CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) FACILITATOR GUIDE

Version 1.1a
February 2017

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The Department of Energy (DOE) acknowledges the dedication and technical expertise of the organizations and individuals who have provided the critiques, evaluations, and modifications to enable the development of this first release of the C2M2 Facilitator Guide.

DOE C2M2 Technical Lead

Jason D. Christopher
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

DOE C2M2 Program Team

Fowad Muneer, ICF International
John Fry, ICF International

Model Architect

Carnegie Mellon University Software Engineering Institute – CERT Division

1. INTRODUCTION

1.1 Purpose of This Guide

The purpose of this document is to enable organizations to conduct a self-evaluation using the Cybersecurity Capability Maturity Model (C2M2) or one of the subsector specific versions of the model (i.e. the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2). The C2M2 models and their self-evaluation survey methods can be completed in a one-day workshop. This guide

- provides information on how to obtain the appropriate survey and scoring tool and prepare for the self-evaluation
- assists the organization in evaluating its cybersecurity capabilities during the workshop
- provides guidance for follow-on activities to prioritize and implement a plan to close identified capability gaps

1.2 Intended Audience

This guide is intended for use by the individual selected by the organization to plan and facilitate a C2M2 self-evaluation. An organization may have one individual perform both planning and facilitation functions. The facilitator is accountable to a sponsor within the organization who has requested the self-evaluation.

1.3 How to Use This Guide

The facilitator should use this guide as a starting point for preparing and executing the C2M2 self-evaluation. The sections of the guide correspond to the three key phases of a typical self-evaluation: Preparation, Survey Workshop, and Follow-Up. The facilitator should read through the entire guide and the supporting documents to become familiar with the model itself as well as the end-to-end process of executing the self-evaluation. Familiarity with the materials is important because each workshop is different and may require the facilitator to move through this guide but not necessarily in the order the material is presented. There also may be some iteration of activities.

Model-specific issues or instructions will be found in boxes like this one

There is only one C2M2 Facilitator Guide for the three C2M2 models because the core material (i.e. the domains and the practices) and the self-evaluation process is the same for all of them. Throughout the rest of this guide, an individual facilitating an ES-C2M2 or ONG-C2M2 self-evaluation can simply interpret the term C2M2 as the subsector-specific version of the model that they are using. Instructions or issues specific to individual models will be identified in call-out boxes throughout the rest of this document.

1.4 Organization of This Guide

This guide is organized as shown in Figure 1. Sections 2-4 provide detailed descriptions of the three key phases of a typical self-evaluation process:

- Preparation phase (preparing for an evaluation)
- Survey Workshop phase (conducting an evaluation)
- Follow-Up Activities phase (analyzing the results and determining next steps)

A brief summary is provided in Section 1, followed by the list of references and an appendix containing a facilitator's checklist.

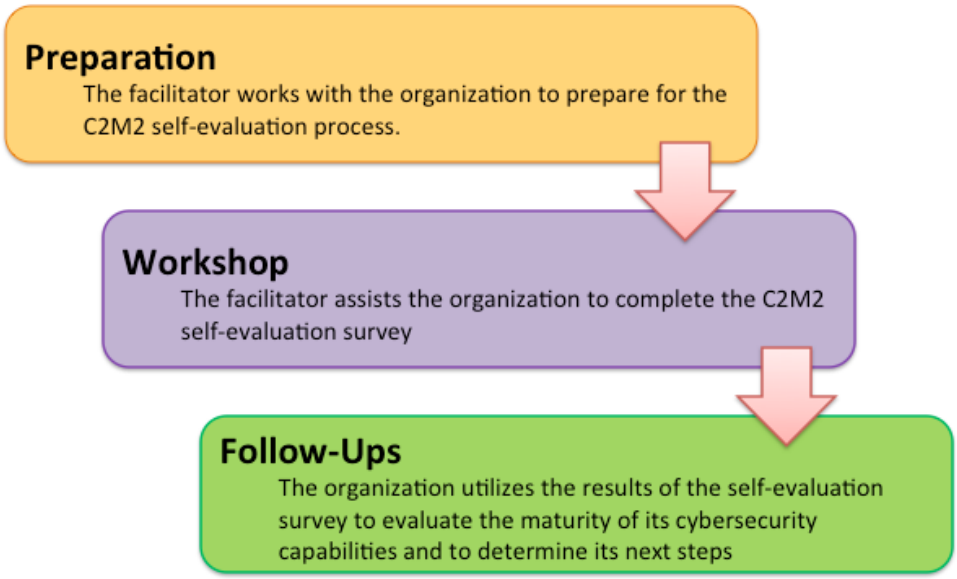

Figure 1: Typical Phases of Self-Evaluation

2. PREPARATION

This section describes the desired skills of the facilitator and the planning and preparation activities that the facilitator should execute during the first of the three phases of the self-evaluation process. The steps listed here are also captured in checklist form in Appendix A.

2.1 Key Skills for a Facilitator

A facilitator helps a group of people understand their common objectives and assists them in planning to achieve these objectives without taking a particular position in the discussion [Facilitator].

The basic skills of a facilitator consist of good meeting leadership practices: timekeeping, following an agreed-upon agenda, and keeping a clear record. The higher-order skills involve observing the group and its individuals in light of group dynamics. In addition, facilitators need a variety of listening skills, including the ability to paraphrase, stack a conversation, draw people out, balance participation, and make space for more reticent group members.

The facilitator must have the knowledge and skill to be able to intervene in a way that adds to the group's creativity rather than takes away from it. A successful facilitator embodies respect for others and a watchful awareness of the many perceptions of reality in a human group. In the event that a consensus cannot be reached, the facilitator should assist the group in understanding the differences that divide it [Facilitator].

In addition to the basic facilitation skills mentioned in Section 2.1, a facilitator for the subsector-specific models will benefit from having knowledge and domain expertise, e.g.,

- the energy sector guidance provided by the U.S. Department of Homeland Security's (DHS) critical infrastructure program, which includes the electricity, petroleum, and natural gas subsectors [DHS Energy]
- the U.S. Department of Energy Electricity Subsector Cybersecurity Risk Management Process Guideline (DOE RMP)
- the electricity portion of the energy sector, which includes the generation, transmission, distribution, and marketing of electricity
- the NERC's Critical Infrastructure Protection (CIP) Standards [NERC CIP]
- the oil and natural gas portion of the energy sector, which includes the search for, production, transportation, processing, storage and delivery of oil and natural gas products from subsurface origins to end consumers (ONG-C2M2)

2.2 Obtaining the Latest Version of C2M2 Facilitation Materials

The facilitator should have the latest version of the complete set of materials listed in Table 1. The facilitator should email DOE at the appropriate address to obtain the latest versions of all items:

- C2M2 materials: C2M2@doe.gov
- ES-C2M2 materials: ES-C2M2@doe.gov
- ONG-C2M2 materials: ONG-C2M2@doe.gov

Table 1: C2M2 Self-Evaluation Materials

Title	Brief Description	File Type
C2M2	the model itself	PDF
C2M2 Evaluation Survey Toolkit	list of questions associated with the C2M2 and tool that generates the Evaluation Scoring Report	MS Excel
C2M2 Evaluation Survey ReadMe Instructions	instructions for using the C2M2 Evaluation Survey and its scoring tool	PDF
C2M2 Domain Maturity Indicator Level (MIL) Reference Cheat Sheet	definitions of C2M2 domains, MILs, and four-point answer scale for survey questions	PDF
C2M2 Evaluation Scoring Report Template	blank template of the Evaluation Scoring Report	MS Word
Optional materials available on request:		
Introduction to the C2M2 Presentation	overview of the C2M2	MS PowerPoint
C2M2 Facilitated Self-Evaluation Presentation	presentation of background information for facilitator to give to workshop participants	MS PowerPoint

2.3 Becoming Familiar with the C2M2 and Self-Evaluation Materials

A C2M2 facilitator should be familiar with the C2M2, this guide, and the materials listed in Table 1 above. It is recommended that a new facilitator follow the steps detailed below to gain the necessary familiarity with the C2M2, the facilitation process, and the required materials:

1. Read the entire C2M2 description [C2M2] and become familiar with its
   - goals
   - objectives
   - model architecture
   - domains and domain structure
   - maturity indicator levels
   - dual progression of maturity (approach progression and institutionalization progression)
   - details of each of the 10 domains (including domain-specific practices and common practices)
   - recommended process improvement approach for using the model
2. Become familiar with the Introduction to C2M2 presentation and develop a version that the facilitator is comfortable presenting [C2M2 Intro].
3. Read this guide in its entirety. The insights provided in this document can be helpful to understanding the self-evaluation survey.

