Dams Sector Cybersecurity Capability Maturity Model (C2M2) Implementation Guide

A companion to the Dams Sector C2M2

2017

Homeland Security

Contents

Acknowledgements

This document was developed with input, advice, and assistance from the Dams Sector Cybersecurity Working Group and council members of the Dams Sector Government Coordinating Council and Sector Coordinating Council, which includes representatives from the public and private sectors.

This Implementation Guide is a supplement to the *Dams Sector Cybersecurity Capability Maturity Model* (Dams-C2M2), which is based on the *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2 Version 1.1) originally developed as part of a White House initiative in 2012 by Carnegie Mellon University and the U.S. Department of Energy (DOE), working in close consultation with owners and operators and cybersecurity experts in the Energy Sector. The U.S. Government has authorized the rights to use, modify, reproduce, release, perform, display, or disclose the Dams-C2M2 (along with the ES-C2M2) and corresponding toolkits provided by the U.S. Department of Homeland Security (DHS) or DOE. Capability Maturity Model® is a registered trademark of Carnegie Mellon University.

Intended Scope and Use of This Publication

The guidance provided in this publication is intended to address only the implementation and management of cybersecurity practices associated with information technology (IT) and operations technology (OT) assets and the environments in which they operate. This guidance is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that Dams Sector organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Compliance requirements are not altered in any way by this model. In addition, this guidance is not part of any regulatory framework and is not intended for regulatory use. Rather, the guidance in this publication is intended to complement a comprehensive enterprise cybersecurity program.

Introduction

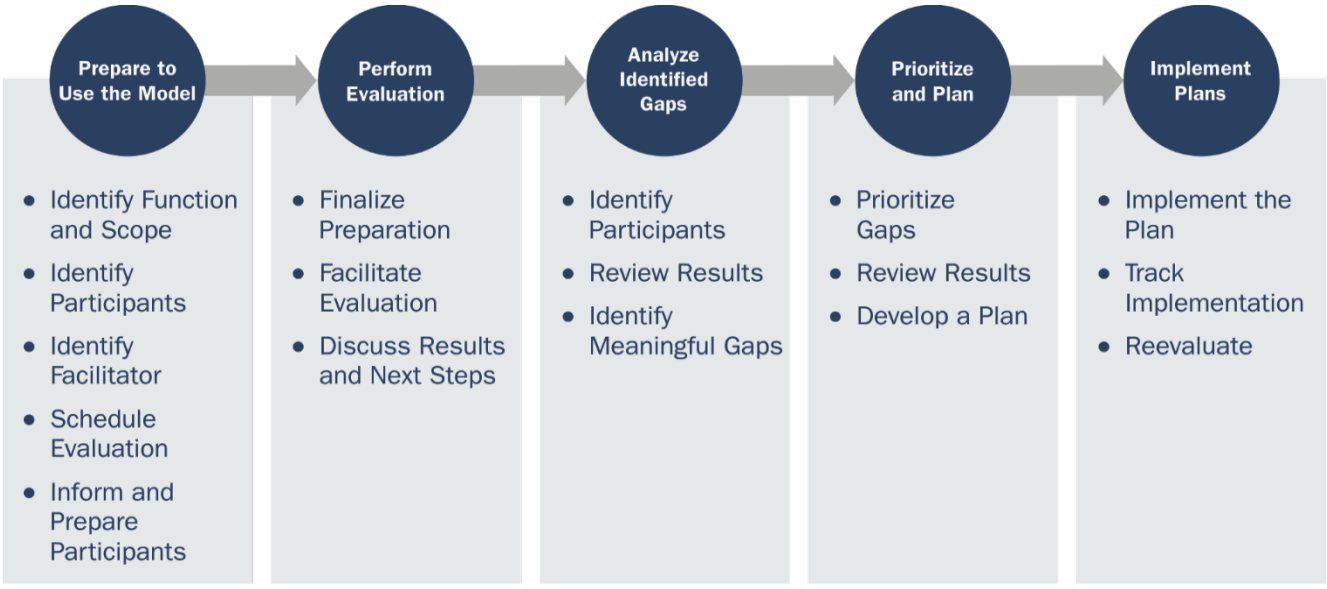
The *Dams Cybersecurity Capability Maturity Model* (Dams-C2M2) was developed by owners and operators and government stakeholders in the Dams Sector Cybersecurity Working Group at the direction of the Dams Sector Joint Council. The model aims to advance the practice of cybersecurity risk management by providing all Dams Sector organizations, regardless of size or type, with a flexible tool to help them evaluate, prioritize, and improve their own cybersecurity capabilities. This *Dams Sector C2M2 Implementation Guide* provides options for implementing the Dams-C2M2 in a systematic manner. Once implemented, the Dams-C2M2 can be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments.

