

**CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)**

**Assessment Plan**

**Target Level <X>**

**for**

*<Company>*

*<Host Unit>*

*<Program Enclave>*

*Version <X.X>*

*<Date>*

Prepared by:

|  |  |
| --- | --- |
| *Certified Assessor* | *<Name>* |
| *C3PAO Representative* | *<Name* |
| *OSC Sponsor* | *<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** |
| *<07-15-20>* | *<V1.0>* | *<Development of Initial Plan Template>* | *<CMMC-AB Method WG>* |
| *<8-26-20>* | *<V2.0>* | *<Baseline with CMMC Assessment Method>* | *<CMMC-AB Method WG>* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*[Instructions on use of the CMMC Assessment Plan template:*

1. *The OSC and Certified Assessor are required to use this template in documenting the CMMC Assessment Plan for any formal Certification Assessment.*
2. *The Assessment Plan template is designed with standard text to record all required planning parameters of the CMMC Assessment Method (CM2CAM).*
3. *Text to be completed by the Assessment Plan authors is noted throughout in <blue italic font within angle brackets>. Font color and style can be changed to* black regular *following input.*
4. *Guidance is provided throughout the template in [italic font within square brackets] and should be deleted (including these Instructions) prior to plan V1.0 baseline.*
5. *The Assessment Plan must be approved by the Certified Assessor and OSC Sponsor prior to the beginning of Assessment Phase 2, “Conduct Assessment” and baselined.*
6. *The final version of the Assessment Plan including updates following baseline must be submitted to the C3PAO and CMMC-AB as part of Assessment Phase 3, “Report Recommended Assessment Results”.]*

**Table of Contents**

[1 Assessment Planning and Preparation 4](#_Toc49337182)

[1.1 Analyze Assessment Requirements 4](#_Toc49337183)

[1.1.1 Certified Third-Party Assessor Organization (C3PAO) 4](#_Toc49337184)

[1.1.2 Assigned Certified Assessor 5](#_Toc49337185)

[1.1.3 OSC Sponsor and Primary Point of Contact (POC) 5](#_Toc49337186)

[1.1.4 High-Level Assessment Scope 5](#_Toc49337187)

[1.1.5 Assessment Scope Details 6](#_Toc49337188)

[1.1.6 Assessment Rough Order of Magnitude (ROM) Estimate 7](#_Toc49337189)

[1.1.7 Objective Evidence - OSC Processes and Process Roles 7](#_Toc49337190)

[1.1.8 Objective Evidence - Adequacy and Sufficiency Criteria 8](#_Toc49337191)

[1.1.9 Assessment Outputs 8](#_Toc49337192)

[1.2 Develop Assessment Plan 9](#_Toc49337193)

[1.2.1 OE Collection Approach 9](#_Toc49337194)

[1.2.2 Assessment Team Members 10](#_Toc49337195)

[1.2.3 Assessment Resources and Schedule 10](#_Toc49337196)

[1.2.4 Assessment Conflicts of Interest 11](#_Toc49337197)

[1.2.5 Assessment Risk Management 12](#_Toc49337198)

[1.3 Readiness to Conduct Assessment 12](#_Toc49337199)

[1.3.1 Assessment Team Preparation and Training 12](#_Toc49337200)

[1.3.2 Inventory and Verify OE 13](#_Toc49337201)

[1.3.3 Certification Assessment Readiness Review (CA-RR) 13](#_Toc49337202)

[2 Assessment Plan Approval 14](#_Toc49337203)

[3 Appendices 15](#_Toc49337204)

[Appendix A – CMMC Assessment Schedule 15](#_Toc49337205)

[Appendix B - <Enter Title> 16](#_Toc49337206)

# Assessment Planning and Preparation

The purpose of this CMMC Assessment Plan is to document results of assessment planning and preparation activities, including the requirements, agreements, estimates, risks, and practical considerations (e.g., schedules, logistics, and contextual information about the organization) associated with the Assessment.

The CMMC Assessment Plan is a required artifact of the CMMC Assessment Method (C2CAM) and is reviewed and approved by the Certified Assessor (CA) and Organization Seeking Certification (OSC) Sponsor.

Documents listed below were used as input to this Assessment Plan and therefore are considered an extension of it. Information obtained from these documents are referenced as needed throughout this plan.

*[Complete this table for each document or form containing planning information or data, including the permanent archival location]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Name** | **Version and Date** | **Authors** | **Location** |
| CMMC-AB Intake Form | *<Vx.x, date>* | *<Enter name(s)>* | *<Link or appendix #>* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Assessment planning and preparation is a series of iterative and incremental activities that continues throughout the assessment, with the content of this plan reflecting associated changes and updates as they occur.