4. Review the C2M2 Domain MIL Reference Cheat Sheet [C2M2 MIL]. This can be used as reminder of the key aspects of the model during preparation for the evaluation workshop.
5. Review the C2M2 Facilitated Self-Evaluation Presentation [C2M2 Self Eval].
6. Review the C2M2 Evaluation Survey document [C2M2 Eval Survey], become familiar with its structure, ensure its fillable PDF capabilities function on the computer on which it will be viewed, and read all the questions in the survey. It is critical for the facilitator to have a good understanding of the survey questions.
7. Review the C2M2 Evaluation Survey ReadMe Instructions document [C2M2 Survey Instructions]. This ReadMe document provides technical instructions for using the C2M2 Evaluation Survey and its scoring tool.
8. Open the C2M2 Toolkit Excel file [C2M2 Toolkit] to ensure it functions on the computer being used. Follow the step-by-step instructions provided in the C2M2 Evaluation Survey ReadMe Instructions [C2M2 Survey Instructions] to use the Toolkit, and go through the process of generating a sample scoring report.
9. Become familiar with the Facilitator's Checklist in Appendix A of this guide.

If you have questions about any of the materials associated with the self-evaluation workshop, email C2M2@doe.gov, ES-C2M2@doe.gov, or ONG-C2M2@doe.gov.

2.4 Key Roles in the Self-Evaluation Process

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

Table 2: Key Roles in the Self-Evaluation Process

Role	Description and Responsibilities
sponsor	The sponsor should have a broad understanding of the status and components of the function for which the survey is being completed. The model defines a function as the as the subset of the operations of the organization that are being evaluated. It is most helpful for a sponsor to be: • part of the senior management team • a respected executive • acknowledged by the staff members as being in charge of their efforts and responsible for results • able give this role sufficient time and thoughtful attention General responsibilities include: • deciding whether the organization should participate in the C2M2 self-evaluation process • selecting an individual to serve as the facilitator • ensuring that the necessary resources for the C2M2 self-evaluation process are available • ensuring that the output from the project will receive the attention it deserves across the organization • participating in resolving issues and problems • committing resources and access to those resources • assigning the point of contact and other personnel resources • communicating the organization's support for the C2M2 self-evaluation process, asking the team members to provide the necessary support • kicking off the C2M2 self-evaluation workshop session
facilitator	The facilitator is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the C2M2 self-evaluation. General responsibilities include: • completing the three phases of a typical C2M2 self-evaluation process • ensuring that all activities in the self-evaluation process are executed efficiently and effectively • working with the organization to ensure the self-evaluation produces high-quality results • facilitating the C2M2 self-evaluation workshop • recording responses and comments during the C2M2 self-evaluation workshop • generating the C2M2 Evaluation Scoring Report • distributing the C2M2 Evaluation Scoring Report to the sponsor and designees • reviewing the detailed outcomes with the sponsor and designees • assisting in the planning of follow-up activities
point of contact (POC)	Depending on parameters such as the physical location of the facilitator, the facilitator's familiarity with the organization, and the organizational relationship between the facilitator and the portion of the organization being evaluated, the sponsor may designate a local POC to expedite the day-to-day interaction between the facilitator and the organization. General responsibilities could include: • assisting the facilitator in understanding the organization and how it functions • working with the facilitator to ensure proper participation for the self-evaluation workshop • ensuring that proper facilities and support staff are available for the self-evaluation workshop • ensuring that participants are available to attend the self-evaluation workshop • acting as liaison between the facilitator and the organization • participating in resolving logistics issues and problems

Role	Description and Responsibilities
subject matter experts (SMEs)	SMEs provide answers to the self-evaluation survey questions that best represent the organization's current cybersecurity capabilities in relation to the function being evaluated. It is most helpful for a SME to be: • 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 functions • able to represent organizational functions being evaluated • able to represent one or more of the organization's activities in the C2M2's 10 domains
participants	All individuals whose presence and active participation is necessary and critical during the self-evaluation workshop (e.g., sponsor, facilitator, POC, SMEs) are referred to as *participants*. The facilitator should ensure all participants are available for the duration of the self-evaluation workshop.
observers	All individuals whose presence and active participation are optional during the self-evaluation workshop are referred to as *observers*. Attendance of observers should be approved by the sponsor or designee (e.g., POC).
support staff	In collaboration with the sponsor and/or POC, the facilitator should identify all other individuals whose support is necessary during all three phases of a typical C2M2 self-evaluation process. Those individuals can include: • administrative assistants (to send meeting invitations, coordinate calendars, copy and assemble materials) • scribes (to take notes during preparatory meetings and/or during the workshop as necessary) • technology support staff (to provide and set up all necessary information technology (IT) and non-IT hardware and software required for the workshop) • site security staff (to issue visitor badges and enable proper physical access by the visitors)

2.5 Meeting with the Sponsor and Other Stakeholders

Prior to setting a date for the planned self-evaluation workshop, the facilitator should meet with the sponsor and other stakeholders identified by the sponsor to prepare the organization for the self-evaluation process. A meeting with the sponsor should take place prior to scheduling the planned day-long self-evaluation workshop.

The objectives of this meeting include the following:

- Familiarize the sponsor and/or stakeholders with the C2M2 (e.g., the facilitator could utilize the Introduction to the C2M2 presentation material [C2M2 Intro] during the meeting).
- Obtain strong and visible executive support for the self-evaluation and the associated workshop.
- Familiarize the facilitator with the organization's operating environment, the business drivers influencing its cybersecurity efforts, and manner in which the C2M2 self-evaluation will be used by the organization.

- Discuss the sponsor's expectations for the self-evaluation process (e.g., the three phases of the process, required resources, timeframe involved, personnel roles and responsibilities).
- Discuss a desired future state of organizational cybersecurity capabilities, consistent with the organization's business objectives and risk environment and the C2M2 as a framing structure.
- Discuss plans for next steps after the self-evaluation is conducted.
- Discuss the need for an additional preparatory meeting(s) with the sponsor and/or other stakeholders in the organization.

2.6 Identifying the Scope of the Self-Evaluation

The term "function" is used here as a mechanism to identify the scope of the self-evaluation activity; i.e., it is used to refer to the subset of the organization that is being evaluated. This subset, or function, could align within organizational boundaries (e.g., departments; lines of business; facilities) or could equally represent certain systems or technology areas that cross organizational boundaries.

For example, an organization is using the model to evaluate its enterprise IT services, including email, internet connectivity, voice over IP (VOIP) telephony, and the like. In the Threat and Vulnerability Management domain, practice 2b states, "Cybersecurity vulnerability information is gathered and interpreted for the function." When evaluating the implementation of this practice, the organization should interpret *function* to mean the operations of the enterprise IT services. In this example, the practice means that cybersecurity vulnerability information is gathered and interpreted for the enterprise IT services—information about vulnerabilities that would affect the enterprise email services, network devices, and the VOIP system.

> For the purpose of applying the C2M2 to the electricity subsector, the advisory group focused on four high-level functions performed by electric utilities: generation, transmission, distribution, and markets. However, the model can be applied to other functions or sub-functions performed by the organization.

The facilitator must work with the organization to determine the *scope of the self-evaluation survey* — the part of the organization's operations to which the model and survey will be applied to and its supporting IT and operations technology (OT). Selecting and documenting the scope before conducting the survey ensures that users of the survey results understand to which part of the organization the results apply.

