

**CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)**

**Assessment Plan**

**Target Maturity Level <X>**

**for**

*<Company>*

*<Host Unit>*

*<Program Enclave>*

*Version 1.0*

*<Date>*

Prepared by:

|  |  |
| --- | --- |
| *C3PAO* | *<Name>* |
| *OSC Sponsor* | *<Name* |
| *Certified Assessor* | *<Name>* |

**CMMC Assessment Plan**

**Document Updates**

Changes to any of the information contained in this document are tracked by 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 Assessment Planning 4](#_Toc44019243)

[1.1 Analyze Requirements 4](#_Toc44019244)

[1.1.1 Certified Third-Party Assessor Organization (C3PAO) 4](#_Toc44019245)

[1.1.2 Assigned Certified Assessor 4](#_Toc44019246)

[1.1.3 OSC Sponsor and OSC Primary Point of Contact (POC) 4](#_Toc44019247)

[1.1.4 Assessment High-level Scope 5](#_Toc44019248)

[1.1.5 Detailed Assessment Scope 6](#_Toc44019249)

[1.1.6 Estimated Assessment Rough Order of Magnitude (ROM) 6](#_Toc44019250)

[1.1.7 Objective Evidence OSC Processes and Process Roles 7](#_Toc44019251)

[1.1.8 Objective Evidence Adequacy and Sufficiency Criteria 8](#_Toc44019252)

[1.1.9 Assessment Outputs 8](#_Toc44019253)

[1.2 Develop Assessment Plan 8](#_Toc44019254)

[1.2.1 Tailoring of CMMC Assessment Method 8](#_Toc44019255)

[1.2.2 OE Collection Approach 9](#_Toc44019256)

[1.2.3 Assessment Team Members 9](#_Toc44019257)

[1.2.4 Assessment Resources and Schedule 10](#_Toc44019258)

[1.2.5 Assessment Conflicts of Interest 10](#_Toc44019259)

[1.2.6 Assessment Risk and Risk Management 11](#_Toc44019260)

[1.3 Readiness to Conduct Assessment 11](#_Toc44019261)

[1.3.1 Assessment Team Preparation and Training 11](#_Toc44019262)

[1.3.2 Identify, obtain, inventory, and verify OE 12](#_Toc44019263)

[1.3.3 Certification Assessment Readiness Review (CA-RR) 12](#_Toc44019264)

[1.3.4 Results of Certification Assessment-Readiness Review 12](#_Toc44019265)

[2 Assessment Plan Approval 14](#_Toc44019266)

[3 Appendices 15](#_Toc44019267)

[Appendix A – OSC Request for Assessment 15](#_Toc44019268)

[Appendix B – CMMC Assessment Schedule 16](#_Toc44019269)

[Appendix C - <Enter Title> 17](#_Toc44019270)

# Assessment Planning

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 Certified Assessor (CA), Organization Seeking Assessment (OSC) Sponsor and Assessment Team Members (ATMs).

## Analyze Requirements

The following sections document analysis results of all appraisal requirements for input to appraisal planning. The analysis is performed by the CA with input and concurrence required from the OSC Sponsor and representative from the Certified Third-Party Assessor Organization (C3PAO).

### Certified Third-Party Assessor Organization (C3PAO)

A Request for Assessment (RFA) was received by the following C3PAO from *<OSC name>* on *<date>*. A copy of the request is attached in Appendix A. *<Attach as an addendum, a copy of the request or engagement letter>*

|  |  |
| --- | --- |
| **C3PAO** | **Description** |
| Name | *<C3PAO Legal Name>* |
| Address | *<C3PAO main address, including city and ZIP / Postal Code>* |

### Assigned Certified Assessor

The following Certified Assessor has been assigned by the C3PAO to perform this assessment.

|  |  |
| --- | --- |
| **Certified Assessor** | **Description** |
| Name | *<Name of assigned CA>* |
| Company | *<Name of Company employing or affiliated with CA>* |
| Company Address | *<Main address, including city and ZIP / Postal Code of Company employing or affiliated with CA>* |

