

**CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)**

**Assessment Plan**

**Target ML <X>**

**For**

*<Company>*

*<Host Unit>*

*<Program Enclave>*

*Version 1.0*

***<date>***

|  |  |
| --- | --- |
| *C3PAO* | *Name* |
| *OSC Requestor* | *Name* |
| *Lead Assessor* | *Name* |

**CMMC Assessment Plan**

**Document Updates**

Changes to any of the information contained in this document should be tracked via appropriate entries in the revision history table below.

**Assessment Plan Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Summary of Changes** | **Authors** | **Reviewers** |
| 02-20-20 | V1.0 | Development of Initial Plan |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of Contents**

[1.1 Analyze Requirements 4](#_Toc42780555)

[1.1.1 Assessment Request Received by C3PAO from OSC <Date> 4](#_Toc42780556)

[1.1.2 Identify Lead Assessor 4](#_Toc42780557)

[1.1.3 Identify OSC Sponsor and OSC POC 4](#_Toc42780558)

[1.1.4 High Level Scoping 5](#_Toc42780559)

[1.1.5 Determine, Record & Review Assessment Scope and Assessment Objectives 5](#_Toc42780560)

[1.1.6 Negotiate and provide Rough Order of Magnitude (ROM) 6](#_Toc42780561)

[1.1.7 Identify/Map OSC Processes and Process Roles 6](#_Toc42780562)

[1.1.8 Verify and Record Objective Evidence (OE) Adequacy and Sufficiency Criteria 6](#_Toc42780563)

[1.1.9 Determine and Confirm Assessment Outputs 7](#_Toc42780564)

[1.2 Develop Assessment Plan 7](#_Toc42780565)

[1.2.1 Allowable Tailoring 7](#_Toc42780566)

[1.2.2 OE Collection Approach 7](#_Toc42780567)

[1.2.3 Assessment Team Members 8](#_Toc42780568)

[1.2.4 Identify Resources & Schedule 8](#_Toc42780569)

[1.2.5 Identify and Manage Conflicts of Interest 9](#_Toc42780570)

[1.2.6 Identify and Manage Assessment Risks and Their Mitigation & Contingency Plans 9](#_Toc42780571)

[1.3 Verify Readiness to Conduct Assessment 9](#_Toc42780572)

[1.3.1 Prepare/Train Assessment Team 9](#_Toc42780573)

[1.3.2 Identify, obtain, inventory, and verify OE 10](#_Toc42780574)

[1.3.3 Perform Certification Assessment Readiness Review (CA-RR) 10](#_Toc42780575)

**Phase 1 - Plan and Prepare for Assessment**

The purpose of this CMMC Assessment Plan is to document the results of planning including the requirements, agreements, estimates, risks, and practical considerations (e.g., schedules, logistics, and contextual information about the organization) associated with the Assessment. It is a required artifact that must be reviewed and approved by the Lead Assessor, OSC Assessment Sponsor and Assessment Team Members.

## Analyze Requirements

### Assessment Request Received by C3PAO from OSC <Date>

#### <Attach as an addendum, a copy of the request or engagement letter>

|  |  |
| --- | --- |
| **Item** | **Description** |
| C3PAO Legal Name |  |
| C3PAO main address including City and ZIP/Postal Code |  |

### Identify Lead Assessor

|  |  |
| --- | --- |
| **Item** | **Description** |
| Lead Assessor Name |  |
| Lead Assessor Company |  |
| LA company main address including City and ZIP/Postal Code |  |

### Identify OSC Sponsor and OSC POC

|  |  |
| --- | --- |
| **Item** | **Description** |
| OSC Assessment Sponsor |  |
| Title |  |
| Relationship to the Organization being assessed |  |
| Main address including City and ZIP/Postal Code |  |
| Email address |  |
| Contact phone number |  |

### High Level Scoping

|  |  |
| --- | --- |
| **Item** | **Description** |
| OSC legal name |  |
| Main address including City and ZIP/Postal Code |  |
| Assessment usage | *[Contractual Certification Requirement, etc..]* |
| Assessment purpose and background | *[Provide a description why the Assessment is being performed, and a brief history of events leading up to this Assessment.]* |
| Identify the minimal set of artifacts to be provided for the assessment |  |
| Target Maturity Level | *Target Maturity Level* |
| OSC Description | ***[****Enter a description in sufficient detail to explain the overall function of the OSC Entity being appraised. This may include, but is not limited to:*   * *Overview of the work performed* * *Description of the customers* * *Organization charts* * *Description of other types of Security certifications/assessments the OSC has earned etc. NIST 800-171 self, ISO 27000]* |

### [Determine, Record & Review Assessment Scope and Assessment Objectives](bookmark://_Toc42693321)

*In this section determine the scope of the assessment. The OSC, in coordination with the Lead Assessor should determine the final scope.  Identify NW diagrams, SSP, contract scope/requirements*

*Note: if OSC is not willing to rescope, becomes an immediate fail.*

#### [Evaluating](bookmark://_Toc42693321) Model Reciprocity

*In this section identify any alternative models that are 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.*

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

*In this section identify assessment pricing, dates, etc. and initiate contract for assessment*