## Analyze Assessment Requirements

Analysis results of assessment requirements are input to assessment planning and scope. The CA performs this analysis with input from and concurrence with the OSC Sponsor and Certified Third-Party Assessor Organization (C3PAO) representative.

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

A Request for Assessment (RFA) was received by the C3PAO from *<OSC name>* on *<date>*.

|  |  |
| --- | --- |
| **C3PAO** | **Description** |
| Name | *<C3PAO Legal Name>* |
| Representative | *<Name of C3PAO representative for this assessment>* |
| Address | *<C3PAO main address, including city and ZIP / Postal Code>* |

### Assigned Certified Assessor

The Certified Assessor is assigned by the C3PAO to perform this assessment.

|  |  |
| --- | --- |
| **Certified Assessor** | **Description** |
| Name | *<Name of assigned CA for this assessment>* |
| 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 Primary Point of Contact (POC)

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

| **OSC** | **Description** |
| --- | --- |
| Assessment Sponsor | *<Name and title of OSC Assessment Sponsor>* |
| Relationship to the OSC being assessed | *< 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) | *<Name of the OSC primary POC for planning the assessment, if not the OSC Assessment Sponsor>* |
| POC Email Address | *<Contact Email of OSC POC>* |
| POC Phone number | *<Contact phone number of OSC POC>* |

### High-Level Assessment Scope

The general high-level assessment scope is concurred to by the CA and OSC Sponsor, working with the C3PAO representative.

| **General Assessment Scope** | **Description** |
| --- | --- |
| OSC Organization | *<OSC Legal Entity Name>* |
| OSC Address | *<Main address, including city and ZIP / Postal Code of OSC>* |
| OSC Host Unit | *<Describe 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 organizational boundaries>* |
| OSC Supporting Unit(s) | *<Describe the name, people, processes, and technology that support the host unit and are included in the assessment>* |
| OSC Associated Enclave(s) | *<Describe the name, people, processes, and technology for any enclaves associated with the host unit that are included in the assessment>* |
| Target CMMC Model Scope / Level | *<Enter CMMC model scope including Target Level>* |
| Assessment Timeframe / Dates | *<Enter the general timeframe / date(s) of the assessment (month/quarter)>* |
| Assessment Location | *<Provide the primary address for the assessment on-site; this may be different from the OSC address>* |
| Assessment Purpose and Background | *<Describe the Assessment purpose (ex. Contractual Certification Requirement) and a brief history of events leading up to the assessment>* |
| Assessment Objectives | *<List the OSC’s objectives for performing the assessment>* |
| Completed Security Assessments | *<Describe any Security certifications/assessments the OSC has earned (ex. NIST 800-171 self-assessment, ISO 27001, etc.)>* |
| Initial Objective Evidence Required | *<List the minimal set of artifacts to be provided to the CA for detailed scope definition, 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>* |

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

Further scoping details and decisions made by the CA and OSC Sponsor in planning this assessment are described in the following sections.

#### Model Reciprocity

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 for reciprocity on *<enter date(s) of examination by CA>*.

*[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 | *<Name of the alternative model results evaluated, ex. Fedramp, NIST 800-181, CMMI V2.0, ISO 27001, etc.>* |
| Date of Assessment / Audit | *<Formal recorded date of the assessment / audit results>* |
| Credentialed Assessor / Auditor / Appraiser | *<Name and validated licensing information for credentialed individual who led the assessment / audit>* |
| CA Reciprocity Examination Results | *<Describe each control / practice validated by the CA for reciprocity or attach validation results as addendum to this plan or provide a link to the validated results.>* |

#### Not Applicable and Inherited CMMC Practices

*[For any practices, controls or processes considered Not Applicable (N/A) or Inherited from other OSC CMMC assessments, describe how they will be verified or provide a reference and link to this information (ex.**CMMC Assessment Tracker tool)].*

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

*[In formulating the ROM estimate, consider if the C3PAO will provide guidelines / limits for assessment pricing, travel and other expense policies and guidelines or restrictions]*

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

The CMMC-AB Assessment Intake Form contains other information used in preparing the ROM estimate. Key assessment dates for each phase of the assessment are summarized below.

|  |  |
| --- | --- |
| **Assessment ROM Estimate** | **Description** |
| Phase 1: Plan and Prepare for Assessment | *<Dates / duration for Assessment Phase 1>* |
| Phase 2: Conduct Assessment | *<Dates / duration for Assessment Phase 2>* |
| Phase 3: Report and Recommend Results | *<Dates / duration for Assessment Phase 3>* |