### OSC Sponsor and OSC Primary Point of Contact (POC)

The OSC has identified the following individuals to serve as Assessment Sponsor and POC.

| **OSC** | **Description** |
| --- | --- |
| Assessment Sponsor | *<Name and title of OSC Assessment Sponsor>* |
| Relationship to the OSC being assessed | *<Describe the OSC Assessment Sponsor’s relationship to the Entity or other part of the organization being assessed>* |
| Assessment Sponsor Email Address | *<Contact Email of OSC Assessment Sponsor>* |
| Assessment Sponsor Phone number | *<Contact phone number of OSC Assessment Sponsor>* |
| Primary Point of Contact (POC) | *<If the OSC Assessment Sponsor is not the primary contact for planning the assessment, enter the name of the primary POC>* |
| POC Email Address | *<Contact Email of OSC POC>* |
| POC Phone number | *<Contact phone number of OSC POC>* |

### Assessment High-level Scope

The following describes the high-level scope of the assessment as concurred to by the CA and OSC Sponsor.

| **High Level Assessment Scope** | **Description** |
| --- | --- |
| OSC Organization | *<OSC Legal Entity Name>* |
| OSC Address | *<Main address, including city and ZIP / Postal Code of OSC>* |
| OSC Host Unit | *[Enter a description in sufficient detail that explains the overall makeup and function (people, processes and technology)of the OSC Host Unit being assessed. This may include, but is not limited to:*   * *Organization Host Unit name / description* * *Location(s)* * *Overview of the work performed* * *Description of the customers* * *Organization charts* * *Other boundaries* |
| OSC Supporting Unit(s) | *<Describe the people, processes, and technology that support the host unit assessment>* |
| OSC Enclave(s) | *<Describe any enclaves included in the assessment>* |
| Target CMMC Scope / Maturity Level | *[Enter Target Maturity Level]* |
| 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.]* |
| Assessment Objectives | *[List the OSC objectives for the assessment]* |
| Other Security Assessments completed | *[Description of other types of Security certifications/assessments the OSC has earned etc. NIST 800-171 self-assessment, ISO 27000, etc.]* |
| Initial Objective Evidence Required | *[List the minimal set of artifacts to be provided to the CA for detailed scope definition in advance of the onsite (Phase II), including:*   * *System Security Plan(s) (SSP)* * *Network diagrams* * *Customer contract scope / requirements* * *Organizational charts* * *Policies, process guidance, outputs, etc* * *List of personnel roles to be included in interviews]* |

### Detailed [Assessment Scope](bookmark://_Toc42693321)

The OSC Sponsor, working in coordination with the C3PAO and Certified Assessor, has determined and agreed to the final assessment scope described throughout this plan.

#### Model Reciprocity

The following alternative model assessment results, including controls and practices, have been evaluated for conformance with CMMC controls and practices and validated / accepted by the Certified Assessor on *<enter date(s) of examination by CA>* as having reciprocity for this CMMC assessment.

*[Include a copy of this table for each alternative model identified and evaluated / validated for reciprocity in this assessment. In evaluating reciprocity, the CA must validate the assumptions and rules of evidence in examining controls and practices as specified in the CMMC Assessment Method (CM2CAM) and maintain results of that evaluation / validation.*

|  |  |
| --- | --- |
| **Reciprocity Model** | **Description** |
| Model Assessment / Audit | *[Provide the name and of the alternative model results evaluated, ex. Fedramp, NIST 800-181, CMMI V2.0, ISO 27001, etc.]* |
| Date of Assessment / Audit | *[Provide the formal recorded date of the assessment / audit results]* |
| Credentialed Assessor / Auditor / Appraiser | *[Provide the Name and validated licensing information for the credentialed individual who led the assessment / audit]* |
| CA Reciprocity Examination Results | *[Provide a description of the controls / practices validated by the CA for reciprocity, attach validation results as addendum to this plan or provide a link to the validated results.]* |

### Estimated Assessment Rough Order of Magnitude (ROM)

*<In formulating the ROM estimate, consider if the C3PAO will provide guidelines / limits for assessment pricing, travel and other expense policies and guidelines, etc.>*

The ROM estimate for this assessment was determined by the CA working with the C3PAO and OSC Sponsor / POC, and serves as the basis for initiating the formal assessment contract and further detailed planning.