How to Use the Dams-C2M2 Implementation Guide

The Dams-C2M2 recommended process for using the model involves five steps, as shown in Figure 1. This Implementation Guide is organized into those steps. The guide highlights approaches to implementing both the administrative and substantive elements of each of the five steps of the model process, taking into account the actions and perspectives of the organization, facilitator, and participants. The approaches are presented as considerations, ranging from simple to complex, which can be selected by the organization based on its structure; available personnel and financial resources; and current processes related to planning, gap analysis, and project management.

Organizations implementing the Dams-C2M2 should first read the Dams-C2M2 document to become familiar with the model's contents and definitions. The sequential application of the Implementation Guide can help owners and operators implement the model and document decisions made throughout the process. The templates included in the appendices are intended to aid in data collection, analysis, and decision documentation. They can be tailored by the organization based on its structure, resources, needs, and current processes (e.g., adjusting document formatting to landscape; increasing column and row sizes to allow for more note-taking space; or adding columns, rows, or additional space for other content). The Dams-C2M2 is available at www.dhs.gov/publication/dams-c2m2 and Microsoft Word versions of the templates are available for download from the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Dams Portal or upon request from the Dams Sector-Specific Agency (dams@hq.dhs.gov).

FIGURE 1. Recommended Process for Implementing the C2M2



The following briefly summarizes the elements of the five Dams-C2M2 implementation steps. Additional information on the various approaches and templates available to owners and operators is found in Chapters 1–5.

Prepare to Use the Model: The organization plans for the model's effective and efficient implementation. Approaches to preparation include selecting the function and scope against which to apply the model, choosing the most appropriate participants related to the function being evaluated, selecting an evaluation facilitator knowledgeable about the C2M2 and the selected function, scheduling the evaluation, and informing and preparing the participants. The appendices include a list of participant types and their roles, a pre-evaluation reference checklist to gather documents and information needed to perform the evaluation, and read-ahead and homework worksheet templates for inviting participants to and preparing them for the evaluation.

Perform an Evaluation: The organization conducts the evaluation to identify maturity indicator levels of cybersecurity practices, discuss successes and gaps related to the practices, and record decisions and associated discussion. Approaches to performing the evaluation include setting up the location, conducting the evaluation, and presenting and discussing initial results and next steps. The appendices include an evaluation preparation checklist to set up the location, a list of C2M2 domains and maturity indicator levels to be used by participants as an easy reference during the evaluation, and two templates—a maturity profile table and a maturity level selection worksheet—to document evaluation decisions and associated discussions about successes and gaps.

Analyze Identified Gaps: The organization reviews the results of the evaluation to identify gaps between where the organization currently stands in cybersecurity maturity and the desired level of maturity. The gaps are then analyzed to determine their significance to the organization. Approaches to analyzing gaps include selecting an appropriate group of personnel to conduct the analysis, reviewing the evaluation outputs to become familiar with the maturity profile decisions and discussions about the identified gaps, and strategically down-selecting the gaps to a manageable grouping to be later prioritized for action. The appendices include a gap mitigation plan template for documenting the gaps selected during the analysis.

Prioritize and Plan: The organization assesses the maturity gaps to determine their priority (i.e., the order in which gaps should be mitigated) and develops a mitigation plan. Approaches to prioritizing and planning include developing a prioritized list of gaps based on criteria selected by the organization and ensuring the mitigation plan includes distinct actions to address those gaps. The gap mitigation plan template can be further refined by recording mitigation action details (e.g., summary, milestones, cost estimate, person responsible).