When determining the scope of the survey, the facilitator must work with the organization to consider the cybersecurity practices applied to the various technologies supporting a given function. It is not necessary to consider the entirety of the technology deployed throughout the organization; selecting the subset of the technology that directly supports the function or selecting a sub-function may be useful when evaluating performance against the model. For example, consider an organization that decides to evaluate the cybersecurity practices it uses to protect and sustain its customer service operations. The organization must then determine which assets are in scope and which are out of scope. If a domain controller is used to manage access to a customer information management system that supports the customer service function as well as the organization's billing system, then that controller would be in scope. If the domain controller manages access to the billing system but not the customer information management system, then the controller and its associated cybersecurity practices would be out of scope.

For the purpose of applying the C2M2 to the oil and natural gas subsector, the advisory group focused on fifteen functions performed by members of the subsector. These functions are organized into three categories: upstream functions, midstream functions, and downstream functions.

Upstream Functions
- Exploration
- Development
- Crude oil production
- Natural gas production
- Research and development

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

Downstream Functions
- Refining
- Natural gas processing
- Distribution
- Retail

However, the model can be applied to other functions or sub-functions performed by the organization.

Though the C2M2 and survey are applicable to the entire organization, the self-evaluation survey is typically applied to a single function of to maintain focus. It may be applied even more granularly. If the organization performs an evaluation of more than one function, it is recommended that each function be evaluated separately, using separate surveys on different days to ensure sufficient consideration of the function's cybersecurity practices. If the organization manages the cybersecurity of these functions in the same way, then the two evaluations should return the same results. If they do not return the same results, the organization should investigate why the differences exist. One reason for a difference might be that the risks faced by each are different. Systems supporting multiple functions should be included in each function's evaluation. This not only produces redundancy in the evaluation results but also ensures that the evaluation of each function stands on its own.

It is expected that the facilitator will assist the sponsor and the organization to identify the scope of the self-evaluation and the key functions for which the survey will be completed. The

meeting with the sponsor (described in Section 2.5) is an excellent opportunity to discuss the self-evaluation and its scope.

This scoping exercise is critical since answers to the survey questions are used to rate the implementation of cybersecurity practices within the function that has been scoped for the evaluation. Additional information about selecting the scope of the survey is provided in Section 2 of the C2M2 Evaluation Survey ReadMe Instructions [C2M2 Survey Instructions].

2.7 Identifying and Preparing Participants and Support Personnel

For the C2M2 survey workshop to be successful, participants should be knowledgeable about cybersecurity practices surrounding the function for which the survey is being completed. There should be SMEs representing how the organization operates in all 10 C2M2 domains (see Table 3). It is not necessary to have a single SME for each domain; an individual can be a SME for multiple C2M2 domains. Alternatively, it may be necessary to engage multiple SMEs to fully cover a single domain.

The SMEs must also have enough knowledge of the operations of the organization to answer survey questions within their area of functional expertise. This may require additional SMEs beyond those representing the C2M2 domains.

Table 3: Identifying Participants and Support Personnel

Domain/Expertise/Function	Name of SME/Participant/POC
Risk Management	
Asset, Change and Configuration Management	
Identity and Access Management	
Threat and Vulnerability Management	
Situational Awareness	
Information Sharing and Communications	
Event and Incident Response, Continuity of Operations	
Supply Chain and External Dependencies Management	
Workforce Management	
Cybersecurity Program Management	
Operations (if needed)	
IT Support	
Scribe (Optional)	

In addition to SMEs discussed above, the facilitator should identify support staff that may be required to assist in conducting the self-evaluation survey (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. Facilitators can help prepare participants by providing them copies of the C2M2 [C2M2] and the Introduction to C2M2 presentation [C2M2 Intro] for self-study and/or having them participate in face-to-face or virtual meetings during which the facilitator provides background information about the C2M2.

2.8 Scheduling the Workshop

In collaboration with the sponsor, POC, and support staff, the facilitator schedules the workshop. Assistance from the sponsor or executive management might be necessary to clear calendars of SMEs and other critical participants. Tasks in scheduling include but are not limited to the tasks in Table 4.

Table 4: Steps and Activities Involved in Scheduling the Workshop

☑	Task Description
☐	Identify the date for the workshop based on the availability of the sponsor and participants
☐	Allocate the entire day (at least 8 hours) for the self-evaluation workshop
☐	Send invitations to selected participants (as described in Section 2.7)
☐	Request that the sponsor communicate to the invitees the importance of the process and their active participation
☐	Ask for acknowledgements and confirmation from invitees
☐	Set expectations and restrictions for invitees with regard to sending alternates
☐	Ensure there are sufficient confirmed participants to conduct the self-evaluation

2.9 Planning Workshop Logistics

Thorough logistical preparation is necessary to ensure a successful self-evaluation workshop. In collaboration with the POC and/or support staff, the facilitator is expected to plan for all workshop logistics including but not limited to the tasks in Table 5.

Table 5: Logistics Preparation Tasks for the Workshop

☑	Task Description
☐	Identify and reserve appropriate meeting space for the workshop
☐	Communicate IT system requirements for the survey and scoring tool (e.g., type and quantity of computing hardware and software applications) to the IT support staff (see the C2M2 Evaluation Survey ReadMe Instructions document [C2M2 Survey Instructions])
☐	Communicate non-IT requirements for the meeting space to the support staff (e.g., type and quantity of computer projectors; Audio/Video equipment; dry-erase boards and pens; easels, easel pads, and markers)
☐	Test all the tools (hardware and software) ahead of time, including files provided by DOE
☐	Coordinate travel arrangements as necessary

- ☐ Arrange for catering if desired
- ☐ Arrange for building access for all participants
- ☐ Establish non-disclosure agreements (NDAs) if necessary (e.g., if some of the participants are not members of the organization)

3. SURVEY WORKSHOP

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

3.1 Preparing the Room

Prior to the scheduled start time, the facilitator should ensure that the room is properly configured to conduct the self-evaluation survey.

Using the current version of the C2M2 Facilitated Self-Evaluation Toolkit as a reference, the facilitator should ensure that the required technology is ready. At least one or more personal computers should be available. One personal computer should be connected to the projector. This computer should meet the system requirements noted in the C2M2 Evaluation Survey ReadMe Instructions [C2M2 Survey Instructions]. Table 6 lists the room preparation tasks.

Table 6: Room Preparation Tasks for Day of the Workshop

☑	Task Description
☐	Sufficient seating is available for all expected survey workshop participants and any observers
☐	The room is set up to facilitate dialog among participants
☐	The screen is visible to the participants
☐	Lighting in the room can be dimmed to ensure that projected information is readable
☐	Flip chart paper and/or white boards (with markers) are available
☐	Test all the tools (hardware and software) including files provided by DOE
☐	The Evaluation Survey [C2M2 Eval Survey] file is open and ready to record responses

Some organizations may wish to designate an individual as the scribe. This allows the facilitator to focus on the discussion and arriving at a consensus response. The scribe would project the Self-Evaluation Worksheet and enter notes.

3.2 Kicking Off the Workshop

DOE provides PowerPoint slides for use by the facilitator to introduce and review the C2M2 Workshop Overview. These slides include a sample agenda for the Workshop. During the Preparation phase, the facilitator may wish to tailor this presentation to be specific to his/her organization. The facilitator might also use the tailorable C2M2 Facilitated Self-Evaluation Presentation [C2M2 Self Eval] material to show how the report that will be generated could be used after the workshop.

It is often useful to begin the workshop with comments from senior management. These comments can help emphasize the importance of the C2M2 to the organization, identify the business drivers for a cybersecurity effort, and highlight the importance of the active participation of workshop attendees.

Remind participants that the survey is intended to provide a snapshot of the maturity of the organization's cybersecurity posture. The facilitator should ensure that the workshop participants are prepared for and comfortable during the one-day workshop.

Table 7 describes several topics that experience has shown deserve special emphasis prior to beginning the workshop.

