42693352)

[2.3.2 Determine Maturity Level Recommendation 6](#_Toc42693353)

[2.3.3 Create and Finalize Final Findings 6](#_Toc42693354)

[2.3.4 Record Final Recommended Assessment Results 7](#_Toc42693355)

[Phase 3 – Report Assessment Results 7](#_Toc42693356)

[3.1 Deliver Recommended Assessment Results 7](#_Toc42693357)

[3.1.1 Deliver Final Findings 7](#_Toc42693358)

[3.1.2 Conduct Tailored/Optional Follow-on Activities 7](#_Toc42693359)

[3.2 Package and Archive Assessment Assets 7](#_Toc42693360)

[3.2.1 Submit Assessment Results Package 7](#_Toc42693361)

[3.2.2 Provide Retrospective Feedback to C3PAO and AB 7](#_Toc42693362)

[3.2.3 Archive or Dispose of Any Assessment Artifacts 7](#_Toc42693363)

[Phase 4 Remediation of Outstanding Assessment Issues 7](#_Toc42693364)

[4.1 Identify Remediation Approach 7](#_Toc42693365)

[4.1.1 Verify and Confirm Outstanding Assessment Issues (Weaknesses) 7](#_Toc42693366)

[4.1.2 Identify Remediation Approach and Update Assessment Plan 7](#_Toc42693367)

[4.1.3 Submit Remediation Approach to C3PAO for Verification to Proceed 7](#_Toc42693368)

[4.2 Execute Remediation Approach and Review 7](#_Toc42693369)

[4.2.1 Review All Outstanding Issues Against Updated OE 7](#_Toc42693370)

[4.2.2 Update Previous Practice Pass/Fail Results and Findings 7](#_Toc42693371)

[4.2.3 Verify and Determine Remediated Recommendation of Maturity Level Rating 7](#_Toc42693372)

[4.2.4 Report Remediation Results 7](#_Toc42693373)

[4.2.5 Reconduct Phase 3 Updated Reporting Steps 7](#_Toc42693374)

# 1.0 Phase I: Plan and Prepare Assessment

## 1.1 Analyze Requirements

*These activities are iterative with the other activities in this Phase to get to initial scoping agreement and pricing.*  
Scoping may be initially difficult based on OSC understanding of what this is all about, planning is always more difficult with an inexperienced POC, C3PAO and the LA can’t control how long it takes the OSC POC to complete 1.16, etc.

### 1.1.1 Assessment Request Received by C3PAO from OSC

### 1.1.2 Identify Lead Assessor

### 1.1.3 Identify OSC Sponsor and OSC POC

### 1.1.4 High-Level Scoping Discussion

Targets: Organization Seeking Certification (OSC) entity, scope, contract information, Maturity Level, etc.

Need to have pre-assessment planning decision gates (if you do not pass, have supporting artifacts, SSP, network diagrams, mapping to policies, processes, etc.)

**Organization**: The Legal Entity that will be delivering services or products under the terms of the contract (one or many). **They could receive a CMMC Maturity Level**, but also can designate a Host Unit.

**Host Unit**: The people, processes, and technology that will be applied to the contract (one or many teams that are doing the work). This is the UNIT that is requesting a **CMMC Maturity Level**

**Supporting Units:** The people, processes, and technology that support the Host unit. They will need to be part of the assessment, but will **NOT receive a CMMC Maturity Level** unless an enterprise assessment is conducted.

**Enclave**: A Unit-within-a-Unit that requires a higher maturity Level. The Host Unit must achieve a ML before the Enclave can be assessed by a Certified Assessor and receive a CMMC Maturity Level

### 1.1.5 Determine, Record & Review Assessment Scope and Assessment Objectives

Responsibility of OSC, in coordination with the Lead Assessor, who has final say on what is in scope. NW diagrams, SSP, contract scope, if OSC is not willing to rescope, becomes an immediate fail.

Add remediation criteria and planning

#### 1.1.5.1. Evaluating Model Reciprocity

Reciprocity for alternative models is permitted within the **CMMC Assessment Methodology (CAM**). The Certified or Provisional Assessor has sole authority to accept results from the examination of controls or practices from an organization’s prior assessments/audits/appraisals (“examinations”) based on alternative models such as Fedramp, NIST 800-181, CMMI V2.0, ISO 27001, or others.

The following assumptions must be validated by the Certified Assessor prior to acceptance of reciprocity:

1. The Examination being presented for reciprocity consideration was conducted by aa credentialed assessor/auditor/appraiser (“examiner”) on behalf of a regulatory body authorized to award accreditations for that model.
2. Each control or practice to be considered for reciprocity must be functionally equivalent to the CMMC practice or control it is replacing. It is the responsibility of the OSC to present evidence of functional equivalency of that practice or control, and evidence of equivalency is accepted at the sole discretion of the Certified Assessor.
3. All alternative controls/practices/requirements presented for reciprocity have received a passing score, characterization, or finding.
4. There is no POAM, list of non-conformances, or rating deficiencies reported as a result of the examination.
5. The Examination was conducted within 180 days prior to Phase II (onsite) of the CMMC Assessment.

The following rules of evidence apply to all CMMC practices/controls where reciprocity may apply:

1. CAM identifies three evidence types, with at least two being required for each control or practice to be rated as “pass.” For controls or practices that are eligible for reciprocity, only one type of evidence will be required, eliminating as much as 70% of the time and effort required to examine the control or practice
2. Controls or practices eligible for reciprocity must also be examined in the context of the CMMC ML2 “Institutionalization” processes, and the Certified Assessor must account for this when interpreting the evidence for the eligible controls or practices.
3. Controls/Practices validated successfully through the use of the reciprocity rules of evidence are to be considered implemented and will not be identified in the assessment report as having met a reduced standard of evidence.