Implement Plans and Periodically Reevaluate: The organization enacts the Gap Mitigation Plan to address prioritized gaps and periodically reevaluates the plan to maintain C2M2 focus and relevance. Approaches to implementation include leveraging established strategic planning processes—or adopting suggested processes—to allocate resources to the mitigation actions, clearly define the scope of the actions, manage the implementation, and track progress based on established metrics and timelines. Reevaluating the Gap Mitigation Plan or maturity profiles takes place when mitigation actions are implemented, business objectives change, and/or the risk environment evolves. The supporting templates noted in the previous step (Prioritize and Plan) are leveraged again for implementation and reevaluation.

About the Dams-C2M2

The Dams-C2M2, depicted in Figure 2, was developed to address the distinct operational characteristics of the Dams Sector. The model is a highly flexible tool that owners and operators can *choose* to use in one or more ways:

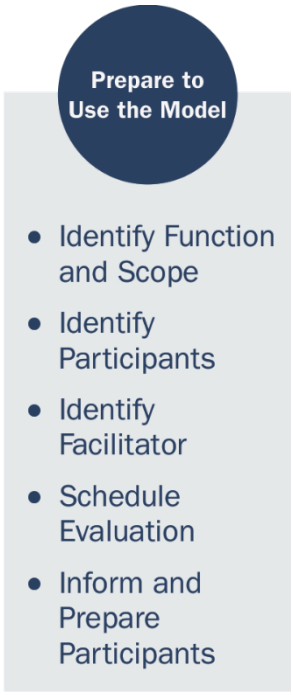
- Identify a progressive, step-wise approach to building strong cybersecurity capabilities, based on industry-wide best practices, existing standards, and cross-sector cyber expertise.
- Effectively evaluate and benchmark cybersecurity capabilities in a clear and organized way.
- Prioritize step-wise actions and investments to improve cybersecurity.
- Consistently measure and demonstrate progress over time toward organization-specific goals.

The Dams-C2M2 is not designed to issue a grade or a rating to an organization's cybersecurity program.

FIGURE 2. Dams-C2M2 Overview

1. Prepare to Use the Model

The Dams-C2M2 (also referred to in this document as the model) is intended to enable Dams Sector owners and operators to complete a self-evaluation of the cybersecurity maturity for a single function—a subset of operations within the facility or organization. The evaluation consists of a facilitated discussion to select maturity indicator levels (MILs) by knowledgeable participants familiar with the function and the analysis of the discussion's results. To adequately and effectively implement the model, careful planning should be undertaken prior to committing to the C2M2. While such planning is critical to a successful evaluation, the subsequent analysis and prioritization steps of the C2M2 implementation process also require thoughtful preparation.



Sample Approaches

Owners and operators are likely to approach their preparation for implementing the C2M2 in different ways, depending on the organization's available resources, risk profile, and knowledge of the model and implementation process. For some organizations, the entire process (including preparation, evaluation, gap analysis, prioritization, and mitigation planning) may occur relatively quickly, with few participants involved. For other organizations, implementing the model may require multiple planning meetings, days of evaluation, and follow-up actions, with many participants involved. Major steps to preparing to use the C2M2 include identifying the function and scope of the evaluation, identifying the appropriate participants, identifying a qualified facilitator to lead and guide the participants, scheduling the evaluation, and preparing the participants to effectively contribute to the evaluation. Owners and operators may choose from the sample approaches included in this chapter to execute these major steps.

Identify Function and Scope

Selecting the function—the subset of operations performed by the organization to which the C2M2 is being applied—is a key early step in implementing the model. The function is an important process, system, or operation the organization intends to evaluate for cybersecurity maturity. The scope limits the focus of the evaluation to logical boundaries for defining what is and is not included in the evaluation of the function. Setting the evaluation scope is essential for an organization to effectively use the C2M2 because the scope defines the context in which to evaluate cybersecurity maturity and ensures consistency throughout the implementation process.