### Objective Evidence - OSC Processes and Process Roles

The following sources of Objective Evidence (OE) have been provided by the OSC for the target Level:

* OSC Pre-assessment / Self-assessment results: *<provide location or link to most recent results>*
* Mapping of OSC OE (artifact and interview) to targeted in-scope CMMC practices: *<provide location or link to most recent results>*

*[Use results of the most recent pre-assessment or self-assessment conducted by the OSC as input to determining the required OE. The OE mapping to CMMC practices must contain all OSC policies, processes and related plans in scope for the assessment; all OSC personnel and their associated process role in scope for the assessment; all demonstrations / tests that will be observed during the assessment]*

### Objective Evidence - Adequacy and Sufficiency Criteria

The CA determines and confirms the number of needed interviews, observations, reviews and related OE that is needed for each CMMC practice, control or process corresponding to OSC functional areas and process roles.

During the assessment, the CA ensuresall Assessment Team members follow established requirements and rating rules for OE adequacy and sufficiency defined by the CMMC Assessment Method to verify artifacts, affirmations and test / demonstrations as accepted evidence against CMMC practices*.*

### Assessment Outputs

The following assessment records will be produced and archived.

*[Required outputs are listed in the table. If remediation actions are requested / approved, update this table to include additional required outputs from Phase 4. Add any optional assessment outputs agreed to with the OSC Sponsor under the Optional Outputs section (see examples)]*

| Required Outputs | Disposition / Archive |
| --- | --- |
| Initial ROM Estimate of Assessment Scope | *Provided to Sponsor and C3PAO* |
| CMMC Assessment Plan and Schedule | *Provided to Sponsor and C3PAO, submitted as final record to CMMC-AB* |
| Certification Assessment-Readiness Review (CA-RR) results | *Provided to Sponsor* |
| Assessment Opening Briefing presentation | *Provided to Sponsor / Sponsor POC* |
| Daily Checkpoint Log(s) | *Intermediate output* |
| Final Report Part 1: Assessment Final Findings and Recommended Level rating | *Provided to Sponsor and C3PAO, submitted as final record to CMMC-AB* |
| Final Report Part 2: CMMC Assessment Tracker Pass / Fail ratings | *Provided to Sponsor and C3PAO, submitted as final record to CMMC-AB* |
| Optional Outputs | **Disposition / Archive** |
| *<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. The baseline plan version is established following CA and OSC Sponsor approval prior to Phase 2. At the conclusion of the assessment, the final Assessment Plan will reflect all actual results, timing, events and scope covered by the assessment.

### OE Collection Approach

The CA has identified the following methods, techniques and responsibilities for collecting and managing OE.

*[For each type of OE listed, describe the data collection approach, strategy / plan and timeline for completion of OE collection activities. Consider preparation for Readiness Review and Conduct Assessment Phase when determining the timeline.]*

|  |  |  |
| --- | --- | --- |
| **Assessment OE** | **OE Collection Approach** | **OE Collection Timing** |
| Artifacts | *<Describe techniques and responsibilities for collecting and mapping artifacts>* | *<Enter timeline>* |
| Interviews | *<Describe techniques for conducting interviews. Include the approach for Daily Checkpoint discussions>* | *<Enter timeline>* |
| Demonstrations / Tests | *<Describe the approach for observing demonstrations / tests>* | *<Enter timeline>* |
| Preliminary Findings | *<Describe how preliminary finding briefing(s) will be conducted>* |  |
| Virtual Data Collection | *<Describe any virtual OE collection techniques, including video conferences, teleconferences, and other similar technologies to be used during the assessment and when.>* |  |
| Management of Controlled Unclassified Information (CUI) | *<Describe management and protection of CUI throughout all assessment phases>* |  |
| Requests for Information | *<Describe how requests for information (including additional OE or clarifications on provided OE) will be handled by the assessment team and OSC (ex. email, survey, etc.>* |  |

The OE Collection Approach will evolve throughout the Assessment planning period and will be reviewed and updated as needed during the Conduct Assessment Phase.

### Assessment Team Members

*[Complete this section for any Assessment Team Members assigned or indicate that ATMs are not needed]*

The following Assessment Team Members (ATMs) will participate on this assessment. The C3PAO has verified that each ATM meets all CMMC Assessment Method requirements for experience, skills, qualifications and training.

| **Name** | **Organization** | **Cyber or other Security Certifications** | **Security Clearances** | Con**tact Information** |
| --- | --- | --- | --- | --- |
| *<ATM Name>* | *<Employer>* | *<List any credentials>* | *<List any security clearances>* | Email:  Phone: |
|  |  |  |  | Email:  Phone: |
|  |  |  |  | Email:  Phone: |
|  |  |  |  | Email:  Phone: |

#### ATM Roles and Responsibilities

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

|  |  |
| --- | --- |
| **Team Member** | **Description of Assigned Roles and Responsibilities** |
|  | *<List ATM responsibilities. At a minimum include assignment of practices or model components to verify during the assessment>* |
|  |  |
|  |  |
|  |  |

### Assessment Resources and Schedule

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

#### Assessment Participants

The following individuals will participate in the assessment through interviews, tests, or demonstrations. *<Complete the following table for each assessment participant or provide reference and link to this information>*

|  |  |  |
| --- | --- | --- |
| **Name** | **Title / Role** | **Organization Affiliation** |
| *[Enter Participant Name]* | *[Enter Title / Role of the participant in context of this assessment]* | *[Enter organization and area, project, etc. represented]* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### Assessment Facilities and Equipment

*<List any facility requirements to be provided by the host organization. Include requirements for rooms with specific seating capacity, configuration of workroom space, equipment (laptops, printers, etc.), security access requirements, etc.>*

#### Assessment Constraints

*<List any schedule, cost, OE access (security of classification requirements) or other constraints considered as part of assessment planning, ex. “Assessment must be completed within five consecutive business days”>*

#### Assessment Costs

*<List any costs that were not directly considered in ROM estimates or pricing the assessment, including those associated with facilities and equipment required, incidentals such as daily travel and meals, etc.>*

#### Assessment Schedule

The detailed assessment schedule is located in Appendix *<enter appendix letter>* of this Assessment Plan.

*<An example Assessment Schedule is provided in Appendix A. The CA may choose another format and maintain the schedule outside of this plan, keeping a revision history current with schedule changes and referencing the schedule location here.>*

### Assessment Conflicts of Interest

Potential Conflicts of Interest (COI) are managed throughout the assessment to ensure they are effectively mitigated.

*<This section identifies known conflicts identified during assessment planning (ex. security clearance constraints, time zone constraints, etc.). Assessment conflicts may be used as inputs to risk management.>*

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

### Assessment Risk Management

Risks that could impact the successful conduct of the assessment are identified below. Each risk is categorized, assessed, assigned a mitigation and managed to ensure the risk is not realized. Risk 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

The following activities are performed under the guidance of the CA in determining readiness to conduct the assessment as planned within the timeframe allocated.

### Assessment Team Preparation and Training

Planned ATM training and other assessment preparation activities are identified and tracked for completion.

*<Define any required training or other preparation activities for ATMs in order to participate on the Assessment Team. If ATMs are not assigned on the assessment, mark as N/A.>*

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

### Inventory and Verify OE

*<In this section describe the review of any OE including pre-assessment results and their applicability to this assessment. Verify any OE practices considered N/A in section 1.1.5.2 of this plan. Identify and list any issues, gaps or risks in refining the OE collection plan.>*

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

The Certified Assessor conducts the CA-RR using the following criteria to determine if the assessment should continue as planned, be re-planned / rescheduled or cancelled. Criteria were approved by the C3PAO and CMMC-AB on *<enter date(s)>*.

| **Verification Criteria** | **CA-RR Results** |
| --- | --- |
| OE Readiness: *<Define criteria>* | *[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: *<Define criteria>* | *[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.]* |
| Logistics Readiness: *<Define criteria>* | *[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: *<Define criteria>* | *[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 criteria>* | *[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.]* |

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

*<Provide additional information explaining any further outcomes of the CA-RR and next steps.>*

# Assessment Plan Approval

*[If using an electronic signing tool (ex. DocuSign, SignIt, etc.) include the approval record below]*

**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 Assessment plan is accurate and reflects my current agreement with the Assessment Sponsor.

CMMC Certified Assessor:

Signature:

Date:

**Assessment Sponsor (required)**

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

Assessment Sponsor:

Signature:

Date:

**Assessment Team Members** *[Complete**if required by the CA, otherwise remove]*

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 – CMMC Assessment Schedule

*[The following is an example CMMC Assessment Schedule. Use this or any preferred schedule format to document a detailed schedule for each day of the assessment.]*

| **Day** | **Date** | **Start** | **End** | **Activity** | **Areas Covered** | **Participants** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  | Conduct Opening Briefing |  | CA, OSC Sponsor, ATMs, OSC Assessment Participants |
|  |  | Assessment Team Training |  | CA, ATMs |
|  |  | Begin OE Artifact Review | <Enter area, practices, controls> | CA, ATMs |
|  |  | Demo Observations | <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 B - <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.>*