### 1.1.6 Negotiate and provide Rough Order of Magnitude (ROM)

For schedule, assessment pricing, dates, etc. and initiate contract for assessment

Questions:

Assume the C3PAO will work in conjunction with the Lead Assessor to determine and finalize scoping and pricing. Will C3PAO provide pricing guidelines/limits? Travel and Expense policies and guidelines? Probably need a standard SOW/BOE, Scoping Template

### 1.1.7 Identify/map OSC Processes and Process Roles

OSC does this under guidance and in coordination with the LA

### 1.1.8 Verify and Record Objective Evidence (OE) Adequacy and Sufficiency Criteria

Assumes that the Assessment method will identify minimum adequacy and sufficiency criteria - this will simply verify that and add any additional as needed

### 1.1.9 Determine and Confirm Assessment Outputs

## 1.2 Development Assessment Plan

*Plan must be kept up to date throughout all assessment phases, including anytime the plan changes significantly -* Spell out criteria for “significantly”

### 1.2.1 Identify Allowable Tailoring of Assessment Method

### 1.2.2 Develop OE Collection Approach

Identify methods, techniques, and responsibilities, etc. for collecting and managing OE

### 1.2.3 Select Assessment Team Members, if applicable

### 1.2.4 Identify Resources and Schedule

### 1.2.5 Identify and Manage Conflicts of Interest

### 1.2.6 Identify and Manage Assessment Risks and Their Mitigation & Contingency Plans

### 1.2.7 Obtain and Record Commitment to the Assessment Plan

C3PAO must confirm adequate and appropriate scope before starting.

YES, to some level (Define in description)

## 1.3 Verify Readiness to Conduct Assessment

### 1.3.1 Prepare and Train assessment team

### 1.3.2 Identify, Obtain, Inventory, and Verify OE

### 1.3.3 Perform Certification Assessment Readiness Review (CA-RR)

Defined as verifying planning and execution preparedness to be able to successfully execute the assessment as planned

Verify that all the requirements and condition covered by the assessment plan are met, and conditions - we need to clarify what criteria meets this requirement (mix of self-assessment or 3rd party)

### 1.3.4: Update the Assessment Plan and Schedule as Needed, Based on CA-RR

# Phase 2 – Conduct Assessment

## 2.1 Collect and Examine Objective Evidence

These activities will be iterative.

### 2.1.1 Assessment Kickoff – Opening Briefing

### 2.1.2 Collect and Examine Artifacts

Assumption: Lead Assessor has verified that the organization is prepared for the assessment through a pre-assessment and/or readiness review.

### 2.1.3 Collect and Examine Affirmations

Lead assessor schedules, works with POC to identify (in Phase 1) who to interview

### 2.1.4 Observe Control and Procedural Demos

Demonstration that controls are working.

### 2.1.5 Verify OE and Record Gaps

### 2.1.6 Update OE Collection Approach

## 2.2 Rate Practices and Validate Preliminary Results

These activities will be iterative

### 2.2.1 Determine and Record Initial Model Practice Ratings

Pass/Fail Results

Practice conditions, outcomes, etc.

### 2.2.2 Generate Preliminary Findings

### 2.2.3 Validate Preliminary Findings

Minimum of one event to all participants prior to final findings, but left at discretion of Lead Assessor to do daily validation sessions, check-in on data, etc.

## 2.3 Generate Final Assessment Results

### 2.3.1 Determine Final Practice Pass/Fail Results

### 2.3.2 Determine Maturity Level Recommendation

Submitted to C3PAO, final approval by AB after QA audit

### 2.3.3 Create and Finalize Final Findings

Built on validate preliminary findings, and model practice pass/fail results and ML recommendation

### 2.3.4 Record Final Recommended Assessment Results

# Phase 3 – Report Assessment Results

## 3.1 Deliver Recommended Assessment Results

### 3.1.1 Deliver Final Findings

### 3.1.2 Conduct Tailored/Optional Follow-on Activities

e.g. Executive Debriefing

## 3.2 Package and Archive Assessment Assets

### 3.2.1 Submit Assessment Results Package

### 3.2.2 Provide Retrospective Feedback to C3PAO and AB

Surveys? Goes to AB, C3PAO and LA

### 3.2.3 Archive or Dispose of Any Assessment Artifacts

# Phase 4 Remediation of Outstanding Assessment Issues

## 4.1 Identify Remediation Approach

### 4.1.1 Verify and Confirm Outstanding Assessment Issues (Weaknesses)

### 4.1.2 Identify Remediation Approach and Update Assessment Plan

Addendum to discuss the deltas only

90 (calendar) days time limit – Recommended by assessment team?

Ron will add strawman criteria for when remediation is feasible or not (e.g. 80% threshold, etc.)

Same LA, Same assessment team, and same C3PAO - Need to make this a clear rule – this is a rule that the AB and C3PAO lays out

### 4.1.3 Submit Remediation Approach to C3PAO for Verification to Proceed

C3PAO reviews and forwards to AB which also has to approve

## 4.2 Execute Remediation Approach and Review

### 4.2.1 Review All Outstanding Issues Against Updated OE

### 4.2.2 Update Previous Practice Pass/Fail Results and Findings

Repeat Activities 2.2.1-2.3.4 where needed, follow threads to other practices as needed

Lead Assessor must preserve previous pass/fail results for historical baselining

### 4.2.3 Verify and Determine Remediated Recommendation of Maturity Level Rating

### 4.2.4 Report Remediation Results

Updated FF to OSC, and then start "delta" package, but need to maintain the original assessment results and the remediation results)

### 4.2.5 Reconduct Phase 3 Updated Reporting Steps

Starting with 3.1.1

Lead Assessor maintains historical baseline of initial results and updated remediation results