- Function–Organizational Boundaries: The function might be defined by organizational boundaries such as a department, a line of business, or a facility. These are lines of separation familiar to the organization and that allow for relatively simplified scoping (e.g., physical security surveillance, or purchasing information and records).
- Function–Common System or Technology: The function might comprise a common system or technology used across organizational boundaries. Examples include the organization's enterprise IT services, including email, Internet connectivity, and voice over Internet protocol (VOIP) telephony.

Function and Scope

Function: Subset of operations to be evaluated for cybersecurity maturity. May be a specific department, line of business, facility, common system, or technology. Owners and operators might choose to strategically focus on those functions relevant to higher-profile cybersecurity risks.

Examples: Operation of facility floodgates, facility control center IT systems, access management system

Scope: Logical boundaries to limit the focus of the evaluation. May be limited to one facility, process, or system.

Examples: Local facility and control center, local facility network (i.e., not remote networking), regulatory compliance-related

- Scope–The scope may be influenced by steps already taken to ensure security of information technology (IT) and operational technology (OT) infrastructure. Examples include an existing enterprise risk management strategy, an existing framework for managing risks, and provisions for identifying critical assets and systems (these may relate to regulatory compliance or common business practices). Because the C2M2 evaluation measures the maturity of cybersecurity capabilities, existing policies and procedures—and operations subject to these policies and procedures—are strong candidates for inclusion in the scope.

Identify Participants

Selecting the appropriate personnel to participate in the evaluation is another important early C2M2 implementation step. Broad representation across the parts of the organization involved in the function to be evaluated yields the best results and enables internal information sharing about the cybersecurity practices. Participants should include operational personnel, management stakeholders, and any others who could provide useful information about the organization's performance of cybersecurity practices.

- Personnel: In general, pertinent personnel include those responsible for IT and OT security (e.g., network engineers, control operators and engineers, security engineers, compliance personnel, and vendors that are integrated into the business environment). Appendix B. Roles of Evaluation Participants provides descriptions of those involved in a typical C2M2 evaluation.
- C2M2 Relevance: Selecting participants based on the C2M2's structure can support effective implementation of the model. Reviewing the domains, objectives, and practices within the C2M2 may help determine who should participate in the evaluation to help determine which cybersecurity practices are complete. For example, if an organization employs a risk management (Domain 1) manager or division, those personnel would be valuable participants or contributors. These participants may be easily identified by reviewing the Maturity Level Selection Worksheet (Appendix E) and determining who is most appropriate to help select which practices the organization has completed.
- Business Units: Selecting a representative from each business unit related to the function to be evaluated (e.g., supply chain, contracting, purchasing, and senior management) can help ensure the sources of input to the model are comprehensive and the results are credible and broadly relevant.
- Sponsor: A sponsor to support C2M2 implementation within the organization can contribute a broad understanding of the function's components and status and suggest or solicit participation from others who would provide valuable input.

Not all organizations contain these suggested personnel types. The organization's personnel composition depends on its size, structure, and available resources. Therefore, organizations can choose the most appropriate participants with roles or duties similar to the suggested types.

Identify Facilitator

Though the C2M2 is intended to guide an organization in a self-evaluation of its cybersecurity maturity, a facilitator can be useful in guiding the participants through the implementation of the model. The basic skills of a facilitator consist of good meeting leadership practices: timekeeping, following an agreed-upon agenda, and keeping a clear record of the discussions. The higher-order skills involve observing the group and its individuals in light of group dynamics. 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 lessening it. In the event that a consensus cannot be reached, the facilitator should assist the group in understanding the differences that divide it.

The major delineation between approaches to identifying a C2M2 facilitator is the selection of a professional within or outside the organization. This choice might be predicated on purely economic reasons—an organization may not have resources available to hire an external facilitator.