*The follow Questions should be considered:*

*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*

### Identify/Map OSC Processes and Process Roles

*[In this section, record the data collection approach, strategy, and plan for the Assessment. This section will evolve throughout the Assessment planning period and will be reviewed and updated during the Conduct Assessment Phase.]*

| OE Collection Task | Detail |
| --- | --- |
| OE collection approach | *[Identify whether the Assessment will be conducted in discovery and describe the strategy behind the mode selected.]* |
| Techniques for collecting OE | *[Identify methods and techniques for collection OE. Examples include:*   * *Artifacts* * *Interviews: describe how interviews will be conducted* * *Demonstrations or presentations: describe the approach to demonstrations or presentations for the collection of affirmations* |
| Use of virtual methods for OE collection | *[Describe the use of virtual OE collection techniques, including video conferences, teleconferences, and other similar technologies.]* |
| Data Collection Timing | *[Identify an overall timeline to set expectations for when OE collection activities need to be completed by the OSC in preparation for the readiness reviews and the Conduct Assessment Phase.] \* Pre Assessment is an analysis of planning, risk and data.* |

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

*Typically in assessments a matrix or map is identified that depicts the Process Area and evidence that will be collected.*

### Determine and Confirm Assessment Outputs

| Selected | Required Outputs | Description and Notes |
| --- | --- | --- |
|  | Assessment plan | Provided to Sponsor & C3PAO |
|  | Final findings including Characterizations of Practices with Weaknesses | Provided to Sponsor & C3PAO |
|  | Maturity Level | To Sponsor and C3PAO |
|  | Assessment Record with validity period | Provided to Sponsor & C3PAO |
|  | **Optional** |  |
|  | Recommendations Report | Provided to OSC Sponsor |
|  | Executive Briefing | Provided to OSC Sr. Management |

## Develop Assessment Plan

*The CMMC Assessment Plan must be kept up-to-date throughout all assessment phases. Therefore, a revision history must be kept up to date.*

### Allowable Tailoring

<This would be based on requirements from the RDD>

| **RDD Process** | **Tailoring Decision** | **Tailoring Rationale (Which option was chosen, and why.)** |
| --- | --- | --- |
| 1.1.1 Assessment Request Received by C3PAO from OSC |  | . |
| 1.1.2 Identify Lead Assessor |  |  |

### OE Collection Approach

*Prior to Phase 2, the OSC must catalog all OE and map the evidence to the CMMC practices in the target maturity level.*

### Assessment Team Members

| **Name** | **Organization** | **Describe Cyber Security or other Security Certifications** | **Clearances** | Con**tact Information**  **Email and Phone** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Identify Resources & Schedule

#### Schedule

*[Below is a example CMMC Assessment Schedule Template]*

| **Day** | **Date** | **Start** | **End** | **Remote** | **PAs** | **Participants** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  | Open Briefing |  | Appraisal Team Members (ATM), Senior Management (Sponsor) & any participants |
|  |  | Appraisal Team Training & begin OE artifact reviews |  | ATM |
|  |  | Demos |  |  |
|  |  | Interview 1 |  | ATM |
|  |  | Characterizations |  |  |
| 2 |  |  |  | Continue OE Artifact Reviews |  | ATM |
|  |  | Continue with other Assessment events |  |  |

### Identify and Manage Conflicts of Interest

*This section identifies known conflicts identified during early Assessment planning when requirements for the Assessment are identified. Assessment conflicts may be used as inputs to risk management.*

| **ID** | **Type of Conflict** | **Conflict Description** | **Impact to Assessment** | **Mitigation** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

*This section identifies risks to the success of conducting the Assessment as planned. Assessment plans should include the documentation of multiple risks.*

| **ID** | **Risk Name** | **Risk Category** | **Risk Description** | **Risk Impact** | **Likelihood** | **Risk Mitigation** | **Risk Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Verify Readiness to Conduct Assessment

*Verifies the readiness of the OSC, the assessment team, OE, logistics, risks, etc.*

### Prepare/Train Assessment Team

*In this section describe the type oi training that will be delivered that describes the assessment process, set assessment team expectations and commitments.*

### Identify, obtain, inventory, and verify OE

*In this section describe the format for identifying the collection and maintenance of OE.*

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

|  |  |
| --- | --- |
| **Item** | **Description** |
| Pre-Assessment review begin/end dates |  |
| Objectives | *[Describe the purpose of the Pre-Assessment review. Examples include, but are not limited to:*   * Logistics readiness * OE (e.g., accessibility, coverage of practices, etc.) |
| Rating criteria |  |
| Members to be present during Pre-Assessment review |  |
| Pre-Assessment review outcomes | *[Outcomes include, but are not limited to:*   * *Remaining OE needs* * *Logistical, facility, access concerns* * *Updated risk considerations* * *Go/No Go decision* * *Other outcomes as defined]* |

1.3.4 Update the Obtain Assessment Plan and Schedule as Needed, Based on. CA-RR

**Assessment Team Lead (required)**

As the designated Assessment Team Lead for this CMMC Assessment, I affirm that to the best of my knowledge the information in this document, the Assessment plan, is accurate, does reflect my current agreement with the Assessment Sponsor.

Assessment Team Lead name:

Assessment Team Lead signature:

Date signed:

**Assessment Sponsor (required)**

As the Assessment Sponsor for this Assessment, I affirm that I have reviewed and do approve this Assessment plan document.

Assessment Sponsor name:

Assessment Sponsor signature:

Date signed:

**Assessment Team Members (If Appropriate)**

By our signatures below we affirm that we have reviewed the Assessment plan; to the best of our knowledge the information in this Assessment plan is accurate, and we commit to performing the Assessment activities as assigned in this plan.

|  |  |  |
| --- | --- | --- |
| **Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |