



Self-Evaluation Guide

Companion Document to
C2M2 Version 2.1

June 2022

TABLE OF CONTENTS

Acknowledgments	ii
Introduction	iii
1. Preparation	1
1.1 Obtain the Latest Version of the C2M2 Materials	1
1.2 Assign Key Roles in the C2M2 Self-Evaluation Process	2
1.3 Select a Facilitator	5
1.4 Hold a Self-Evaluation Preparation Meeting	6
1.5 Manage Workshop Logistics	11
2. The Self-Evaluation Workshop	12
2.1 Kick Off the Workshop	12
2.2 Facilitate the Workshop	13
2.3 Generate Self-Evaluation Results	14
2.4 Present Self-Evaluation Results	14
2.5 Close the Workshop	18
3. Follow-Up	19
3.1 Perform Further Analysis	19
3.2 Review Outcomes with the Sponsor	20
3.3 Plan Follow-Up Actions	20
Appendix A: Self-Evaluation Checklist	21
Appendix B: Common Discussions	26
Appendix C: Related Practices	29
Appendix D: Setting Targets	39
Appendix E: Scoring Guidance for Multiple Organizational Functions	42

LIST OF FIGURES

Figure 1: Example of a C2M2 Self-Evaluation Virtual Workshop Schedule	10
Figure 2: Example Summary of Responses by MIL and Domain	15
Figure 3: Example Implementation of Management Activities across Domains	17
Figure 4: Example Detailed Self-Evaluation Results for the ASSET Domain	18

LIST OF TABLES

Table 1: Key C2M2 Self-Evaluation Materials	1
Table 2: Key Roles in the Self-Evaluation Process	2
Table 3: Possible Roles of Participants Needed	8
Table 4: Topics for Discussion at the Start of the Workshop	12
Table 5: Practices with Dependencies	29
Table 6: Input-From Relationships	30
Table 7: Practice Progressions	34
Table 8: Information-Sharing Practices	38

ACKNOWLEDGMENTS

The Department of Energy (DOE) thanks the individuals who provided the experience and technical expertise that enabled development of this document.

Program Lead

Fowad Muneer

Office of Cybersecurity, Energy Security, and Emergency Response
United States Department of Energy

Program Team

Name	Organization
Brian David Benestelli	Carnegie Mellon University Software Engineering Institute – CERT Division
Richard Caralli	Axio
Pamela Curtis	Axio
John Fry	Axio
Cynthia Hsu	National Rural Electric Cooperative Association
Lindsay Kishter	Nexight Group
Annabelle Lee	Nevermore Security
Julia Mullaney	Carnegie Mellon University Software Engineering Institute – CERT Division
Ryan Subers	Axio
David White	Axio

INTRODUCTION

The purpose of this guide is to help organizations to conduct a Cybersecurity Capability Maturity Model (C2M2) self-evaluation. Typically, a C2M2 self-evaluation is done during a facilitated, one-day, in-person workshop or a series of 60-to-90-minute sessions if conducted virtually. Workshop participants would include key individuals who understand how the organization being evaluated implements cybersecurity practices.

This organization of this guide follows the phases of a typical self-evaluation:

1. Preparation
2. Performing the Self-Evaluation
3. Follow-Up

[Appendix A](#) is a checklist of the tasks in each of these phases. [Appendix B](#) provides guidance to help facilitators prepare for discussion topics that commonly arise during self-evaluations. [Appendix C](#) describes and provides lists of four types of practice relationships that can be important in self-evaluation scoring and cybersecurity program planning. [Appendix D](#) provides information about why and how to set domain-based or practice-based performance targets. [Appendix E](#) contains guidance for aggregating scores for multiple functions within the same organization.

Those using this guide should review the introductory sections of the [C2M2 model document](#), in particular the “Core Concepts” and “Model Architecture.”

1. PREPARATION

This section describes the planning and preparation activities that should be executed during the first phase of the C2M2 self-evaluation process, then reviews some common issues that can impact the success of the C2M2 self-evaluation process.



- 1.1 Obtain the Latest Version of the C2M2 Materials**
- 1.2 Assign Key Roles in the C2M2 Self-Evaluation Process**
- 1.3 Select a Facilitator**
- 1.4 Hold a Self-Evaluation Preparation Meeting**
- 1.5 Manage Workshop Logistics**

1.1 Obtain the Latest Version of the C2M2 Materials

Those involved in planning for the self-evaluation should have the latest version of the complete set of materials listed in Table 1. These materials and additional resources can be downloaded or obtained from the [C2M2 Program web page](#).

Table 1: Key C2M2 Self-Evaluation Materials

Title	Brief Description
Cybersecurity Capability Maturity Model V2.1	The model, including the introductory sections (“Introduction,” “Background,” “Core Concepts,” etc.)
Self-Evaluation Guide	This document
Self-Evaluation Tools	There are a variety of free and commercial software tools for completing and scoring a C2M2 evaluation, including a free C2M2 tool , offered by the Department of Energy, that is available on two platforms: a PDF-based and HTML-based tool. The tools offer interactive features and help text, allow users to securely record results, and automatically generate a detailed, graphical report. In both tool formats, all user data remains on user devices.
Self-Evaluation Report	The report, generated by the DOE C2M2 V2.0 Self-Evaluation Tool (or an equivalent report generated by another tool), documents the results of the self-evaluation. There is no need to obtain this document separately. It is part of the self-evaluation tools mentioned above.
Self-Evaluation Workshop Kickoff Presentation	The presentation can be used to kick off a C2M2 self-evaluation workshop. The presentation provides an overview of the model, helps participants

Title	Brief Description
C2M2 Overview Presentation	understand the scope of the self-evaluation, and helps participants understand the response scale and other elements of the self-evaluation. The presentation provides a high-level overview of C2M2 that can be used during presentations to executives and other stakeholders to brief them about what C2M2 is and how it can be leveraged in the organization.
Self-Evaluation Cheat Sheet	The two-page, placemat-style guide is populated with condensed C2M2 information for use as a reference by workshop participants during a C2M2 self-evaluation.

1.2 Assign Key Roles in the C2M2 Self-Evaluation Process

A successful C2M2 self-evaluation process requires the involvement and active participation of members of the organization who serve in a variety of roles. The roles and responsibilities involved in a typical C2M2 self-evaluation process are described in Table 2.

Table 2: Key Roles in the Self-Evaluation Process

Role	Description and Responsibilities
Organizer	<p>The organizer has the overall responsibility for preparing the organization for the C2M2 self-evaluation and ensuring its success. The organizer role, required skills, and responsibilities are similar to that of a project manager.</p> <p>Organizer responsibilities may include the following tasks:</p> <ul style="list-style-type: none"> • Ensure that all activities in the self-evaluation process are executed efficiently and effectively • Work with the sponsor and facilitator to define the scope of the self-evaluation • Assist the sponsor in making important decisions • Help the sponsor determine the scope of the self-evaluation • Support the sponsor in identifying appropriate personnel to fill each role needed to complete the self-evaluation • Communicate with the facilitator, the sponsor, and others • Escalate unresolved issues to the sponsor • Assist the facilitator in understanding the organization and how it functions, if needed • Ensure that participants are available to attend the workshop • Ensure that proper facilities and support staff are available for the workshop

Role	Description and Responsibilities
Facilitator	<p>The facilitator is responsible for planning and facilitating the C2M2 self-evaluation workshop. The facilitator should be familiar with all the materials listed in Table 1 in advance of the self-evaluation workshop.</p> <p>Facilitator responsibilities may include the following tasks:</p> <ul style="list-style-type: none"> • Work with the sponsor, organizer, and participants to ensure the self-evaluation workshop produces high-quality results • Work with the sponsor and organizer to confirm or refine the scope of the self-evaluation • Facilitate the C2M2 self-evaluation workshop • Answer questions about the model content and the intent of the practices • Generate the C2M2 Self-Evaluation Results • Distribute the C2M2 Self-Evaluation Results to the sponsor and designees • Review the detailed outcomes with the sponsor and designees • Assist in the planning of follow-up activities <p>The facilitator may also be responsible for recording responses and comments during the self-evaluation workshop, if a scribe is not available to perform this responsibility.</p>
Sponsor	<p>The sponsor demonstrates organizational management’s commitment to using the C2M2 self-evaluation and helps ensure the participation of staff members needed to obtain meaningful results. The sponsor should have a broad understanding of the status and components of the function for which the self-evaluation is being completed. It is most helpful for a sponsor to be:</p> <ul style="list-style-type: none"> • Part of the senior management or executive team • Acknowledged by the participating staff members as being in charge of their efforts and responsible for results • Motivated and able to dedicate sufficient time and thoughtful attention as needed <p>Sponsor responsibilities may include the following tasks:</p> <ul style="list-style-type: none"> • Decide whether the organization should complete a C2M2 self-evaluation • Select an individual to serve as the facilitator • Work with the organizer to define the scope of the self-evaluation • Ensure that the necessary resources for the self-evaluation process are available, including by: <ul style="list-style-type: none"> ○ Committing resources and access to those resources ○ Assigning the point of contact and other personnel resources ○ Asking the team members to provide the necessary support • Communicate the business driver and the organization’s support for the self-evaluation process • Ensure that the self-evaluation output will receive the attention it deserves across the organization • Kick off the C2M2 self-evaluation workshop • Participate in resolving issues and problems that arise during the self-evaluation process

Role	Description and Responsibilities
SMEs	<p>Subject matter experts (SMEs) evaluate the organization’s current cybersecurity capabilities in relation to the C2M2 domain practices and the function being evaluated. It is most helpful for an SME to be:</p> <ul style="list-style-type: none"> • Closely involved in the planning, implementation, or management of the domain represented • Able to understand or speak about one or more of the following areas: cyber and physical security, business continuity and disaster recovery, security architectures, critical infrastructure protection, operation of the function • Able to assess the organization’s capabilities for the function being evaluated
Observers	<p>Observers may benefit from the facilitation but may not be required for the development of responses during the self-evaluation. The facilitator, sponsor, and participants should be notified of any potential observers.</p>
Scribe	<p>An individual should be assigned to capture responses, on-screen notes, and action items. A scribe enables the facilitator and SMEs to focus on the self-evaluation discussions without the need to stop to take notes.</p>
Support staff	<p>In collaboration with the sponsor and organizer, the facilitator should identify all other individuals whose support is necessary during all three phases of a typical C2M2 self-evaluation process, such as:</p> <ul style="list-style-type: none"> • Administrative assistants to send meeting invitations, coordinate calendars, copy and assemble materials • Technology support staff to set up and manage necessary technology and equipment for the workshop • Site security staff to issue visitor badges and enable physical access by the visitors • Virtual workshop support staff to monitor audio and mute participants as needed, manage questions or key discussion points in the chat, and manage screen-sharing
Participants	<p>All individuals whose presence and active participation is necessary during the self-evaluation workshop (e.g., sponsor, facilitator, SMEs) are referred to as <i>participants</i>. The sponsor should encourage all participants to be present for the duration of the workshop.</p>

1.3 Select a Facilitator

Selecting an effective facilitator is critical. The facilitator is an individual who helps self-evaluation workshop participants have productive discussions, reach consensus, and document decisions and outcomes. The facilitator helps to plan an effective workshop agenda and helps keep discussions on time and on track.

An effective facilitator will perform the following actions:



Prepare

- Attain proficiency with the model and self-evaluation tools prior to the workshop, including the model practices and associated help text.
- Be well-versed in the technical and strategic environment that falls within the scope of the organization's self-evaluation.



Moderate

- Exhibit strong listening and synthesis skills, including the ability to paraphrase and summarize discussions.
- Act as a timekeeper, enforcing an agreed-upon agenda and adjusting in real time.
- Ensure a balanced discussion among participants by drawing out input from key stakeholders and more reticent group members.
- Clarify points of disagreement to help move discussions toward consensus.
- Act as a neutral party and not contribute to or influence decisions.



Document

- Document results and key notes from the discussion using the chosen self-evaluation tool, unless this responsibility is delegated to a scribe.

The facilitator needs to have a thorough knowledge of and experience with the C2M2 to be able to help set the scope of the self-evaluation and to answer questions during the self-evaluation and follow-up. The facilitator should have sufficient technical competence to be able to understand and participate in discussions about the technical aspects of implementing C2M2 practices.

Facilitators can help prepare participants by providing them copies of the C2M2 and/or having them participate in face-to-face or virtual meetings during which the facilitator provides background information about the C2M2.

1.4 Hold a Self-Evaluation Preparation Meeting

Prior to setting a date for the self-evaluation workshop, the organizer should schedule a meeting with the sponsor, the facilitator, and possibly other key participants to prepare for the self-evaluation. The objectives of this meeting (or meetings) include the following:

- Familiarize the sponsor and other key participants with the C2M2.
- Obtain strong and visible executive support for the C2M2 self-evaluation process and the associated workshop.
- Discuss the sponsor’s expectations for the self-evaluation process logistics (e.g., the three phases of the process, required resources, time frame involved, personnel roles and responsibilities).
- Discuss the sponsor’s expectations for how the C2M2 self-evaluation results might be used.
- If the facilitator is external to the organization, familiarize the facilitator with the organization’s operating environment and the business drivers influencing its cybersecurity efforts.
- Determine the scope of the self-evaluation (described in [Identify the Scope of the Self-Evaluation](#)).
- Identify the participants that will be needed for the self-evaluation workshop (described in [Identify Workshop Participants](#)).
- Determine the schedule and timing of the self-evaluation workshop to optimize participation (described in [Schedule the C2M2 Self-Evaluation Workshop](#)).
- Decide whether the workshop will be in person or virtual, and if in person, decide on the location.
- Decide whether to set targets and, if so, how and when (described in Appendix D, [Setting Targets](#)).
- If performing self-evaluations for multiple functions in the same organization, decide whether scores will be aggregated and, if so, how (described in Appendix E, [Scoring Guidance for Multifunction Organizations](#)).

1.4.1 Identify the Scope of the Self-Evaluation

Though the C2M2 can be applied to an entire enterprise, organizations often perform separate self-evaluations for individual functions, particularly in cases where cybersecurity is managed differently across functions. The sponsor, the organizer, the facilitator, and other key participants should collaborate to identify the appropriate scope for each self-evaluation. Selecting the scope before conducting the self-evaluation workshop is essential. The scope determines who will participate in the self-evaluation.

The term *function* is used in the model to refer to the part of the organization that is in scope for each self-evaluation. See Section 3.2.1, “Function,” in the model for further information about the term *function*.

Identifying the right scope improves the accuracy of self-evaluation results. Limiting the scope of a self-evaluation to one part of the organization that manages cybersecurity in a similar manner avoids a situation where two different groups of participants may respond differently to a practice. In the event that two different groups have two different responses, a compromise must be made, which could dilute the accuracy of the response.

Care should be given to select a scope that provides a good balance between accuracy and time spent performing individual self-evaluations. When time is limited, multiple, parallel self-evaluations can be performed in one workshop. Additionally, a single self-evaluation can be split into two during a workshop if it becomes evident that participant responses may not accurately reflect the organization’s cybersecurity practices. A general rule for finding the right balance between accuracy and the time spent performing self-evaluations is to identify the fewest number of self-evaluations that still provides an accurate picture of the organization’s cybersecurity practices.

1.4.2 Identify Workshop Participants

For a C2M2 self-evaluation to be successful, participants with knowledge of how cybersecurity practices are implemented in the organization will be required. What is important is having the right mix of participants in the workshop to provide accurate responses for each of the 10 C2M2 domains. It is not necessary to have a single SME for

Energy Sector Scope Examples

The examples below identify typical functions for each subsector; however, the model can be applied to other functions or subfunctions performed by the organization, or to the entire enterprise.

Electricity Subsector

The typical focus is on high-level functions performed by electric utilities such as generation, transmission, distribution, and markets.

Oil and Natural Gas Subsector

The typical scope is on a subset of functions performed by members of the subsector, in these three categories:

Upstream Functions

- Crude oil production
- Natural gas production

Midstream Functions

- Transportation
- Marine terminals
- Underground storage
- Aboveground storage
- Petroleum markets
- Natural gas markets

Downstream Functions

- Refining
- Natural gas processing
- Distribution
- Retail

each domain; an individual can be an SME for multiple C2M2 domains. Alternatively, it may be necessary to engage multiple SMEs to fully cover a single domain.

Table 3 lists the relevant staff who may participate in the C2M2 self-evaluation. Three roles are common to all 10 domains: cybersecurity leadership, IT leadership, and OT leadership.

Table 3: Possible Roles of Participants Needed

Domain	Relevant Staff
Asset, Change, and Configuration Management (ASSET)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • IT and OT team members responsible for asset inventory management
Threat and Vulnerability Management (THREAT)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • IT and OT patching team members • Security Operations Center (SOC) leadership • Team members responsible for tracking external cybersecurity threats and events
Risk Management (RISK)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Enterprise Risk Management team members • Team members responsible for cybersecurity risk • Internal audit team members • Legal team members
Identity and Access Management (ACCESS)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Facilities management team members • IT and OT team members responsible for provisioning logical and physical access • Human resources team members
Situational Awareness (SITUATION)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Incident response team members • Security Operations Center (SOC) leadership • Team members responsible for logging and monitoring IT and OT assets
Event and Incident Response, Continuity of	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership

Domain	Relevant Staff
Operations (RESPONSE)	<ul style="list-style-type: none"> • Security Operations Center (SOC) leadership • Incident response team members • Business continuity team members • Facilities team members
Third-Party Risk Management (THIRD- PARTIES)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Procurement team members • Third-party vendor management • Third-party risk management • Human resources team members • Legal team members • IT and OT team members responsible for provisioning logical and physical access
Workforce Management (WORKFORCE)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • IT and OT team members responsible for provisioning logical and physical access • Human resources team members • Team members responsible for cybersecurity awareness training • Team members responsible for job skill assessment and training program
Cybersecurity Architecture (ARCHITECTURE)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Team members responsible for IT and OT architecture • Team members responsible for cybersecurity architecture • Team members responsible for IT and OT software development • Team members responsible for data protection and privacy
Cybersecurity Program Management (PROGRAM)	<ul style="list-style-type: none"> • Cybersecurity leadership • IT leadership • OT leadership • Enterprise • Legal team members • Compliance team members • Internal audit team members

The selected function may not perform *all* the practices in each domain and may, instead, inherit the performance of those practices from another part of the organization that is also conducting a self-evaluation. In this instance, an individual from that part of the organization should attend the workshop to enable a complete representation of practices for each

domain. If certain activities are outsourced, it may be necessary to ask a representative from the outsourced third party to attend the workshop.

In addition to SMEs discussed above, the sponsor or organizer should identify support staff that may be required to assist in conducting the self-evaluation (e.g., scribes, IT support). Although not required, it is helpful if the SMEs, executives, operations personnel, and other participants are familiar with the C2M2 prior to beginning the self-evaluation.



A list of potential workshop participants is included in Identify Workshop Participants.

1.4.3 Schedule the C2M2 Self-Evaluation Workshop

The organizer collaborates with the facilitator, the sponsor, and participants to schedule the self-evaluation workshop. Assistance from the sponsor or executive management might be necessary to communicate the importance of workshop attendance and enable SMEs and other critical participants to allocate the required amount of time.

The organizer should schedule at least eight hours for the workshop. An on-site workshop can be done in one day or split into two four- or five-hour sessions during two consecutive days. If the workshop is conducted virtually, it should be scheduled in 60-to-90-minute sessions over several days, across ideally one week or a maximum of two weeks. While several sessions can occur in one day, sessions are more effective when participants have a break after 90 minutes. For virtual workshops, it can be more difficult to get all participants to attend every session, although that is ideal. Additionally, for both on-site and virtual workshops, the facilitator should allocate extra time for the first domain (approximately one hour) to allow for additional discussions and questions that normally occur within groups new to the C2M2. Figure 1 is a notional depiction of how C2M2 domains could be split across a set of five virtual workshop sessions.

	Monday	Tuesday	Wednesday	Thursday	Friday
9:00 AM	Workshop Session One				Workshop Session Five
	C2M2 Introduction and ASSET Domain	Workshop Session Two	Workshop Session Three		ARCHITECTURE and PROGRAM Domains, and Self-Evaluation Results
10:00 AM		THREAT and RISK Domains	ACCESS and RESPONSE Domains	Workshop Session Four	
				SITUATION, THIRD-PARTIES, and WORKFORCE Domains	
11:00 AM					

Figure 1: Example of a C2M2 Self-Evaluation Virtual Workshop Schedule



A checklist of specific tasks for scheduling the self-evaluation workshop is included in Appendix A.

1.5 Manage Workshop Logistics

An efficient self-evaluation workshop requires considerable logistical preparation in the days and weeks leading up to the workshop. This includes planning, agenda setting, and participant preparation several weeks before the workshop; room preparation, dry runs, and role coordination on the day and morning of the workshop; and post-workshop tasks in the week following. The organizer, the facilitator, and support staff should collaborate to manage all workshop logistics.



A checklist of specific tasks for self-evaluation workshop logistics is included in Appendix A.

2. THE SELF-EVALUATION WORKSHOP

This section describes the second phase of the C2M2 self-evaluation process: conducting the self-evaluation workshop.



- 2.1 Kick Off the Workshop**
- 2.2 Facilitate the Workshop**
- 2.3 Generate Self-Evaluation Results**
- 2.4 Present Self-Evaluation Results**
- 2.5 Close the Workshop**

2.1 Kick Off the Workshop

Begin the workshop with comments from the organization’s senior management if possible. These remarks can help emphasize the importance of completing a C2M2 self-evaluation to the organization, identify the business drivers for the organization’s cybersecurity efforts, and highlight the importance of the active participation of self-evaluation workshop attendees.

Either before or after comments from senior management (depending on their preference), the facilitator should present the self-evaluation workshop kickoff presentation completed in the Preparation phase.

It is useful to remind participants that the self-evaluation is intended to provide a current snapshot of the maturity of the organization’s cybersecurity practices. Table 4 describes several topics that may require special emphasis when beginning the workshop. Slides for some of these are included in the self-evaluation workshop kickoff presentation.

Table 4: Topics for Discussion at the Start of the Workshop

Topic	Discussion
Agreed-upon function and scope	Remind participants that the self-evaluation is focused on a specific part of the organization. Confirm participants’ understanding of the scope. See Identify the Scope of the Self-Evaluation for more guidance on scoping.
Assets related to the function in scope	These are the IT, OT, and information “assets that support the delivery of the function” and “assets within the function that may be leveraged to achieve a threat objective.” Participants may need some guidance about the intended meaning of these terms in the model. See Section 3.3, “Assets,” in the model for more information.

Topic	Discussion
Addressing activities planned for the future	<p>When evaluating possible responses, participants should consider practices as they are implemented on the day of the workshop. Do not consider activities that are planned or are in the process of implementation. This process can be a good opportunity for capturing notes about in-progress or planned projects. Participants can then consider updating their self-evaluation when in-progress or planned projects are complete.</p> <p>Also, do not consider practices that have not been performed for extended periods of time. For example, if the organization has a disaster recovery plan that, in the opinion of the participants, is out of date to the point of being unusable, the plan should not be considered.</p>
Four-point response scale	<p>Participants use a four-point response scale to evaluate the degree to which the organization has implemented each practice. Review with the participants the meaning of each of the four response options. See Appendix B for additional information about the distinction between Largely Implemented and Partially Implemented.</p>
Follow-up activities	<p>The facilitator sets the expectation for the workshop and the roles of the participants. It is important to discuss how the survey will be used within the organization’s overall cybersecurity program. Emphasize that next steps will be based on the organization’s risks and maturity. The output of the C2M2 self-evaluation should drive risk conversations and allow organizations to plan periodic reviews of their cybersecurity program to track progress and validate goals. Point out the roles of participants in follow-up activities. See the Follow-Up section for additional information.</p>

2.2 Facilitate the Workshop

For each domain, read the description of the domain, each objective name, and each practice. Describe the intent of each practice. Consult the glossary in the model or the help text, as needed. Where necessary, remind participants that if not all activities in a practice are implemented, the response should reflect the incompleteness of implementation.

Most groups find it helpful to view a visual (projected) display of the practices as they are considered, and to be able to see the responses they have already provided. The facilitator or scribe records the participant’s responses in the C2M2 Self-Evaluation Tool. The C2M2 practices and participant responses are displayed on the screen for everyone to see. Record important points from discussions (such as the rationale for a response) in the evaluation tool’s “Notes” field.

At times the facilitator will need to remind participants not to get stuck on the specific phrasing of a question but to focus on the intent behind the question. When consensus cannot be achieved, it may be useful add the topic to a “parking lot” list and return to it later. The glossary in the model and the C2M2 help text can be useful in helping participants reach this understanding and should be made available to participants during the workshop.

2.2.1 Consensus and Dialogue

The facilitator guides the participants in reaching consensus responses to each practice listed in the self-evaluation. The facilitator does not provide responses but rather helps the group come to a consensus response. Open dialogue and consensus building is an important part of the self-evaluation process. Consensus has been achieved when every participant feels that his or her views have been heard and when all participants feel they can support the proposed response. Consensus does not mean that all participants agree with the proposed response.

2.2.2 Visual Aids

Materials such as dry-erase boards, easels, and flip charts with markers may help to support self-evaluation. These materials can be used to illustrate or diagram concepts, as well as to capture and display common assumptions developed by the group that were key to allowing the group to come to consensus. The facilitator can refer to these illustrations throughout the discussion to provide useful reminders of the participants' rationale when needed.

2.2.3 Related Practices

There are four types of related practices: dependencies, practice progressions, input-from relationships, and information-sharing practices. Each type is described in detail in Appendix C. Dependencies are noted in parentheses in the practice text, while the other types of related practices are noted in the help text within the self-evaluation tool.

Dependencies and practice progressions are important to consider when choosing the implementation level for a practice during a self-evaluation. Input-from relationships and the information-sharing practices group are less likely to impact the self-evaluation, but may need to be explained to participants.

2.3 Generate Self-Evaluation Results

After all responses to the C2M2 self-evaluation have been entered into the self-evaluation tool, the facilitator can generate the report. During this time, it may be useful to allow participants to take a short break.

2.4 Present Self-Evaluation Results

Use the C2M2 Self-Evaluation Report to conduct a review at the end of the self-evaluation. The facilitator should consider the time remaining and the expectations of the participants. Most participants are tired at the end of the day and do not have energy to listen to a detailed review of the report. Nevertheless, participants usually appreciate some same-day discussion and presentation of the results so that they see tangible results.

The Self-Evaluation Report presents the results at varying levels of detail, using a variety of visuals. The following sections offer guidance on interpreting and presenting several of the report’s key summary graphics.

2.4.1 Interpreting the Donut Charts

Figure 2 provides a graphical summary of overall results, depicted as a 3x10 matrix of donut charts that relate each domain to progressively advancing maturity indicator levels (MILs).

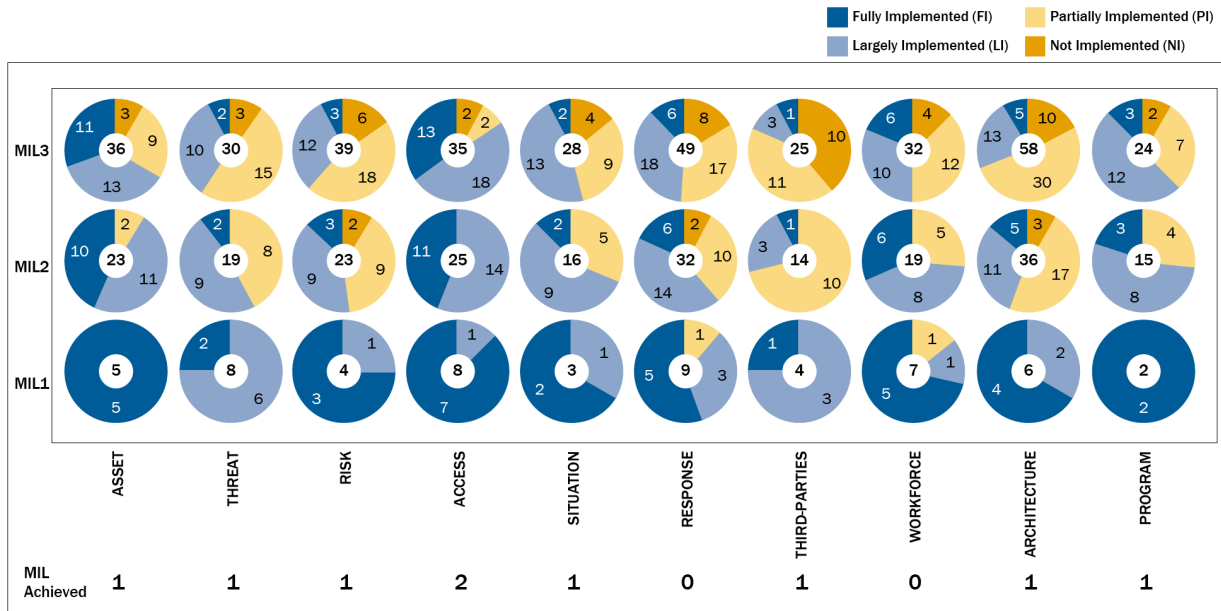


Figure 2: Example Summary of Responses by MIL and Domain

The blue sectors show the number of practices rated “Fully Implemented (FI)” in dark blue or “Largely Implemented (LI)” in light blue. Yellow sectors provide a count of the number of practices rated “Partially Implemented (PI)” in light yellow or “Not Implemented (NI)” in dark yellow. For example, the PROGRAM domain MIL3 donut chart from Figure 2 shows that there are 24 practices in the PROGRAM domain; 2 practices are scored as NI, 7 practices are PI, 12 practices are LI, and 3 practices are FI.

The number in the center of each donut chart represents the cumulative number of practices for each MIL. Looking at the PROGRAM domain MIL1 donut chart shows that there are 2 PROGRAM domain practices at MIL1, an additional 13 practices at MIL2 (15–2), and an additional 9 practices at MIL3 (24–15).

To achieve a MIL in a domain, all practices in that MIL and in all preceding MILs must have responses of either Fully Implemented or Largely Implemented. A MIL is not achieved if any practices in that MIL or a preceding MIL were rated Partially Implemented or Not Implemented. For example, to achieve MIL3, all responses for MIL3, MIL2, and MIL1 must receive a response of Largely Implemented or Fully Implemented.

To demonstrate, a quick inspection of the domain summary example in Figure 2 indicates that at MIL1, there are two domains, RESPONSE and WORKFORCE, where some practices were rated Partially Implemented. Therefore, MIL1 has not been achieved in RESPONSE and WORKFORCE, and these two domains are at MILO.

The facilitator should clarify that achieving the highest MIL in all domains may not be optimal for an organization. Some practices may not make sense for implementation based on the organization's operations, risk, or business considerations. Organizations are encouraged to set their own targets for implementation of C2M2 practices, either before or after conducting a self-evaluation. For more information, see Appendix D, [Setting Targets](#).

The domain summary may highlight potential areas for cybersecurity investment by drawing attention to domains where there are differences between implementation levels and organizational targets.

2.4.2 Interpreting the Summary Implementation of Management Practices

The final objective of each C2M2 domain includes practices focused on cybersecurity management activities. These practices focus on the extent to which cybersecurity practices are institutionalized, or ingrained, in the organization's operations. The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the activity over time; the activity will be retained under times of stress; and the outcomes of the activity will be consistent, repeatable, and of high quality.

Figure 3 provides a high-level overview of implementation of the Management Activities practices from two perspectives: 1) implementation of all Management Activities within each domain and 2) implementation of each Management Activities practice across the ten C2M2 domains.

MANAGEMENT PRACTICES	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	WORKFORCE	ARCHITECTURE	PROGRAM
Documented procedures are established, followed, and maintained for activities in the domain	FI	PI	LI	FI	LI	FI	PI	FI	PI	LI
Adequate resources (people, funding, and tools) are provided to support activities in the domain	LI	PI	PI	FI	LI	LI	PI	LI	PI	LI
Up-to-date policies or other organizational directives define requirements for activities in the domain	LI	PI	PI	FI	LI	LI	NI	LI	PI	LI
Personnel performing activities in the domain have the skills and knowledge needed to perform their assigned responsibilities	PI	PI	LI	FI	PI	LI	NI	NI	PI	LI
Responsibility, accountability, and authority for the performance of activities in the domain are assigned to personnel	FI	LI	LI	LI	LI	PI	NI	PI	PI	LI
The effectiveness of activities in the domain is evaluated and tracked	NI	PI	PI	PI	PI	NI	NI	NI	NI	PI

Figure 3: Example Implementation of Management Activities across Domains

2.4.3 Interpreting Detailed Self-Evaluation Results for Each Domain

For each domain, the detailed self-evaluation results summary includes:

- Donut charts depicting practice implementation for each objective within the domain
- A horizontal chart detailing practice implementation for each MIL within the domain
- Implementation for each practice within the domain

Figure 4 provides an example of results presented for the ASSET domain.

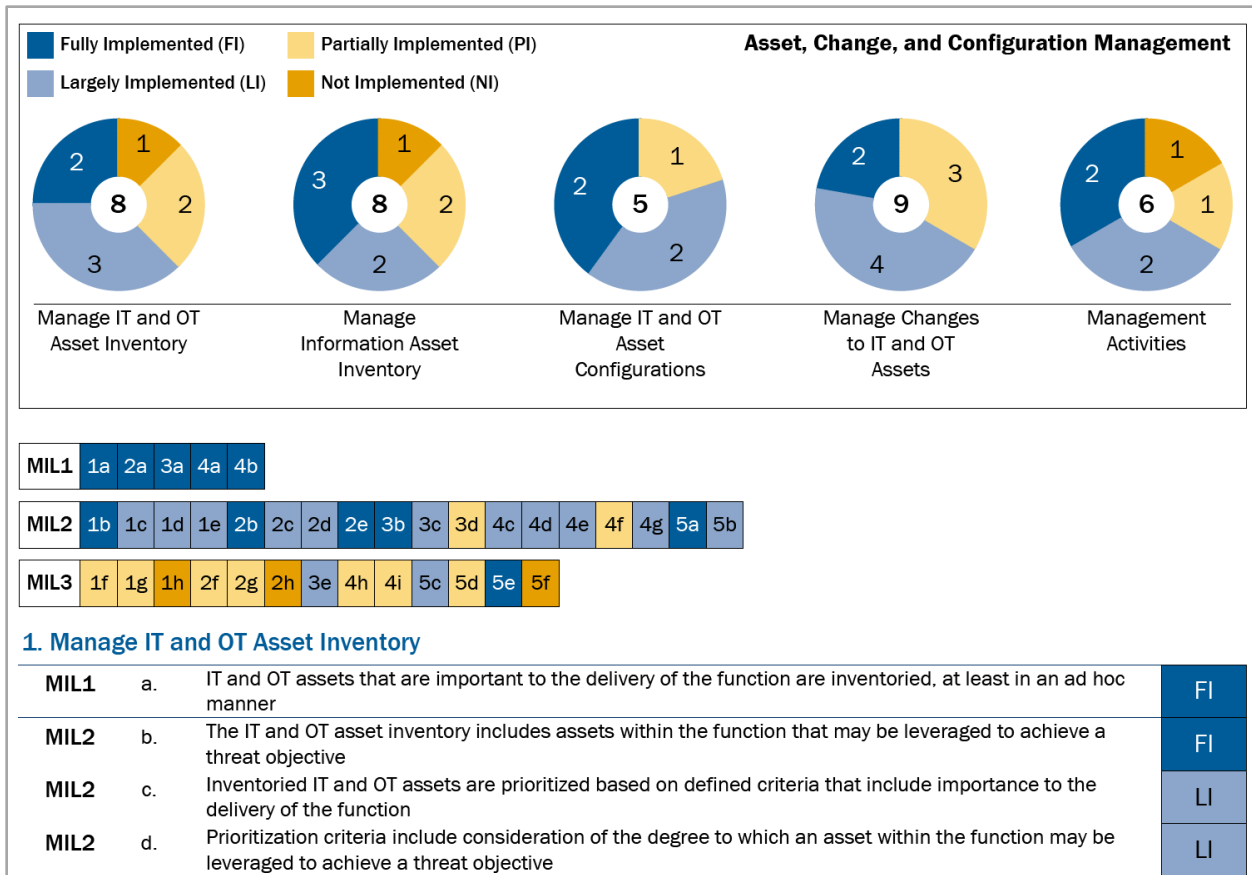


Figure 4: Example Detailed Self-Evaluation Results for the ASSET Domain

2.4.4 Other Report Results

Additional sections in the report include a summary of notes captured for each practice and a list of Partially Implemented and Not Implemented practices. While the facilitator should be prepared to briefly review these report sections during the workshop, they are particularly useful in supporting post-working analysis and action planning.

2.5 Close the Workshop

The facilitator can, with input from the organizer and sponsor, discuss potential follow-up activities with participants prior to closing the workshop. The facilitator or the organizer should also tell the participants what, if anything, they will receive after the workshop, such as a copy of the report or a summary of the report results. Provide an opportunity for all participants to make final comments or observations, and give the sponsor an opportunity to make closing remarks.

3. FOLLOW-UP

This section describes the third phase of the self-evaluation process.



- 3.1 Perform Further Analysis**
- 3.2 Review Outcomes with the Sponsor**
- 3.3 Plan Follow-Up Actions**

3.1 Perform Further Analysis

Before submitting results to the sponsor, the organizer, along with the facilitator and other relevant participants, may want to conduct a detailed analysis of the self-evaluation results. This list below includes aspects of the results that may warrant more detailed analysis and the sponsor's attention:

- Identify strengths and potential target areas for improvement. In particular, examine the following:
 - MILs with very few unimplemented practices
 - Domains or objectives with very few unimplemented practices
 - Objectives that are wholly unimplemented
 - Practices in Management Activities that are unimplemented or that are implemented in very few domains
 - Contradictory implementation results
 - Observations that are counter to the organization's stated or implied objectives
- Conduct comparisons of results that may provide insights to support action plans:
 - Results from different organizational units to identify commonalities and exceptions
 - Results over time
 - Results to target scores
- Examine results from the enterprise-focused domains—RISK, ARCHITECTURE, and PROGRAM—to obtain enterprise-level insights. For example, cyber risk management may be a subset of enterprise risk activities, and results from the RISK domain may identify strengths or weaknesses in enterprise-level activities.

3.2 Review Outcomes with the Sponsor

The organizer and the facilitator should present findings, analysis, and recommendations to the sponsor, organizational leadership, and other key participants. It may be best to extract portions of the report to display in presentation form rather than reviewing the full report itself.

3.3 Plan Follow-Up Actions

Organizations can use their self-evaluation results to identify gaps and plan actions and investments to improve their cybersecurity capabilities. Section 5, “Using the Model,” in the model outlines the iterative process of setting a target profile, identifying gaps between current and target profiles, implementing improvements, and re-evaluating. Appendix D, [Setting Targets](#), also provides further guidance on setting a target profile.

Identifying improvements begins with a gap analysis between the organization’s current state and target state. Consider reviewing notes captured during the self-evaluation workshop to support gap analysis and action planning. Notes often contain details and suggestions from workshop participants that may inform follow-up actions.

After the gap analysis is complete, the organizer can prioritize potential actions to address gaps. Several factors affect prioritization, including organizational objectives, budget, cost-benefit, risk to the organization, the organization’s critical infrastructure role, compliance obligations, and the availability of people and tools to implement practices.

Next, the organizer, sponsor, and other key participants may develop a plan to address the selected gaps. These plans can address short- and long-term actions, depending on the organization’s strategic planning horizon and the level of effort needed to close the selected gaps. Planning should follow standard organizational planning and budgetary processes. Typically, a key organizational leader, such as the sponsor or organizer, would own the plan, track progress, clear obstacles, and identify necessary course corrections as implementation progresses.




A checklist of specific follow-up tasks is included in Appendix A.






APPENDIX A: SELF-EVALUATION CHECKLIST


Some tasks in the checklist apply only to in-person self-evaluation workshops, and others apply only to virtual workshops. Icons indicate the type of workshop for specific tasks. Tasks with both icons apply to both workshop types.

 In-person workshop

 Virtual workshop











Time periods for tasks are included as recommendations and should be adjusted as needed.

Type	Task	Role
Four Weeks Prior to Self-Evaluation Workshop		
<input type="checkbox"/>	 Obtain the latest version of C2M2 documentation and facilitation materials	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Refresh familiarity with C2M2 and all self-evaluation materials	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Refresh familiarity with key roles in the C2M2 self-evaluation process	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Hold preparation meeting	<ul style="list-style-type: none"> Organizer Facilitator Sponsor Other Participants, as needed
<input type="checkbox"/>	 Determine the organizational scope of the self-evaluation	<ul style="list-style-type: none"> Organizer Facilitator Sponsor Other Participants, as needed
<input type="checkbox"/>	 Identify participants and support personnel	<ul style="list-style-type: none"> Organizer Facilitator Sponsor

Type	Task	Role
Four Weeks Prior to Self-Evaluation Workshop (continued)		
<input type="checkbox"/>	 Identify workshop dates based on the availability of the facilitator, sponsor, participants, and meeting space (if applicable)	<ul style="list-style-type: none"> • Organizer
<input type="checkbox"/>	 Communicate to participants the importance of the self-evaluation and their active participation	<ul style="list-style-type: none"> • Sponsor
<input type="checkbox"/>	 Send invitations and agenda to participants and ask for confirmation	<ul style="list-style-type: none"> • Organizer
<input type="checkbox"/>	 Send preparatory reading material to participants	<ul style="list-style-type: none"> • Organizer
<input type="checkbox"/>	 Identify and reserve appropriate meeting space for the workshop	<ul style="list-style-type: none"> • Organizer
<input type="checkbox"/>	 Make travel arrangements, if necessary	<ul style="list-style-type: none"> • Facilitator • Support Staff
<input type="checkbox"/>	 Establish non-disclosure agreements (NDAs), if necessary (e.g., if some of the participants are not members of the organization)	<ul style="list-style-type: none"> • Organizer • Support Staff
Two Weeks Prior to Self-Evaluation Workshop		
<input type="checkbox"/>	 Ensure there are sufficient confirmed participants to conduct the self-evaluation	<ul style="list-style-type: none"> • Organizer
<input type="checkbox"/>	 Communicate IT system requirements for the chosen Self-Evaluation tool (e.g., type and quantity of computing hardware and software applications) to the IT support staff. (See the C2M2 Self-Evaluation Tool User Guide for the chosen tool.)	<ul style="list-style-type: none"> • Organizer • Facilitator
<input type="checkbox"/>	 Determine and obtain audiovisual and other requirements for the meeting space (e.g., type and quantity of computer projectors; audio equipment; dry-erase boards and markers; easels, easel pads, and markers)	<ul style="list-style-type: none"> • Facilitator • Support Staff
<input type="checkbox"/>	 Prepare the self-evaluation workshop kickoff presentation	<ul style="list-style-type: none"> • Facilitator

Type	Task	Role
Two Weeks Prior to Self-Evaluation Workshop (continued)		
<input type="checkbox"/>	 Determine and obtain materials needed for the participants (e.g., copies of the C2M2)	<ul style="list-style-type: none"> Facilitator Support Staff
<input type="checkbox"/>	 Arrange for someone to be the scribe and take notes	<ul style="list-style-type: none"> Organizer
<input type="checkbox"/>	 Arrange for catering if desired	<ul style="list-style-type: none"> Support Staff
<input type="checkbox"/>	 Arrange for building access for those visiting	<ul style="list-style-type: none"> Organizer
One Week Prior to Self-Evaluation Workshop		
<input type="checkbox"/>	 Test all the hardware and software that will be used for the self-evaluation	<ul style="list-style-type: none"> Facilitator
The Day Before Self-Evaluation Workshop		
<input type="checkbox"/>	 Ensure that sufficient seating is available for all expected survey workshop participants and any observers	<ul style="list-style-type: none"> Support Staff
<input type="checkbox"/>	 Ensure that the room is set up to facilitate dialogue among participants	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Ensure that projection equipment is working	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Ensure that the screen is visible to the participants	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Ensure that lighting in the room can be dimmed so that projected information is readable	<ul style="list-style-type: none"> Support Staff
<input type="checkbox"/>	 Ensure that flip chart paper or white boards and markers are available	<ul style="list-style-type: none"> Support Staff
<input type="checkbox"/>	 Confirm catering, if needed	<ul style="list-style-type: none"> Support Staff
<input type="checkbox"/>	 Validate the chosen Self-Evaluation tool is operating as intended on the designated computers	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>	 Ensure that all materials have been distributed	<ul style="list-style-type: none"> Facilitator

Type	Task	Role
The Day of Self-Evaluation Workshop		
<input type="checkbox"/>	 At least 30 minutes prior to the start of the workshop, ensure that the meeting room is set up correctly	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Open the C2M2 Self-Evaluation Tool or other tool and be ready for recording responses	<ul style="list-style-type: none"> • Facilitator • Support Staff
<input type="checkbox"/>	 Ensure that any other required technology is present and functioning	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	  Review agenda and timing	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Identify backup presenters and the order in which they will assume responsibility, in the event that an issue affects the primary presenter	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Review workshop responsibilities of each role	<ul style="list-style-type: none"> • Facilitator • Presenters • Support Staff
<input type="checkbox"/>	 Open the C2M2 Self-Evaluation Tool or other tool, and be ready to record responses	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Double-check roles assigned by the virtual platform (e.g., host, presenter, etc.) to ensure that they are assigned to the correct individuals	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Distribute hard copies of presentation materials	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Check sharing configuration settings within the virtual platform, such as the ability of audience to share audio, typed comments, or images with other audience members	<ul style="list-style-type: none"> • Facilitator
<input type="checkbox"/>	 Perform an audio, video, and screen-sharing check for all presenters	<ul style="list-style-type: none"> • Facilitator • Presenters
<input type="checkbox"/>	 Review transitions between speakers and handoffs between presenters	<ul style="list-style-type: none"> • Facilitator • Other Speakers (e.g., the sponsor) • Presenters
<input type="checkbox"/>	 Review plan for introducing poll questions and presenting results	<ul style="list-style-type: none"> • Facilitator

Type	Task	Role
The Day of Self-Evaluation Workshop (continued)		
<input type="checkbox"/> 	Log in to appropriate systems to be displayed during the presentation	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/> 	Consider incorporating a five-minute break just prior to the start time of the workshop session	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/> 	After completion of the workshop, collect all printed sensitive material	<ul style="list-style-type: none"> Facilitator and/or Sponsor
<input type="checkbox"/> 	After completion of the workshop, copy the necessary files to a secure location, create file backups, and delete all workshop files from shared meeting room computers, if applicable	<ul style="list-style-type: none"> Facilitator
Within One Week After Self-Evaluation Workshop		
<input type="checkbox"/>  	Organize the reports generated by the self-evaluation tool and all other relevant notes and materials	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>  	Deliver the final package of materials to the sponsor	<ul style="list-style-type: none"> Facilitator
<input type="checkbox"/>  	Plan follow-up activities	<ul style="list-style-type: none"> Organizer Facilitator Sponsor

APPENDIX B: COMMON DISCUSSIONS

Experiences using the model and facilitating C2M2 self-evaluations have revealed many topics that commonly surface during workshop discussions. The facilitator should prepare for these discussions in advance. Facilitator guidance for these common discussion topics is documented below.

- **Distinction between *Largely Implemented* and *Partially Implemented***

Participants may begin with different interpretations of these responses. The facilitator must provide a way for the group to come to consensus on a definition of these responses early on, so that the responses have a consistent meaning throughout the evaluation. A useful technique is to ask, “How many actions do we need to take before we can consider this practice Fully Implemented?” If participants name more than one action, the practice may be considered Partially Implemented or Largely Implemented, depending on the number of actions required to be Fully Implemented. If only one action is required, or the group views the actions described as minor, consider the practice Largely Implemented. The scribe should record the discussions, rationale, and actions proposed in the notes. This information can be useful to the organization when reviewing the Self-Evaluation Report and planning follow-up actions.

- **Responses to practices with compound statements**

If some but not all activities in a practice are implemented, the response should reflect the level of implementation (i.e., it should not be considered Fully Implemented). For example, ARCHITECTURE-1b states “A strategy for cybersecurity architecture is established and maintained in alignment with the organization’s cybersecurity program strategy (PROGRAM-1b) and enterprise architecture.” If the strategy exists but is not routinely updated, Largely Implemented should be considered instead of Fully Implemented.

- **Questions about C2M2 terminology**

Be prepared to clarify key phrases in the practices, such as “at least in an ad hoc manner” and “is established and maintained.” Use the glossary to help answer specific questions about terms. Use the help text to help answer specific questions about practices.

- **Meaning of *at least in an ad hoc manner***

When reading MIL1 practices in the C2M2, you will encounter the phrase “at least in an ad hoc manner.” This should be covered with participants in the beginning of the workshop, and you are likely to be asked what this phrase means. Prepare by reading

the explanation of “ad hoc” in Section 4.3, “Approach Progression” and the “ad hoc” item in the glossary of the model and have that content handy for this discussion.

- **Addressing in-progress or planned projects**

Responses should reflect the current state of the organization. Consider documenting in-progress or planned projects in the notes field. Consider updating your self-evaluation when in-progress or planned projects are complete or at a set period, such as every six months.

- **Cybersecurity Architecture domain**

The Cybersecurity Architecture domain was added to the C2M2 in Version 2.0. Some participants may need assistance in understanding the purpose of the domain and how it relates to other domains. Prepare by reading Section 4.6, “Considerations for the Cybersecurity Architecture Domain,” in the model.

Also, as you lead participants through the practices in this domain, it might be useful to emphasize the “as an element of the cybersecurity architecture” aspect of each objective name and remind them that all the practices should be understood in that context. The cybersecurity architecture is a framework that “guides the selection of tools, techniques, methods, and controls to meet the organization’s cybersecurity objectives” (as stated in Section 4.6 in the model); implementation of the architecture is realized through the practices in other domains, such as ACCESS. This reminder may be needed to help participants understand that there is no redundancy between the Cybersecurity Architecture domain and other domains in the model.

- **Review of “Management Activities” objectives**

The last objective in each domain is “Management Activities.” These practices help the organization determine the degree to which the other practices in the domain have been institutionalized—that is, the extent to which the practices are established in the organization’s operations. The more established an activity, the more likely it is that the organization will continue to perform the activity over time.

When discussing the Management Activities practices in one domain, it is important to remind participants that their responses to these should consider all practices in that domain. For example, when evaluating Management Activities in the Asset, Change, and Configuration domain, participants consider whether the Management Activities practices are implemented for asset inventory, change management, and configuration management. You may need to remind participants to consider the entire domain each time you reach the Management Activities. If participants appear to be arriving at their responses too quickly, it may be worth rephrasing or contextualizing these practices.

- **MILs and the dual progression of the model**

The model describes dual progression in Section 4.3, “Approach Progression,” and Section 4.4, “Management Progression.” In each domain, practices within the Approach objectives (the objectives that precede the Management Activities objective), refer to the completeness, thoroughness, or level of development of an activity. As an organization progresses from one MIL to the next, it will have more complete or more advanced implementations of the core activities in the domain. Management Activities practices refer to the degree to which the other practices in the domain have been institutionalized—that is, the extent to which the practices are established and are routine in the organization’s operations. The progression within the Approach objectives and the progression within the Management Activities objective together constitute a dual progression of maturity within the model. You may need to explain dual progression to the participants as you facilitate the self-evaluation.

- **Examples**

Many practices in C2M2 contain lists of examples preceded by either “such as” or “for example.” Self-evaluation participants may need to be reminded that the purpose of these examples is only to better communicate the intended meaning of the practices. They should not be interpreted as specifying exactly what must be done to correctly implement the practice. See Section 4.7, “Examples Lists Included in Practices,” in the model for further explanation.

APPENDIX C: RELATED PRACTICES

This appendix reviews the four types of related practices in the C2M2:

- Practices with dependencies
- Input-from relationships
- Practice progressions
- Information-sharing practices

Practices with Dependencies

There are several practices that, depending on how they are scored, inform the logical response for certain other practices. Practices that contain dependencies reference the related practice in parentheses within the text of the practice. For example, THREAT-2j is dependent upon SITUATION-3g. THREAT-2j states “Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g).” If SITUATION-3g is scored as Not Implemented (i.e., the organization has not identified predefined states of operation), then THREAT-2j should not be scored as Largely Implemented or Fully Implemented.

The facilitator should point out practices that contain dependencies, review the referenced practice and its response, and discuss the implications of that response on the current practice. You may encounter practices that are dependent on practices that have not yet been discussed. When this occurs, the facilitator should guide participants to first respond to the referenced practice, and then respond to the practice that contains the dependency.

Table 5 includes a complete list of the practices that contain a dependency (left column), along with the practices that they are dependent upon and the object of the dependency (right column).

Table 5: Practices with Dependencies

Practices with Dependencies	Practice and Object of the Dependency
ASSET-3c	ARCHITECTURE-1f (cybersecurity requirements)
ARCHITECTURE-1b, RISK-1b	PROGRAM-1b (cybersecurity program strategy)
RESPONSE-2h	RISK-3b (cyber risk prioritization criteria)
ARCHITECTURE-1j	RISK-3d (risk analysis information)

Practices with Dependencies	Practice and Object of the Dependency
RESPONSE-2g	SITUATION-3d (situational awareness reporting requirements)
ARCHITECTURE-1k, RESPONSE-3i, THREAT-2j, WORKFORCE-2f	SITUATION-3g (predefined states of operation)
ARCHITECTURE-1j, PROGRAM-1h, RESPONSE-1e, RESPONSE-4m, SITUATION-2f, WORKFORCE-2c	THREAT-2e (threat profile)

Input-From Relationships

Many practices in the model have input-to or input-from relationships that are similar to but not as strong as dependencies. These are shown in the help text within the self-evaluation tools. For example, a number of practices refer to “higher priority assets.” The help text for those practices shows an input-from relationship with ASSET-1c, “Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function.”

Note that if the input-from practice is in a practice progression (see Practice Progression in this appendix), other practices in its progression might also be included in the input-from relationship. Table 6 contains a list of all practices with input-from relationships.

Table 6: Input-From Relationships

Practice	Has Input From
ACCESS-2	ARCHITECTURE-3a
ACCESS-3	ARCHITECTURE-3a
ACCESS-4c	PROGRAM-2d
ARCHITECTURE-1c	ASSET-1a, ASSET-2a, ASSET-1c, ASSET-2c
ARCHITECTURE-1g	ARCHITECTURE-1f
ARCHITECTURE-1i	ARCHITECTURE-1c
ARCHITECTURE-2c	ASSET-1c, ASSET-1d
ARCHITECTURE-2d	ASSET-1a, ASSET-2a
ARCHITECTURE-2h	ASSET-1f, ARCHITECTURE-1f
ARCHITECTURE-3a	ASSET-1a, ASSET-2a
ARCHITECTURE-3b	ASSET-1a
ARCHITECTURE-3h	ASSET-1f, ASSET-2f
ARCHITECTURE-3k	ASSET-1c
ARCHITECTURE-4a	ASSET-1c

Practice	Has Input From
ARCHITECTURE-4b	ASSET-1c
ARCHITECTURE-5b	ASSET-2c
ARCHITECTURE-5c	ASSET-2c
ARCHITECTURE-5d	ASSET-2c
ARCHITECTURE-6c	PROGRAM-2d
ASSET-1c	ASSET-1a
ASSET-1d	ASSET-1b
ASSET-1e	ASSET-1a, ASSET-1b
ASSET-2c	ASSET-2a
ASSET-2e	ASSET-2a
ASSET-3c	ARCHITECTURE-3f
ASSET-4d	ASSET-1c
ASSET-4f	ASSET-1a, ASSET-2a
ASSET-4h	ASSET-1c
ASSET-4i	ARCHITECTURE-1f
ASSET-5c	PROGRAM-2d
PROGRAM-2b	PROGRAM-1b
PROGRAM-2e	PROGRAM-2b
PROGRAM-2g	PROGRAM-1b
PROGRAM-2h	ASSET-5a, ASSET-5c
PROGRAM-2h	THREAT-3a, THREAT-3c
PROGRAM-2h	RISK-5a, RISK-5c
PROGRAM-2h	ACCESS-4a, ACCESS-4c
PROGRAM-2h	SITUATION-4a, SITUATION-4c
PROGRAM-2h	RESPONSE-5a, RESPONSE-5c
PROGRAM-2h	THIRD-PARTIES-3a, THIRD-PARTIES-3c
PROGRAM-2h	WORKFORCE-5a, WORKFORCE-5c
PROGRAM-2h	ARCHITECTURE-6a, ARCHITECTURE-6c
RESPONSE-1e	RISK-2a
RESPONSE-1f	SITUATION-3d, SITUATION-3f
RESPONSE-2b	RESPONSE-1a
RESPONSE-2d	RESPONSE-2c
RESPONSE-3d	RESPONSE-4a, RESPONSE-4h

Practice	Has Input From
RESPONSE-3g	RESPONSE-4i
RESPONSE-4a	ARCHITECTURE-2j
RESPONSE-4d	RISK-3c
RESPONSE-4f	ASSET-1a, ASSET-2a
RESPONSE-4g	ASSET-1a, ASSET-2a
RESPONSE-4j	ARCHITECTURE-1g
RESPONSE-4m	RISK-2a
RESPONSE-4n	RISK-3a
RESPONSE-4o	RESPONSE-4g
RESPONSE-5c	PROGRAM-2d
RISK-2b	THIRD-PARTIES-1c
RISK-2h	ASSET-1e
RISK-2i	THREAT-1i
RISK-2j	THREAT-2h
RISK-2k	THIRD-PARTIES-1c
RISK-2l	ARCHITECTURE-1i
RISK-3c	RISK-3a
RISK-3d	RISK-3a
RISK-3e	RISK-3a
RISK-4c	ARCHITECTURE-1g
RISK-5c	PROGRAM-2d
SITUATION-1a	ASSET-1a
SITUATION-1c	ASSET-1a, ASSET-1b
SITUATION-1f	ASSET-1c
SITUATION-2g	ASSET-1c
SITUATION-3b	SITUATION-2a, SITUATION-2b
SITUATION-3g	THREAT-2j, RESPONSE-3i
SITUATION-4c	PROGRAM-2d
THIRD-PARTIES-1b	ASSET-1a, ASSET-2a
THIRD-PARTIES-2c	ARCHITECTURE-1f, ARCHITECTURE-1g
THIRD-PARTIES-2e	THIRD-PARTIES-1d
THIRD-PARTIES-2k	ASSET-1c
THIRD-PARTIES-2l	ASSET-1c

Practice	Has Input From
THIRD-PARTIES-3c	PROGRAM-2d
THREAT-1b	THREAT-1a
THREAT-1d	THREAT-1c
THREAT-1e	ASSET-1c
THREAT-2b	THREAT-2a
THREAT-2c	THREAT-2b
THREAT-2d	THREAT-2c
THREAT-2f	THREAT-2e
THREAT-3c	PROGRAM-2d
WORKFORCE-1c	ASSET-1a, ASSET-2a
WORKFORCE-4a	WORKFORCE-3b
WORKFORCE-4c	WORKFORCE-4b
WORKFORCE-4d	ASSET-1a, ASSET-2a
WORKFORCE-4f	WORKFORCE-3c
WORKFORCE-5c	PROGRAM-2d

Practice Progressions

Practice progressions are groups of related practices that represent increasingly complete, comprehensive, or advanced implementations of an activity. For example, in ASSET objective 1, there are two sets of practice progressions: 1) ASSET-1a, ASSET-1b, ASSET-1f, and ASSET-1g, which has to do with the IT and OT asset inventory being created and matured; and 2) ASSET-1c and ASSET-1d, which has to do with prioritization of inventoried assets based on defined criteria.

Practice progressions usually exist within an objective, but may also cross objectives within a domain. For example, RESPONSE-1a and RESPONSE-2f form a progression regarding documentation of cyber events and incidents.

Note that while some practice progressions may represent steps in a process (do this and then do that, etc.), their primary importance is in showing progress in practice maturity—doing an activity in an increasingly complete, comprehensive, or advanced way. They can therefore be useful in planning target profiles or cyber program growth over time.

Table 7: Practice Progressions

Progression	Subject of Progression
ASSET-1a, ASSET-1b, ASSET-1f, ASSET-1g	IT and OT asset inventory
ASSET-1c, ASSET-1d	Prioritization of inventoried assets
ASSET-2a, ASSET-2b, ASSET-2f, ASSET-2g	Information asset inventory
ASSET-2c, ASSET-2d	Categorization of inventoried assets
ASSET-3a, ASSET-3c, ASSET-3d	Creating and maintaining configuration baselines
ASSET-3b, ASSET-3e	Using configuration baselines
ASSET-4a, ASSET-4d, ASSET-4e, ASSET-4f, ASSET-4h	Making changes to assets in a secure manner
ASSET-4b, ASSET-4c, ASSET-4i	Documentation of changes to assets
THREAT-1a, THREAT-1e, THREAT-1j	Cybersecurity vulnerability information sources
THREAT-1b, THREAT-1i, THREAT-1m	Obtaining and sharing cybersecurity vulnerability information
THREAT-1c, THREAT-1f, THREAT-1k	Performing cybersecurity vulnerability assessments
THREAT-1d, THREAT-1g, THREAT-1l	Mitigating cybersecurity vulnerabilities
THREAT-2a, THREAT-2f	Threat information sources
THREAT-2b, THREAT-2h, THREAT-2k	Obtaining and sharing threat information
THREAT-2c, THREAT-2e, THREAT-2i	Threat objectives and threat profiles
THREAT-2d, THREAT-2g, THREAT-2j	Responding to threats
RISK-1a, RISK-1b, RISK-1c, RISK-1g, RISK-1h	Establishing cyber risk management strategy and program
RISK-1e, RISK-1f	Establishing governance and sponsorship for the cyber risk management program
RISK-2a, RISK-2b, RISK-2c, RISK-2g, RISK-2h, RISK-2i, RISK-2j, RISK-2k, RISK-2l, RISK-2m	Identifying cyber risks
RISK-2d, RISK-2e, RISK-2f, RISK-2i, RISK-2j, RISK-2k, RISK-2l, RISK-3f	Organizing and describing cyber risks
RISK-3a, RISK-3b	Prioritizing cyber risks
RISK-3b, RISK-3c, RISK-4c, RISK-4d	Mitigating the impact of cyber risks
RISK-3c, RISK-3d, RISK-3e	Analyzing cyber risks
RISK-4a, RISK-4b, RISK-4e	Risk responses
ACCESS-1a, ACCESS-1c, ACCESS-1e, ACCESS-1f, ACCESS-1j	Establishing identities
ACCESS-1b, ACCESS-1d, ACCESS-1g, ACCESS-1h, ACCESS-1i	Managing authentication
ACCESS-2a, ACCESS-2c, ACCESS-2d, ACCESS-2e, ACCESS-2f	Logical access controls and requirements

Progression	Subject of Progression
ACCESS-2b, ACCESS-2g, ACCESS-2h	Logical access privileges
ACCESS-3a, ACCESS-3d, ACCESS-3e, ACCESS-3f, ACCESS-3g	Physical access controls and requirements
ACCESS-3b, ACCESS-3h, ACCESS-3i	Physical access privileges
ACCESS-3c, ACCESS-3j	Monitoring physical access
SITUATION-1a, SITUATION-1b, SITUATION-1c, SITUATION-1d, SITUATION-1f	Logging and logging requirements
SITUATION-2a, SITUATION-2b, SITUATION-2c, SITUATION-2f, SITUATION-2g	Monitoring and monitoring requirements
SITUATION-2d, SITUATION-2h, SITUATION-2i	Indicators of anomalous activity
SITUATION-3b, SITUATION-3f	Aggregating and analyzing monitoring data
SITUATION-3c, SITUATION-3e, SITUATION-3f	Collecting information for situational awareness
RESPONSE-1a, RESPONSE-1b, RESPONSE-1c, RESPONSE-1f	Detecting and documenting cybersecurity events
RESPONSE-2a, RESPONSE-2c, RESPONSE-2e, RESPONSE-2h	Cybersecurity incident declaration criteria
RESPONSE-2b, RESPONSE-2d, RESPONSE-2f, RESPONSE-2i	Analyzing cybersecurity events and incidents
RESPONSE-1a, RESPONSE-2f	Documentation of cyber events and incidents
RESPONSE-3a, RESPONSE-3d, RESPONSE-3f, RESPONSE-3g, RESPONSE-3h, RESPONSE-3i	Cybersecurity incident response plans
RESPONSE-3b, RESPONSE-3e, RESPONSE-3h, RESPONSE-3i, RESPONSE-3i	Responses to cybersecurity incidents
RESPONSE-3g, RESPONSE-3k	Cybersecurity incident response exercises
RESPONSE-4a, RESPONSE-4d, RESPONSE-4e, RESPONSE-4f, RESPONSE-4g, RESPONSE-4m, RESPONSE-4p	Continuity plans
RESPONSE-4b, RESPONSE-4f, RESPONSE-4j, RESPONSE-4k	Data backups
RESPONSE-4c, RESPONSE-4f, RESPONSE-4i	Spares for selected IT and OT assets
RESPONSE-4i, RESPONSE-4n	Continuity plans tests and exercises
THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-1c, THIRD-PARTIES-1d, THIRD-PARTIES-1e, THIRD-PARTIES-1f	Identifying and prioritizing third parties and cyber risks arising from third parties
THIRD-PARTIES-2a, THIRD-PARTIES-2d	Considering cybersecurity and cyber risks in selection of third parties
THIRD-PARTIES-2b, THIRD-PARTIES-2i, THIRD-PARTIES-2j, THIRD-PARTIES-2k, THIRD-PARTIES-2l, THIRD-PARTIES-2m	Considering cybersecurity and cyber risks in selection of products and services

Progression	Subject of Progression
THIRD-PARTIES-2c, THIRD-PARTIES-2e	Mitigating cyber risks arising from third parties
THIRD-PARTIES-2c, THIRD-PARTIES-2f, THIRD-PARTIES-2g, THIRD-PARTIES-2h	Cybersecurity requirements for third parties
WORKFORCE-1a, WORKFORCE-1c, WORKFORCE-1f	Personnel vetting
WORKFORCE-1b, WORKFORCE-1d	Addressing cybersecurity in personnel separation and transfer procedures
WORKFORCE-1e, WORKFORCE-1g	Acceptable use and other general cybersecurity responsibilities
WORKFORCE-2a, WORKFORCE-2b, WORKFORCE-2c, WORKFORCE-2d, WORKFORCE-2e, WORKFORCE-2f, WORKFORCE-2g	Cybersecurity awareness activities
WORKFORCE-3a, WORKFORCE-3d, WORKFORCE-3e	Identifying and documenting cybersecurity responsibilities
WORKFORCE-3b, WORKFORCE-3c, WORKFORCE-3f	Assigning cybersecurity responsibilities
WORKFORCE-4a, WORKFORCE-4d, WORKFORCE-4f	Cybersecurity training
ARCHITECTURE-1a, ARCHITECTURE-1b, ARCHITECTURE-1h	Cybersecurity architecture strategy
ARCHITECTURE-1c, ARCHITECTURE-1f, ARCHITECTURE-1j, ARCHITECTURE-1k	The cybersecurity architecture
ARCHITECTURE-1d, ARCHITECTURE-1e	Establishing governance and sponsorship for the cybersecurity architecture
ARCHITECTURE-2b, ARCHITECTURE-2d, ARCHITECTURE-2h, ARCHITECTURE-2i, ARCHITECTURE-2j, ARCHITECTURE-2l	Asset segmentation
ARCHITECTURE-2a, ARCHITECTURE-2c, ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-2k	Network protections
ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3h, ARCHITECTURE-3k	IT and OT asset security
ARCHITECTURE-3e, ARCHITECTURE-3f, ARCHITECTURE-3l	Asset configuration security
ARCHITECTURE-4a, ARCHITECTURE-4d, ARCHITECTURE-4f, ARCHITECTURE-4h, ARCHITECTURE-5h	Secure software development use in-house
ARCHITECTURE-4b, ARCHITECTURE-4e, ARCHITECTURE-4g, ARCHITECTURE-4h, ARCHITECTURE-5h	Secure software development use by vendors
ARCHITECTURE-5a, ARCHITECTURE-5b, ARCHITECTURE-5c, ARCHITECTURE-5d, ARCHITECTURE-5e, ARCHITECTURE-5f, ARCHITECTURE-5g, ARCHITECTURE-5h	Data security

Progression	Subject of Progression
PROGRAM-1a, PROGRAM-1b, PROGRAM-1c, PROGRAM-1d, PROGRAM-1e, PROGRAM-1f, PROGRAM-1g, PROGRAM-1h	The cybersecurity program strategy
PROGRAM-2b, PROGRAM-2g, PROGRAM-2h, PROGRAM-2i	The cybersecurity program
PROGRAM-2a, PROGRAM-2c, PROGRAM-2d	Senior management support and sponsorship for the cybersecurity program
PROGRAM-2f, PROGRAM-2j	Collaboration with internal and external stakeholders in cybersecurity program management

Information-Sharing Practices

This is a group of cross-domain practices, shown in Table 8, that enable information sharing with organizational stakeholders. Some of the practices in this group were formerly in the prior Information Sharing and Communications domain in C2M2 Version 1.0 and Version 1.1.

Table 8: Information-Sharing Practices

Practice ID	Practice Text
RESPONSE-2g	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)
RESPONSE-3c	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner
RESPONSE-3f	Cybersecurity incident response plans include a communications plan for internal and external stakeholders
RISK-1d	Information from RISK domain activities is communicated to relevant stakeholders
SITUATION-3a	Methods of communicating the current state of cybersecurity for the function are established and maintained
SITUATION-3c	Relevant information from across the organization is available to enhance situational awareness
SITUATION-3d	Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders
SITUATION-3e	Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness
THREAT-1i	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders
THREAT-2h	Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs])
THREAT-2k	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action

APPENDIX D: SETTING TARGETS

Either before or after conducting a self-evaluation, the organization should determine the level of practice performance and MIL achievement for each domain that best enables it to meet its business objectives and cybersecurity strategy. This collection of performance targets is the organization's target profile. There are two common approaches for identifying a target profile. The first approach, which involves using the results of the C2M2 self-evaluation to identify the target profile, is often adopted by organizations that are new to the C2M2 and have not previously established a target profile. The second approach, which involves setting targets before performing an evaluation, is often adopted by organizations that have previous experience with the model.

Performance targets help organizations establish organizational goals for their cybersecurity program and capabilities, relative to their unique operating environment and threat exposure. They are fundamental to helping organizations make effective use of their C2M2 self-evaluation results to identify improvements. Once the target profile is set, the organization can use the Self-Evaluation Report to compare the organization's current state against its target profile and identify gaps. The report documents the current state, including summary charts showing MIL achievement by domain and detailed tables showing the responses for each practice. The report also contains a list of Partially Implemented or Not Implemented practices, which may be useful in conducting a gap analysis.

The self-evaluation workshop may include a target-setting session, led by the facilitator, with similar participants to the self-evaluation sessions. A variety of valuable opinions and expertise will be provided by C2M2 self-evaluation participants in the target-setting discussion, and facilitators should capture this input to support gap analysis.

When setting targets, organizations should consider the following: establishing the right target, setting time boundaries, establishing a continuous process, prioritizing cybersecurity risk, addressing resource constraints, and investing in institutionalization of capabilities.

Establish the Right Targets

Some C2M2 users may focus on setting targets at the domain level, while others may focus on setting targets at the practice level. Focusing solely on domain level targets may overlook practice-level improvements that, over time, can help the organization expand its capabilities. Either approach is legitimate; the organization should consider both and choose the one that works best for achieving overall cybersecurity program improvement goals. Facilitators will need to astutely understand the organization's motivation for embarking on a C2M2 self-evaluation to guide their decisions about which is the right approach. Organizations may also consider using a combination of both approaches. Consider the following factors for each approach:

- **Domain-level target setting**

Organizations that focus target-setting at the domain level should have process institutionalization or “maturity” as their main focus. This is best for organizations that have demonstrated high levels of performance at the practice level and desire to ensure their performance is sustainable as the organization changes, grows, or adapts to changing cybersecurity events, threats, and incidents.

Setting targets at the domain level involves establishing a maturity indicator level (MIL) target for each domain that is commensurate with the desired and necessary level of maturity to sustain performance and manage risk. Note that organizations often overshoot this target, believing that they must achieve the highest MIL levels in all domains to be effective. This may not be optimal and could increase cybersecurity program costs relative to performance.

- **Practice-level target setting**

Setting practice-level performance targets is often the appropriate approach for organizations that want to improve their overall cybersecurity capabilities. Setting targets at the practice level involves establishing a target implementation level (e.g., Fully Implemented or Largely Implemented) for each practice in a domain.

In this approach, the organization focuses on identifying more granular targets that reflect the organization’s business, operational, and risk considerations. For example, largely implementing rather than fully implementing a practice might provide the desired level of capability at a lower resource cost, including the overall cost of managing and maintaining the practice. And, in some cases, it may be perfectly reasonable for an organization to consider partially or not implementing a particular practice if it does not ultimately provide value to their cybersecurity program.

Set Time Boundaries

The facilitator should encourage participants to establish time boundaries on all targets to ensure realistic consideration of organizational priorities that could affect or impede process improvement. Many key factors may affect the time boundaries for goal achievement, including organizational imperatives and business objectives, regulatory and compliance requirements, resource availability, or impending merger and acquisition activity. Anything that affects the time horizon for organizational projects needs to be considered in setting time boundaries for C2M2 performance improvement goals.

Establish a Continuous Process

Organizational change is a given, so setting and maintaining performance targets should be approached as a continuous process, not a discrete activity that only occurs as part of one C2M2 self-evaluation. Facilitators will need to guide organizations to establish the appropriate time intervals to review and consider changes to targets. Rather than definitive

time frames (such as “every six months”), this could involve establishing criteria or events that would trigger opportunities to revisit targets and make adjustments.

Cybersecurity Risk

Organizations can use their risk exposure and risk tolerance to guide and prioritize target-setting. Based on what is known about the organization’s cybersecurity risk exposure, risk tolerance, and risk prioritization, the domains or practices can be prioritized for target setting. Domains or practices that most impact the organization’s risk profile may be given higher priority when setting performance targets.

Resource Constraints

The balance between resource availability and cybersecurity risk reduction is an important constraint when setting realistic targets. The facilitator should guide participants to consider how the allocation of finite human and financial resources affects their ability to improve capabilities across the C2M2 domains.

For example, participants may decide during this exercise that gaps in THIRD-PARTIES capabilities would require higher levels of investment, and therefore consider lowering the performance target for other domains.

Investing in Institutionalization of Capabilities

MIL achievement is dependent on institutionalization. In C2M2, practice institutionalization—or the degree to which capabilities can be retained in times of stress and established as part of the organization’s cybersecurity culture—is achieved through the accomplishment of the domain’s Management Activities. This means that for each domain with a performance target higher than MIL1, additional institutionalizing features must be implemented, such as documenting procedures, assigning adequate resources, establishing policies or directives, assigning responsibility and accountability, demonstrating sufficient knowledge of the domain, and measuring and adjusting performance on a regular basis. Through these activities may increase cost above and beyond achieving the practices in the Approach objectives, they carry significant benefits. Discussions about capability maturity are encouraged as early in the self-evaluation process as possible, and particularly when setting performance targets.

APPENDIX E: SCORING GUIDANCE FOR MULTIPLE ORGANIZATIONAL FUNCTIONS

A large, complex, or geographically distributed organization will likely have many functions that are important to its mission, goals, and objectives, and therefore may perform more than one self-evaluation, sometimes simultaneously. Organizations often conduct more than one self-evaluation for different functions that have different risk profiles, governance structures, or board membership. For example, consider a large natural gas organization that operates distinct lines of business: a production division that produces natural gas, a midstream division that operates pipelines, and a distribution division that delivers natural gas to consumers. Each of these lines of business may have different IT and OT infrastructures, risk tolerances, operating regions, and compliance regulations.

When performing multiple self-evaluations, an organization may want to understand how it is performing overall relative to cybersecurity objectives. The organization will need to choose a method for aggregating organization-level scores for multiple assessments.

Organizations may develop an organizational-level score using several methods, such as: low watermark (selecting the lowest MIL achieved in each domain across functions), simple average, and weighted-average (assigning weight based on the importance of each function). In some cases, it may not be advisable to develop an organization-level score, especially if such aggregation would provide an inaccurate or misleading characterization of cybersecurity capabilities. In these cases, the range of self-evaluation scores may be more informative for understanding the state of the organization's cybersecurity program, especially if there are significant differences in scores between divisions or lines of business.