Table 7: Topics for Discussion at the Start of the Workshop

Topic	Discussion
C2M2 definitions	Having a copy of the glossary of terms from Appendix C of the C2M2 is useful for discussions during the self-evaluation. Allow participants an opportunity to review prior to beginning the Workshop. The ES-C2M2 and ONG-C2M2 glossaries contain entries for terms that are specific to the model subsectors.
Organization's vocabulary	Discussion of terms found in the C2M2 may prompt discussions relating to terms used within an organization. Although not all terms can be anticipated in advance, this discussion is useful to highlight possible conflicts.
Agreed-upon function and scope	It is important to remind the participants that the self-evaluation survey is being applied to a specific set of activities performed by the organization and to describe those activities prior to beginning the Workshop.
Organization's environment	It is useful to discuss the organization's environment to add context to the description of the function being evaluated.
Implemented practices	When completing the survey, participants must consider practices as they are implemented on the day the survey is completed. Do not consider activities that are planned or in the process of implementation. Likewise, 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.
Four-point response scale	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 so that all participants have a common understanding of when a particular response will be used. See Appendix B -Frequently Encountered Discussions for additional discussion.
Follow-on activities	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. The facilitator should emphasize that next steps will be based on the organization's risks and maturity. The output of the C2M2 survey should drive risk conversations and allow organizations to plan yearly reviews of their cybersecurity program to track progress and validate goals. The facilitator should also point out the roles of participants in follow-up activities.

3.3 Facilitating the Workshop

The facilitator guides the participants through the survey questions. Remember that open dialog and consensus building is as important as the completed survey. Consensus has been achieved when every participant feels that his/her views have been heard *and* when all participants feel they can support the proposed decision. The facilitator assists the group in formulating high-quality, consistent responses based upon consensus.

After introducing the agenda for the day and providing an overview of the C2M2 and general guidelines, the facilitator shows participants the first questions from the Risk Management domain. Read the description of the domain, the first goal, and the first question verbatim. Describe the intent of the Risk Management practice, and remind participants of the scoring guidelines.

Most groups find it helpful to view a visual (projected) display of the questions they are considering and responses they have already provided. The facilitator controls the responses recorded on the survey instrument and can display questions and responses as required. Notes regarding the discussions can also be reviewed to determine the rationale behind the responses given.

The list of materials to support the facilitation recommends that dry-erase boards, easels, and flip charts with markers be on hand. These materials can be used to illustrate or diagram key concepts as well as to capture and display common assumptions developed by the group that are key to allowing the group to come to consensus. Having such illustrations available throughout the discussion provides useful reminders.

It is important to encourage discussion. There is value in allowing participants to interact and discuss as a group what the consensus answer will be rather than using predeveloped responses. The facilitator does not provide answers to the survey questions but rather helps the group come to a consensus response. The process of facilitating the workshop assists the organization not only in answering survey questions but also in formulating the next steps the organization must take when defining gaps and developing an improvement plan.

At times the facilitator must remind participants not to get stuck on the specific phrasing of a question but to focus on the intent behind the question. The C2M2 Glossary [C2M2 Glossary] is useful in coming to this understanding and should be given to all participants prior to the workshop; the glossary should also be on hand during the workshop.

3.4 Processing the Collected Data

After all answers to the survey questionnaire have been entered into the C2M2 Evaluation Survey [C2M2 Eval Survey], the facilitator releases participants for the Report Generation break listed on the agenda. During this break the facilitator prepares the reports and projects them for the participants.

Detailed procedures for preparing these reports are provided in the C2M2 Evaluation Survey ReadMe Instructions [C2M2 Survey Instructions].

3.5 Presenting the Scoring Report

The facilitator will use the C2M2 Evaluation Scoring Report to review the results at the end of the evaluation. The facilitator must be flexible, considering time remaining in the day and the expectations of the participants. Most participants are tired at the end of the day and do not have the energy for a detailed review of the report. Nevertheless, participants will expect some same-day discussion and presentation of the results. A logical place to begin is with a presentation of the Domain view. The Domain view presents evaluation results using donut charts. A single donut chart shows achievement of a specific MIL [MIL Scale] level in a domain. The donut chart, as shown in Figure 2 provides count of questions that received responses of:

- Not Implemented (dark red – 6 practices)
- Partially Implemented (light red – 8 practices)
- Largely Implemented (light green – 8 practices)
- Fully Implemented (dark green – 2 practices)

The number 24 at the center of the donut represents the total number of questions that must be answered "Largely Implemented" or "Fully Implemented" to achieve the MIL for the sample domain in Figure 2. The presence of dark red and light red colors on the donut indicates that the organization did not achieve that MIL.

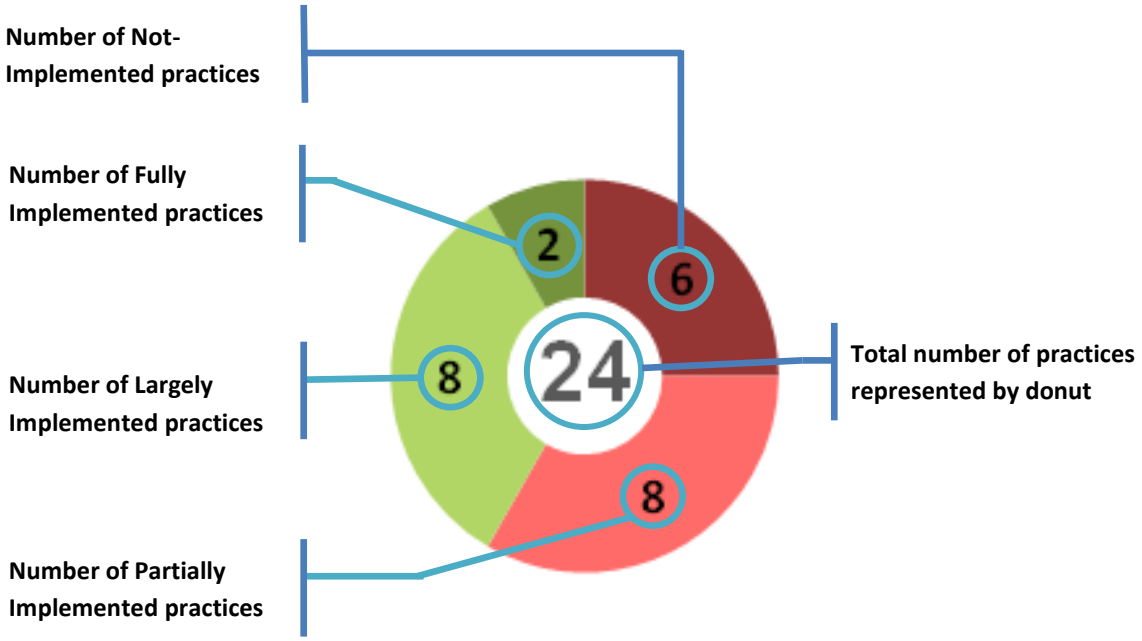

Figure 2: Graphical Representation of Single Donut

It is important to mention that the number at the center of the donut indicates the cumulative number of practices at each MIL level. Considering the example of the RM domain in Figure 3, there are two practices at MIL 1, and eleven practices at MIL 2. Therefore, the center of the middle donut in the RM domain shows the number (2+11) 13. There are eleven practices at MIL 3, so the top dount in the RM domain shows the number (2+11+11) 24.

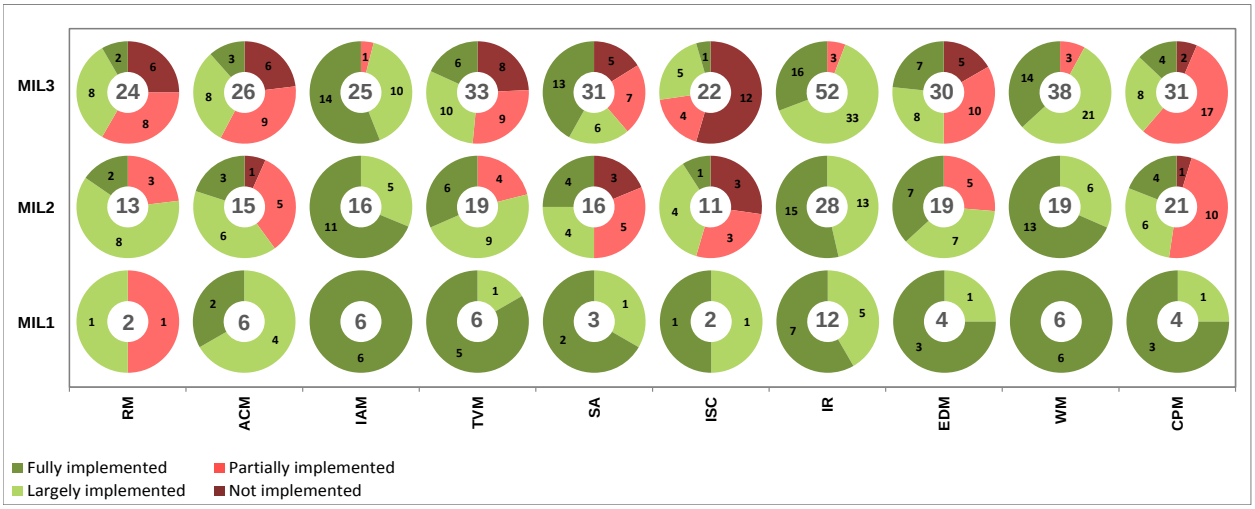

Figure 3: Domains Graphical Summary of the C2M2 Survey

The Domain view provides the simplest graphical summary of maturity assessments, depicted as a 3x10 array of donut charts that relate each domain to progressively advancing MILs [MIL Scale]. To demonstrate, a quick inspection of the example in Figure indicates the following:

- None of the domains are assessed at MIL 3.
- Three domains are assessed at MIL 2 (IAM, IR, WM).
- Six domains are assessed at MIL 1 (ACM, TVM, SA, ISC, EDM, CPM).
- One domain is assessed at MIL 0 (RM).

The facilitator should emphasize that getting high MIL scores is not the goal of conducting the survey. Some practices do not make sense for an organization based on its risk profile. It is useful to point out to the participants that within any domain, the specific practice questions that prevent an organization from achieving a specific MIL are prerequisites to practice questions that allow the organization to achieve a higher MIL. Addressing such disqualifying factors at their lowest MIL offers the shortest path to advancement to a higher MIL. The Domains display may give some initial insights into where to invest in cybersecurity improvement by drawing attention to the absence of qualifying practices at the low MIL.

The Objective view presents additional detail by providing a graphic showing practice question responses by domain and objectives (as opposed to the breakdown by domain and MIL in the Domain view). The facilitator may or may not wish to use this display during the end-of-day discussions; it may provide participants a more detailed look at goals in a specific domain.

The Objective view uses the same donut chart used in the Domain view; however, the donut charts show responses for each domain-specific objective rather than MIL. For brevity, Figure 4 shows only 4 of the 10 domains.

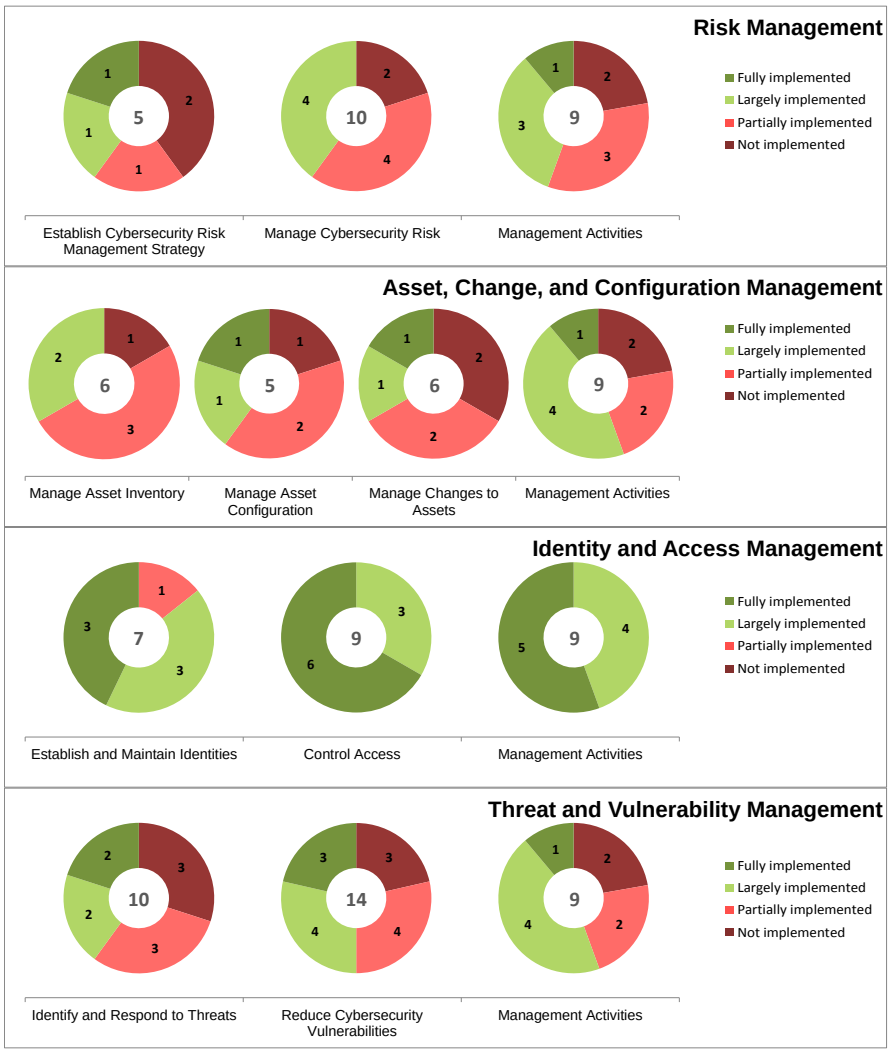

Figure 4: Objectives Graphical Summary of 4 of the 10 Domains on the C2M2

After completing the review of the data reports, the facilitator reminds participants and the sponsor that a typical goal is to first achieve MIL 1 in all domains and then —based on the organization's risk tolerance select other areas for improvement. Organizations should set their own path for improvement based on their organizational needs. If an organization has a compliance issue that will cost a lot of money, the organization should address that issue first. Follow-up activities will be discussed in the next chapter but should be highlighted for all participants prior to closing the workshop. It is recommended that the facilitator provide an opportunity for all participants to make any last comments or observations and provide the sponsor an opportunity to make closing remarks. Be sure to thank all participants and collect all relevant materials.

4. FOLLOW-UP ACTIVITIES

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

4.1 Collecting All Workshop Artifacts and Submitting Them to the Sponsor

The electronic files involved in the self-evaluation workshop, including the completed survey, the self-evaluation tool, and the generated reports, are the property of the organization undergoing the self-evaluation. The sponsor should be given these files. The facilitator should collect any other notes taken but not entered into the self-evaluation survey and consolidate them with his/her own notes in preparation for working with the sponsor to plan follow-up activities.

4.2 Reviewing the Detailed Outcomes with the Sponsor

The facilitator remains engaged in follow-up activities, as familiarity with the model and the workshop results can help identify follow-up actions.

The C2M2 evaluates maturity across 10 domains of cybersecurity and identifies specific gaps as a means to initiate a process improvement project as depicted in Figure 5 below.

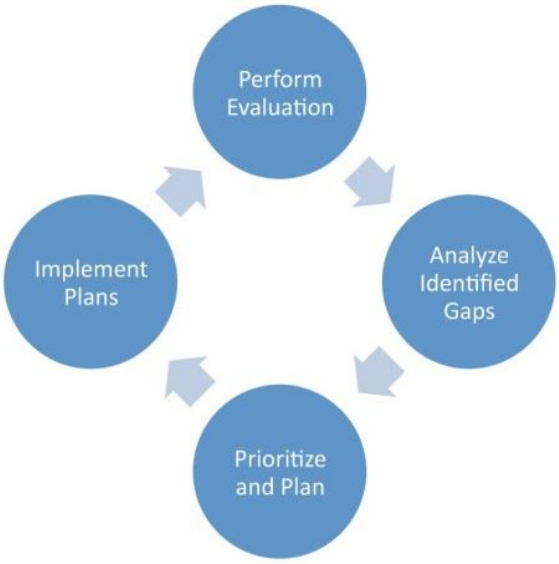

Figure 5: Steps in a Typical Process Improvement Activity

Follow-up action is guided in part by

- the organization's maturity self-evaluation using the C2M2, which organizes each domain's gaps into progressive MIL categories

- a subjective alignment of each domain's practices against the organization's business missions, corporate values, and the risk to critical infrastructure (if applicable), which results in a desired state (the desired state is usually expressed as a profile showing each domain and the associated desired capability)

A more detailed assessment of these four steps is summarized in a table in Section 5.2 of the Survey Report, reproduced in Table 8 below. Further details on specific references for follow-up action on each domain are given in Appendix B of the Survey Report.

Table 8: Recommended Process for Using Results

	Inputs	Activities	Outputs
Perform Evaluation	1. C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct C2M2 Self-Evaluation Workshop with appropriate attendees	C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

The C2M2 does not prescribe specific maturity levels for organizations in any particular industry. However, achieving MIL 1 across all C2M2 domains is a worthwhile goal for any organization.

For example, a facilitator, working with the sponsor, might determine that the organization's desired capability for the Information Sharing and Communications (ISC) domain is set at MIL 2, while the organization's desired capability for the Asset, Change, and Configuration Management (ACM) domain is set at MIL 3.

When identifying ISC gaps, the facilitator would compare the organization's desired capability profile with its C2M2 assessments for this domain, summarized in the ISC view of the C2M2 Evaluation Scoring Report.

MIL1		MIL2									MIL3										
1a	1b	1c	1d	1e	1f	1g	2a	2b	2c	2d	1h	1i	1j	1k	1l	2e	2f	2g	2h	2i	2j

1. Share Cybersecurity Information

MIL1	a. Information is collected from and provided to selected individuals and/or organizations	**FI**
	b. Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), law enforcement)	**LI**
MIL2	c. Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected organizations, vendors, sector organizations, regulators, internal entities)	**LI**
	d. Information is collected from and provided to identified information-sharing stakeholders	**PI**
	e. Technical sources are identified who can be consulted on cybersecurity issues	**PI**
	f. Provisions are established and maintained to enable secure sharing of sensitive or classified information	**NI**
	g. Information-sharing practices address both standard operations and emergency operations	**NI**

Figure 6: A Sampling of Individual Domain Reports

In this situation, a sponsor's desire to advance from the current MIL 1 state to a target MIL 2 state might require the organization to complete its inventory of relevant information-sharing stakeholders (ISC-2c), establish a secure means to communicate sensitive or classified information (ISC-2f), and implement practices that address both standard and emergency operations (ISC -2g).

An inspection of the ACM tab reveals the organization is already performing at its target goal of MIL 3; efforts may be better focused addressing the deficient domains of IAM, TVM, WM, and CPM that have not achieved even a basic level of MIL 1. Inspection of those four tabs in the ES-C2M2 Toolkit Excel file [C2M2 Toolkit] would provide initial and specific guidance on the process improvements the sponsor might consider undertaking.

4.3 Assisting the Organization with Planning Follow-Up Actions

Figure presents a notional improvement approach. This section focuses on the three phases:

1. Analyze Identified Gaps
2. Prioritize and Plan
3. Implement Plans

4.3.1 Analyzing Identified Gaps

The C2M2 Evaluation Scoring Report provides graphs and tables that detail an analysis based on the C2M2. There are summary charts showing achievement of MIL by Domain as well as detailed tables showing the responses for each survey question. These graphs and tables present how well an organization scores against the C2M2. The next step is to understand how the organization is positioned against its identified desired capability profile. The organization's Evaluation Scoring report contains Table 5.1, Summary of Identified Gaps. This table lists the survey questions that were answered either "Partially Implemented" or "Not Implemented" and is useful in setting a Target Profile.

It probably is not optimal for an organization to strive to achieve the highest MIL in all domains. Rather 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 desired capabilities 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 evaluation to identify the 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 walking through the practices before performing an evaluation, is most typically adopted by organizations that have more experience and familiarity with the model.

4.3.1.1 Setting a Target Profile – Method 1

In this approach, an organization uses the results of a completed C2M2 evaluation to jumpstart the identification of its Target Profile. The organization begins by walking through the results section in each domain and performing the following steps:

1. Identify all of the practices that have been scored as "Not Implemented."
2. For each practice that is "Not Implemented," review the practice and determine whether the practice needs to be performed to meet the organization's business and cybersecurity objectives.
3. If "yes" then document that practice.
4. If "no" then move on the next "Not Implemented" practice.
5. Repeat steps 1 to 4 for all practices in the domain that have been identified as "Partially Implemented."
6. Repeat steps 1 to 4 for all practices in the domain that have been identified as "Largely Implemented."
7. Repeat for all 10 model domains.

Once this review is complete, the organization should have a documented list of practices that need to be performed. In the report, the organization has the list of practices it is already performing. The combined set of practices is the organization's Target Profile. This approach has the advantage that the generated list of practices that need to be performed also serves as

the list of gaps to be addressed. This list of gaps gives the organization a starting point for prioritizing and planning.

4.3.1.2 Setting a Target Profile – Method 2

In this approach, an organization walks through the C2M2 practices before undergoing an evaluation to identify its Target Profile. The organization begins by walking through each of the practices in each domain in the model and performing the following steps:

1. Review the practice and determine whether the practice needs to be performed to meet the organization's business and cybersecurity objectives.
2. If "yes" then document that practice.
3. If "no" then move on to the next practice in the domain.
4. Repeat for all 10 model domains.

Once this review is complete, the organization will have a documented list of practices that it believes it needs to perform to meet its goals. This selection of practices is the organization's Target Profile. This Target Profile can then be compared against the results of the evaluation to determine where gaps exist that need to be addressed.

4.3.2 Prioritizing and Planning

After the gap analysis is complete, the facilitator must work with the sponsor to prioritize the actions needed to fully implement the practices that enable the achievement of the desired capability in specific domains. The prioritization should be done using criteria such as how gaps affect organizational objectives, critical infrastructure, the criticality of the business objective supported by the domain, the cost of implementing the necessary practices, and the availability of resources to implement the practices. A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed.

Next, a plan is developed to address the selected gaps. These plans can span a period of three to five years depending on the extent of improvements needed to close the selected gaps and achieve the desired capability. The sponsor would ideally be the owner of the plan, although responsibility for implementation might be assigned to a person designated by the sponsor (typically the facilitator).

4.3.3 Implementing Plans

The sponsor must provide adequate resources for the plan to be a success, including people with the necessary skills to accomplish the planned tasks and a budget that will allow them to be successful. In addition, the sponsor must continue supporting the execution of the plan through tracking progress and recognizing accomplishments.

After plans have been developed and implemented to address selected gaps, the facilitator should periodically re-evaluate organizational business objectives and risk to critical infrastructure to check for changes in desired capability. A periodic re-assessment using the C2M2 can track progress towards the organization's desired capability profile.

5. SUMMARY

This document describes how an organization should prepare and conduct a C2M2 self-evaluation using its own facilitator. This guide contains information about how to prepare for the self-evaluation, how a facilitator assists the organization in evaluating the maturity of its cybersecurity capabilities during the workshop, and guidance for follow-on activities to prioritize and implement a plan to close identified capability gaps.

For additional assistance, the facilitator and other participants can email DOE at C2M2@doe.gov, ES-C2M2@doe.gov, or ONG-C2M2@doe.gov.