Details of the ROM estimate are located in the CMMC Assessment ROM Estimate document located at *<provide the location or link to the completed CMMC Assessment ROM Template for this assessment.>*

|  |  |
| --- | --- |
| **Assessment ROM Estimate** | **Description** |
| *Phase 1: Plan and Prepare* | *<Enter dates / duration for Assessment Phase 1>* |
| *Phase 2: Conduct Assessment* | *<Enter dates / duration for Assessment Phase 2>* |
| *Phase 3: Report Results* | *<Enter dates / duration for Assessment Phase 3>* |
| *Pricing* | *<Enter Pricing estimate including labor, travel, expenses and other direct costs.* |

### Objective Evidence OSC Processes and Process Roles

The following sources of Objective Evidence (OE) will be provided by the OSC as required by the target Maturity Level of this assessment.

| Assessment OE | Description |
| --- | --- |
| Artifacts | *[List all of the OSC policies, processes and related plans in scope for the assessment or provide the location / link to a listing of this information. These artifacts will be reviewed provide during the assessment conduct phase.]* |
| Affirmations | *[List all of the OSC personnel and their associated process role in scope for the assessment or provide the location / link to this listing. These individuals will provide affirmation OE during the assessment conduct phase]. [Describe how interviews will be conducted.]* |
| Demonstrations / Tests | *[List all of the demonstrations / tests that will be observed during the assessment or provide the location / link to a listing of this information. Demonstrations / tests may provide both artifacts and affirmations for the assessment.] [Describe how demonstrations will be conducted.]* |
| Virtual data collection techniques | *[Describe how virtual OE collection techniques, including video conferences, teleconferences, and other similar technologies will be used during the assessment.]* |
| 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.* |
| Management of Controlled Unclassified Information (CUI) | *[Describe how CUI will be managed and protected throughout the assessment phases.]* |

### Objective Evidence Adequacy and Sufficiency Criteria

*[A matrix or mapping is typically created that depicts the CMMC practices and controls and the evidence that will be collected to demonstrate conformance.]*

The CA will ensure that Assessment Team follows all established CMMC Practice and Domain rating rules and meet all requirements and criteria for determining the adequacy and sufficiency of OE.

### Assessment Outputs

The following assessment outputs will be produced and archived as part of performing this assessment. Are all required??

| Selected | Required Outputs | Description and Notes |
| --- | --- | --- |
|  | Initial ROM Estimate of Assessment Scope | Established within this plan |
|  | CMMC Assessment Plan and Schedule | Provided to Sponsor & C3PAO |
|  | Certification Assessment-Readiness Review (CA-RR) results | Sampled practice percentage and results (75% success) |
|  | Assessment Draft Findings | Intermediate output |
|  | Assessment Final Findings including Recommended Maturity Level rating | Provided to Sponsor & C3PAO |
|  | Recommended in-scope domains and CMMC practice ratings | Provided to Sponsor & C3PAO |
|  | Potential Remedial Actions (if applicable) | Provided to Sponsor & C3PAO |
| Selected | **Optional Outputs** | **Description and Notes** |
|  | Assessment Recommendations Report | Provided to OSC Sponsor |
|  | Assessment Executive Briefing | Provided to OSC Sponsor and invited Sr. Management |

## Develop Assessment Plan

This CMMC Assessment Plan is updated whenever a significant change occurs and is kept current throughout all assessment phases. A description of changes made is recorded in the revision history. At the conclusion of the appraisal the Appraisal Plan will reflect all actual results, timing, events and scope covered by the assessment.