APPENDIX A: FACILITATOR'S CHECKLIST

☑	Task Description	Facilitator Guide Section
	Four Weeks Prior to Survey Workshop	
☐	Obtain the latest version of C2M2 documentation and facilitation material	2.1.2
☐	Become familiar with C2M2 and self-evaluation artifacts	2.1.3
☐	Meet with the sponsor and other stakeholders	2.3
☐	Determine organizational scope of the survey	2.4
☐	Answer questions 1-3 of the survey	2.4
☐	Identify participants and support personnel	2.2
☐	Prepare participants	2.5
☐	Identify date for the workshop	2.6
☐	Have the sponsor communicate to the participants the importance of the activity	2.6
☐	Send invitations to participants	2.6
☐	Send preparatory reading material to participants	2.5
☐	Identify and reserve appropriate meeting space for the workshop	2.7
☐	Make travel arrangements (if necessary)	2.7
☐	Establish non-disclosure agreements (NDAs) if necessary	2.7
☐	Meet with local point of contact	2.7
☐	Identify and document risks to the successful execution of the process; consider mitigations	2.7
	Two Weeks Prior to Survey Workshop	
☐	Ensure there are sufficient confirmed participants to conduct the self-evaluation workshop	2.5
☐	Communicate IT system requirements for the survey and scoring tool to IT support staff	2.7
☐	Communicate non-IT system requirements for the survey and scoring tool to support staff	2.7
☐	Arrange for someone to scribe/take notes	3.1
☐	Arrange for catering (if necessary)	2.7
☐	Arrange for building access for those visiting	2.7
☐	Touch base with local point of contact	2.7
	One Week Prior to Survey Workshop	
☐	Test all the tools (hardware and software) ahead of time, including files provided by the DOE	2.7
☐	Touch base with local point of contact	2.7
☐	Ensure support staff will provide supplies for the room	2.7

☑	Task Description	Facilitator Guide Section
	The Day Before the Survey Workshop	
☐	Ensure the meeting room has been set up properly	3.1
☐	Ensure the required technology (computers, projectors, etc.) is present and functioning	3.1
☐	Load the necessary files onto the designated computers and test	2.7
☐	Confirm catering (if necessary)	2.7
	The Day of Survey Workshop	
☐	Arrive at the meeting room at least 30 minutes prior to the start of the workshop	3.1
☐	After completion of the workshop, collect all printed sensitive material	3.4
☐	After completion of the workshop, copy necessary files from the room computer onto two other locations/media; delete all workshop files from the room computers	3.4
	Within One Week After Survey Workshop	
☐	Collect notes	4.1
☐	Organize the reports generated by the self-evaluation survey tool and all other relevant notes and material	4.1
☐	Deliver final package of material to the sponsor	4.1
☐	Meet with the sponsor to assist the organization with planning follow-up actions	4.2

APPENDIX B: FREQUENTLY ENCOUNTERED DISCUSSIONS

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

1. Discussions Relevant to the Entirety of a C2M2 Self-Evaluation

- The distinction between *largely* implemented and *partially* implemented

Participants will arrive at the workshop with their own ideas of what these responses mean. The facilitator must provide a means for the group to come to a consensus on a definition of these responses early on so that the response has a consistent meaning throughout the survey. 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 should be considered partially implemented. If only one action is required, or the group views the actions described as minor, consider the practice largely implemented. The facilitator should record what action(s) the group articulates. This information can be useful to the organization when reviewing the scoring report and planning follow-up actions.

- The meaning of "implemented in an ad hoc manner"

When reading the domain-specific practice questions from the survey form, you will encounter the phrase "at least in an ad hoc manner." All MIL 1 practice questions on the survey contain this phrase. If the participant is familiar with the C2M2 only through review of the model documentation, he/she will not encounter this phrase while reviewing the domain-specific practices. It is good practice to keep the glossary handy for this discussion.

It is important to remind participants that even ad hoc practices must meet business and operations objectives to be considered fully implemented.

- Questions with cross-domain dependencies

There are six practice questions that—depending on how they are answered—limit the responses that can logically be given for later questions. These dependencies are clearly identified in the survey as they occur; however, the survey does not identify the practice question that initiates the dependency. It is important to remind participants that a dependency is being established when they first encounter these practice questions so that these questions can be fully discussed and described.

The domain and practice question number of those questions that initiate a dependency are listed below. The practice questions that depend on the response are also listed.

Table 9: Practices with Cross-Domain Dependencies

Question	Dependency
RM-1c (risk criteria)	IAM-1g, TVM-1i, TVM-2l, IR-3m, IR-4h, EDM-1g, EDM-2j, EDM-2k
RM-2j (risk register)	TVM-1j, TVM-2m, SA-2j, IR-1g, IR-2g, EDM-2c
TVM-1d (threat profile)	SA-2f, IR-1g, IR-2g, IR-3m, WM-4c, CPM-1g
IR-1b (cybersecurity event detection)	SA-2d
SA-3a (common operating picture)	IR-1h, IR-2h
SA-3f (predefined states of operation)	WM-4d

- Reminders when reviewing common objectives

The last nine practice questions in each domain are listed under the heading "Management Activities." These questions are similar in criteria for each domain, but the phrasing of each question changes to focus on the domain at hand.

These questions help the organization determine the degree to which practices have been institutionalized—that is, the extent to which a practice or activity is established in an 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 common objectives and practices, it is important to remind participants that their responses to these questions should consider the entire domain and all the domain-specific subgoals and practices. For example, when answering the Manage ACM Activities practice questions, participants consider whether these practices are implemented for asset inventory *and* change management *and* configuration management. Often, because of the structure of the survey and the repetitive nature of the Management Activities practice questions, the facilitator must remind participants to consider the entire domain. If participants appear to be arriving at their responses too quickly, it is often worth re-phrasing or re-asking these questions.

Question C under Management Activities ("Adequate resources [people, funding, and tools] are provided to support <domain> activities") may be difficult to interpret. This question relates to whether or not resources are provided to support the practices already being implemented in that domain. This is not intended as a place to capture "lack of resources" as the reason practices within the domain are not implemented. Such factors should be captured when the implementation of the specific practice is recorded, for the specific practice that is impacted.

- MILs and the dual progression of the model

The C2M2 describes the dual progression of the model in its discussion of MILs [C2M2]. As the model states, the MILs define a progression of both approach and of institutionalization. The progression of the approach to cybersecurity for each domain in the model is described by the domain-specific objectives and practices. "Approach" refers to the completeness, thoroughness, or level of development of an activity in a domain. As an organization progresses

from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain. The progression of institutionalization is described by a set of practices that can be performed to institutionalize the domain-specific practices. These practices are similar across domains and are called the Management Objective and Practices. The progression of the practices within a domain-specific objective corresponds to the progression of the management practices, though not necessarily practice-to-practice.

The facilitator should remind participants of this dual progression during the completion of the self-evaluation survey. Participants may struggle within the domain-specific objective as the practices described become more complex. Each question in an objective builds upon the previous question. The organizational approach to the practice reflected in the question becomes more mature. Similarly, the management questions reflect how the domain-specific practices have been institutionalized. Remind participants that the MIL increases as participants get closer to the last practice question within an objective or management practice. Participants should not expect to achieve a high MIL unless they have achieved the lower, foundational practices.

2. C2M2 Domain-Specific Discussions

Each domain begins with a purpose statement and introductory material. Reading this purpose statement and allowing participants to view the introductory material helps prepare participants to begin the new domain.

As each domain is addressed in the survey, there can be questions about unfamiliar terms and concepts as well as uncertainty about how to answer some questions. The explanations provided below address many discussion points that have been raised in previous survey workshops. This subsection is organized according to C2M2 domain, and its content can help workshop participants to better understand the intent of the survey questions.

Risk Management

What is Risk Management?

Risk management is the first discussion the facilitator encounters during the self-evaluation survey. The facilitator should have formulated an understanding of what constitutes the depth and breadth of this domain before beginning the survey. The facilitator may wish to review NIST's Special Publication 800-39, *Managing Information Security Risk* [NIST 800-39], or the Department of Energy's *Electricity Subsector Cybersecurity Risk Management Process* [NERC CIP], which was derived from the NIST publication. The developers of the C2M2 intentionally positioned the discussion of RM first in the survey because its implementation creates a ripple effect throughout the model.

The C2M2 self-evaluation can assist utilities in identifying gaps in their adoption of a risk management plan across an organization. The C2M2 self-evaluation examines how utilities have constructed an enterprise risk management strategy and risk management program and asks about the use of enterprise-derived criteria within key risk management practices. It also requires that organizations investigate their practices for developing and stabilizing important

cybersecurity practices and ensure those practices are consistent and institutionalized. Finally, the C2M2 self-evaluation guides the organization in a review of its threat, vulnerability, and asset management practices as these practices apply to information technology and operations technology.

It is also important to realize that the first objective in this domain asks if a documented cybersecurity risk management strategy exists. The existence of a documented strategy is a MIL 2 practice. This is different from most other domains and practices within the model. As discussed in the dual progression of the model, the practice questions within an objective usually progress from MIL 1 through MIL 2 to MIL 3. However, the importance of the RM domain to all areas of the C2M2 must be established early and warrants this unconventional approach.

What are risk criteria?

Risk criteria articulate an organization's tolerance for risk as well as its risk response approaches. Linking cybersecurity risks to organizational risks in a defined and documented manner is a reflection on the overall maturity of the organization's risk management program. Participants should focus on their response to this practice question without regard to the dependency between the implementation of risk criteria and responses to practice questions in the IAM, TVM, IR, and EDM domains. This dependency can be articulated as those practice questions are asked.

What is a risk register, and why is it important?

A risk register is a structured repository where identified risks are recorded to support risk management. Documenting and recording risk in a risk register ensures that these risks are monitored and addressed in a timely manner and assists in identifying trends. As a MIL 3 product, the risk register represents an artifact developed and maintained by an organization with mature risk management practices. Once again, participants should focus on their response to this practice question without regard to the dependency between implementing a risk register and responses to practice questions in the TVM, SA, IR, and EDM domains. This dependency can be articulated as those practice questions are asked.

Asset, Change, and Configuration Management

Participants often discuss question ACM-1f at length ("There is an inventory of all connected OT and IT assets related to the delivery of the function"). This discussion relates primarily to the inclusion of both routable and non-routable IT assets, but there has also been debate concerning the need to inventory all assets *related* to the delivery versus only those assets *important* to the delivery. The question may need some clarification. Although both routable and non-routable assets should be inventoried, only those IT assets important to the delivery of the function need to be considered when answering this question. Practice question ACM-1f is the culmination of an approach progression from ACM-1a (important) to ACM-1f (all).

Question ACM-3f ("Change logs include information about modifications that impact the cybersecurity requirements of assets [availability, integrity, confidentiality]") introduces the

concept of cybersecurity requirements to the participants. Cybersecurity requirements relate to the confidentiality, availability, and integrity of the IT and OT assets. This may be a new concept for participants who do not have a cybersecurity background.

Identity and Access Management

It is important to emphasize that the concept of access goes beyond physical access to include the management of credentials, which go beyond individuals and can include devices, services, and shared identities.

As noted earlier, the response to question IAM-1g ("Requirements for credentials are informed by the organization's risk criteria") depends on the existence of organizational risk criteria (RISK-1c).

Situational Awareness

The third objective in the SA domain describes the practices required to establish and maintain a common operating picture (COP). It is important to emphasize to the participants that the goal refers to establishing an aggregated, near-real-time understanding of the operational state of the function being examined. It does not necessarily require that a visual representation be rendered. Such representations can be costly to implement and maintain. The emphasis should be on developing an understanding of the state of operations, *not* the manner in which this understanding is visually conveyed.

Information Sharing and Communications

The facilitator should take advantage of the first practice question to allow the participants to discuss which organizations and individuals must be considered in the context of ISC activities. This first question frames the discussion in this domain and allows participants to examine this requirement in detail.

Supply Chain and External Dependencies Management

The facilitator should reinforce the difference between upstream and downstream dependencies; the practice questions themselves provide good definitions. Some organizations find it useful to establish a boundary condition for upstream dependencies by examining whether or not a ready substitute exists. A corresponding boundary may also exist in downstream dependencies.

Many organizations will invite their external contracts managers to participate in the discussions relating to dependencies. This can lead to useful discussion and insight. It is important to remember, however, that the existence of service level agreements (SLAs) does not necessarily imply that established criteria exist for the management of upstream or downstream dependencies. Rather, the existence of these criteria should be used as a basis for the development of SLAs.

Workforce Management

The concept of risk designations for workforce positions may be new for some organizations. Comparing the responsibilities and access level that a systems administrator requires with those of other staff members helps explain this concept.

Cybersecurity Program Management

The CPM domain can be thought of as defining and describing a cybersecurity program. When discussing a cybersecurity program, the participants should realize that such a program is composed of the other nine domains and how they are managed as a coherent cybersecurity program.

APPENDIX C: REFERENCES

[C2M2]	*Cybersecurity Capability Maturity Model (C2M2).* <http://energy.gov/node/795796> *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).* <http://energy.gov/node/369271> *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2).* <http://energy.gov/node/795806>
[C2M2 Eval Survey]	"Capability Maturity Model (C2M2) Evaluation Survey." Available from U.S. Department of Energy by emailing C2M2@doe.gov. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Evaluation Survey." Available from U.S. Department of Energy by emailing ES-C2M2@doe.gov. "ONG-C2M2 Evaluation Survey." Available from U.S. Department of Energy by emailing ONG-C2M2@doe.gov.
[C2M2 Glossary]	"C2M2 Glossary," Appendix B of *Cybersecurity Capability Maturity Model (C2M2).* <http://energy.gov/node/795796> "ES-C2M2 Glossary," Appendix B of *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).* <http://energy.gov/node/369271> "ONG-C2M2 Glossary," Appendix B of *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2).* <http://energy.gov/node/795806>
[C2M2 Intro]	"Introduction to C2M2 Presentation." Available from U.S. Department of Energy (DOE) by emailing C2M2@doe.gov. "Introduction to ES-C2M2 Presentation." Available from U.S. Department of Energy (DOE) by emailing ES-C2M2@doe.gov. "Introduction to ONG-C2M2 Presentation." Available from U.S. Department of Energy (DOE) by emailing ONG-C2M2@doe.gov.
[C2M2 MIL]	"C2M2 Domain MIL Reference Cheat Sheet." Available from U.S. Department of Energy (DOE) by emailing C2M2@doe.gov. "ES-C2M2 Domain MIL Reference Cheat Sheet." Available from U.S. Department of Energy (DOE) by emailing ES-C2M2@doe.gov. "ONG-C2M2 Domain MIL Reference Cheat Sheet." available from U.S. Department of Energy (DOE) by emailing ONG-C2M2@doe.gov.
[C2M2 Toolkit]	"C2M2 Toolkit," available from U.S. Department of Energy (DOE) by emailing C2M2@doe.gov. "ES-C2M2 Toolkit," available from U.S. Department of Energy (DOE) by emailing ES-C2M2@doe.gov. "ONG-C2M2 Toolkit," available from U.S. Department of Energy (DOE) by emailing ONG-C2M2@doe.gov.

[C2M2 Self Eval]	"C2M2 Facilitated Self-Evaluation Presentation," Available from U.S. Department of Energy (DOE) by emailing C2M2@doe.gov. "ES-C2M2 Facilitated Self-Evaluation Presentation." Available from U.S. Department of Energy (DOE) by emailing ES-C2M2@doe.gov. "ONG -C2M2 Facilitated Self-Evaluation Presentation." Available from U.S. Department of Energy (DOE) by emailing ONG-C2M2@doe.gov.
[C2M2 Survey Instructions]	"C2M2 Evaluation Survey ReadMe Instructions." Available from U.S. Department of Energy (DOE) by emailing C2M2@doe.gov. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Evaluation Survey ReadMe Instructions." Available from U.S. Department of Energy (DOE) by emailing ES-C2M2@doe.gov. "ONG-C2M2 Evaluation Survey ReadMe Instructions." Available from U.S. Department of Energy (DOE) by emailing ONG-C2M2@doe.gov.
[DHS Energy]	"U.S. Department of Homeland Security Energy Sector – Sector Overview." <http://www.dhs.gov/energy-sector>
[DOE RMP]	U.S. Department of Energy. *Electricity Subsector Cybersecurity Risk Management Process* (DOE/OE-0003). DOE, May 2012. <http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf>
[Facilitator]	"Facilitator." <http://en.wikipedia.org/wiki/Facilitator>
[MIL Scale]	Butkovic, Matthew; and Caralli, Richard. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale* (CMU/SEI-2013-TN-028). Software Engineering Institute, Carnegie Mellon University. December 2013. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187>
[NERC CIP]	North American Electric Reliability Corporation. "CIP [Critical Infrastructure Protection] Standards." <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
[NIST 800-39]	NIST Joint Task Force, Transformation Initiative. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. National Institute of Standards and Technology Computer Security Division, Information Technology Laboratory, Gaithersburg, MD, March 2011. <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>