### Tailoring of CMMC Assessment Method

Identify practices and/or controls that the OSC and Assessor believe should be deemd “out of scope.”

| **Process or Practice** | **Tailoring Decision** | **Tailoring Rationale (Which option was chosen, and why.)** |
| --- | --- | --- |
|  |  | . |
|  |  |  |

### Objective Evidence 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.*

*<Identify the methods, techniques and responsibilities for collecting and managing the Objective Evidence on this assessment. This may include data collection approach, strategy, and plan including artifact gathering and availability, interview conduct, requests for information (email or surveys) and Assessment Readiness Review (CA-RR) results.*

*This section will evolve throughout the Assessment planning period and will be reviewed and updated as needed during the Conduct Assessment Phase.]*

### Assessment Team Members

The following individuals will participate on this assessment as Assessment Team Members (ATMs). The C3PAO has performed the required due diligence to verify that each ATM meets all CMMC Assessment Method requirements for experience, skills, qualifications and training.

| **Name** | **Organization** | **Registered Practitioner or Certified Professional? (Y/N)** | **Security Clearances (if required)** | Con**tact Information** |
| --- | --- | --- | --- | --- |
|  |  |  |  | Email:  Phone: |
|  |  |  |  | Email:  Phone: |
|  |  |  |  | Email:  Phone: |
|  |  |  |  | Email:  Phone: |

### Assessment Resources and Schedule

The following sections describe the required resources and schedule for conducting the assessment. Significant changes to either resources or planning schedule activities may require an assessment replan.

#### Assessment Resources

*This section should includeresource needs, assessment participants, facility requirements, constraints, and costs not already included in the ROM.*

#### Assessment Schedule

The detailed assessment schedule for each day of the assessment can be found in Appendix B of this Appraisal Plan.

*<An example Assessment Schedule is provided in Appendix B. The CA may choose to use another format and maintain the schedule outside of this plan. If this is done, the assessment schedule must have a revision history that is kept current with schedule changes and the location of the schedule must be referenced here.>*

### Assessment Conflicts of Interest

The following potential Conflicts of Interest (COI) have been identified during assessment planning. Each COI listed has a corresponding mitigation and will be managed throughout this assessment to ensure the mitigation is effectively mitigated.

*<This section identifies known conflicts identified during assessment planning. Assessment conflicts may be used as inputs to risk management. To be updated with common COIs.>*

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

### Assessment Risk and Risk Management

This section identifies risks that could impact the successful conduct of the assessment as planned. Risks are first identified as part of planning, categorized, assessed, assigned a mitigation and then managed to ensure the risk is not realized. Risks status is communicated to the OSC Sponsor throughout the assessment lifecycle.

*<Identify and manage risks to closure throughout the assessment. Consider the risk sources below as part of assessment planning and conduct.>*

| **ID** | **Risk Name** | **Risk Category** | **Risk Description** | **Risk Impact** | **Likelihood** | **Risk Mitigation** | **Risk Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | *<Personnel>* |  |  |  |  |  |
|  |  | *<Logistics>* |  |  |  |  |  |
|  |  | *<Facilities>* |  |  |  |  |  |
|  |  | *<Schedule>* |  |  |  |  |  |
|  |  | *<Cost>* |  |  |  |  |  |
|  |  | *<Data>* |  |  |  |  |  |

## Readiness to Conduct Assessment

This section of the Assessment Plan covers the activities performed under the guidance of the CA to determine readiness to conduct the assessment as planned, including team preparedness, availability of OE, risks and logistics of the OSC, the assessment team, OE, logistics, risks, etc.

### Assessment Team Preparation and Training

The following table defines planned training and other assessment preparation activities required for ATMs. The CA will track completion of these activities as part of verifying assessment readiness.

*<Define any required training or other preparation activities such as appraisal plan review that ATMs will be required to complete in order to participate on the Assessment Team. >*

| **Activity** | **Team Member(s)** | **Plan Date** | **Completion Date** |
| --- | --- | --- | --- |
| <Assessment Scope Orientation> |  |  |  |
| <CMMC Assessment Method Training> |  |  |  |
| <Review Assessment Plan> |  |  |  |
| <Assessment Tool training> |  |  |  |

The following table defines ATM roles and responsibilities during the assessment.

*<Document the assigned roles and responsibilities of team members during the assessment. Include specific responsibilities during the assessment onsite period for artifact review, interview and demo/test conduct.>*

|  |  |
| --- | --- |
| **Team Member** | **Description of Assigned Roles and Responsibilities** |
|  |  |
|  |  |
|  |  |
|  |  |

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

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

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

The Certified Assessor will conduct the CA-RR to verify that the OSC and Assessment Team are ready to conduct the assessment as planned and within the timeframe allocated.

*Need criteria for verification*

The results of the CA-RR provide input to the decision to continue the assessment as planned, replan / reschedule the assessment, or cancel the assessment. The CA and OSC Sponsor defined the following criteria to determine the “go / no-go” decision. As required by the CMMC Assessment Method, these criteria have been reviewed and approved by the C3PAO and CMMC-AB on <enter date(s)>.

1. *<Define Criteria 1>*
2. *<Define Criteria 2, etc.>*

### Results of Certification Assessment-Readiness Review

Based on the results of the CA-RR conducted on *<date>* by *<CA, any ATMs>* and the criteria defined by the OSC Sponsor and CA, the decision has been made to <proceed with the assessment as planned><replan / reschedule the assessment><cancel this assessment>.

| **Verification Criteria** | **Description** |
| --- | --- |
| OE Readiness | *[Describe how the CA will verify that OE provided by the OSC is in a state that supports readiness to proceed with the assessment]*  *[Describe the results of the CA-RR for this criterion.]* |
| Assessment Team Readiness | *[Describe how the CA will verify that the Assessment Team is prepared, trained and ready to conduct the assessment as planned.]*  *[Describe the results of the CA-RR for this criterion.]* |
| Logistical Readiness | *[Describe how the CA will verify that the logistics required to conduct the assessment are available as planned.]*  *[Describe the results of the CA-RR for this criterion.]* |
| Assessment risk status | *[Describe how Assessment Risks will be reviewed to determine if mitigations and status are sufficient to conduct the assessment as planned.]*  *[Describe the results of the CA-RR for this criterion.]* |
| Overall Assessment feasibility | *[Define how the CA will determine if there are any concerns that affect the feasibility of conducting the assessment as planned.]*  *[Describe the results of the CA-RR for this criterion.]* |

# Assessment Plan Approval

**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 required by the Certified Assessor>*

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** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendices

## Appendix A – OSC Request for Assessment

*<Attach a copy of the OSC Request for Assessment as received by the C3PAO>*

## Appendix B – CMMC Assessment Schedule

*[The following is an example CMMC Assessment Schedule Template]*

| **Day** | **Date** | **Start** | **End** | **Activity** | **Areas Covered** | **Participants** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  | Conduct Opening Briefing |  | CA, OSC Sponsor, ATMs, OSC Appraisal Participants |
|  |  | Appraisal Team Training |  | CA, ATMs |
|  |  | Begin OE Artifact Review | <Enter area, practices, controls> | CA, ATMs |
|  |  | Demos | <Enter area, practices, controls> | CA, ATMs, OSC Participant Name(s) |
|  |  | Interview 1 | <Enter area, practices, controls> | CA, ATMs, OSC Participant Name(s) |
|  |  | Day 1 Review | <Enter area, practices, controls> | CA, ATMs, OSC Sponsor |
| 2 |  |  |  | Continue OE Artifact Reviews | <Enter area, practices, controls> | CA, ATMs |
|  |  | *<Continue with other Assessment events>* |  |  |

## Appendix C - <Enter Title>

<*This Appendix is a placeholder to be used (or deleted) by the CA as needed.>*

*<To add additional Appendices, simply add a blank page and copy the Appendix heading and update numbering as appropriate.>*