- Internal Facilitator: Current personnel familiar with the function to be evaluated could serve as effective facilitators, if they clearly possess the qualifying skills and knowledge. However, the facilitator should not also serve as a participant in the evaluation, as this could slow down or complicate the process of implementing the C2M2. The internal facilitator should not be directly involved in the function being evaluated; organizations should exercise caution to avoid the possibility of an internal facilitator's instilling positive bias into the evaluation.
- External Facilitator: Hiring an external facilitator with experience supporting organizations' implementation of the C2M2 might be advantageous. In addition to having an unbiased and effective approach, an external facilitator could expedite the C2M2 process by guiding the participants relatively quickly through implementation. Potential sources for external facilitators include private consulting companies, industry associations (for dams or utilities), local or regional dams or utilities that have implemented the C2M2, or the U.S. Department of Energy. Non-disclosure agreements are commonly employed to protect sensitive information when an external facilitator is selected.

Schedule the Evaluation

Scheduling the evaluation includes selecting when to run the evaluation and for what duration.

- Strategic Considerations: The evaluation may take place prior to an upcoming budget cycle (i.e., to identify and justify needed investments); prior to implementing technology or policy changes; in preparation for another site visit, assessment, or inspection by a Federal, State, or local agency; or to coincide with another event (e.g., training).
- Date and Time Selection: A primary consideration for organizations undertaking the evaluation is how long participants will need to complete their review of all 37 objectives across the ten cybersecurity domains. While the evaluation was designed to be completed in an average of two days, the actual duration depends on a number of factors, including the number of participants and their knowledge of the C2M2, the complexity of the function being evaluated, the facilitator's effectiveness, and whether homework was assigned and completed. The following sample approaches can help an organization determine whether a one- or two-day evaluation is most appropriate:
  - One-Day Evaluation: This approach is appropriate when the organization invited fewer than ten participants and/or is familiar with the C2M2 model and implementation process, a simple function is being evaluated, the facilitator conducting the evaluation is familiar with the model, and/or homework was assigned and completed.
  - Two-Day Evaluation: This approach is appropriate when the organization invited more than ten participants and/or is new to the C2M2 model and implementation process, a complex function is being evaluated, the facilitator conducting the evaluation is unfamiliar with the model, and/or no homework was assigned or completed.

Inform and Prepare the Participants

Prior to performing the evaluation, it is prudent that all participants become familiar with the C2M2 model and implementation process, especially if the evaluation will bring together people from different parts of the organization and with diverse roles. Planning calls and read-ahead materials (possibly including homework) are effective mechanisms to communicate with participants about the evaluation and their role, as well as answer questions about the model and/or implementation process.

- Planning Calls: Two or three planning calls can facilitate administrative decisions that ensure a smooth evaluation and educate participants about the C2M2 model, how to prepare for the evaluation, the evaluation process, and identifying and mitigating gaps in cybersecurity maturity. The evaluation sponsor and/or facilitator can determine how many calls to schedule, when to conduct them, who should participate, and what topics to cover. Sample topics include:

- Identify the function and scope to be evaluated.
- Select participants, observers, and note taker(s).
- Determine the duration (i.e., one or two days), date, and time of the evaluation.
- Finalize room setup and technology needs.
- Gather documents to reference during the evaluation (see Appendix C for a checklist).
- Review and approve evaluation materials (e.g., agenda, read-ahead) (see below and Chapter 2).
- Review the C2M2 model and terminology with participants (see C2M2 Chapters 5 and 7).
- Assign homework to help participants to become familiar with the model and how to apply it to the function being evaluated (see below).
- Develop the organization's definition of Fully Complete, Largely Complete, Partially Complete, and Not Complete practices (see Chapter 2).
- Guide participants through the model's application by practicing selecting the actual and target MIL for one objective.
- Identify criteria for determining which gaps are meaningful to the organization (see Chapter 3).
- Identify criteria for prioritizing gaps identified through the evaluation (see Chapter 4).

- Read-Ahead Materials: Documents valuable to understanding the C2M2 are disseminated to all the participants prior to the scheduled evaluation, providing adequate time for their review. Key documents include a save-the-date notice, evaluation agenda, Dams-C2M2 (especially Chapters 5 and 7), Evaluation Read-Ahead (Appendix D), and Maturity Level Selection Worksheet (Appendix E). The evaluation sponsor and/or facilitator can determine when to disseminate the materials and whether homework will be assigned to participants.
- Homework: In addition to reading about the model, understanding how to apply it will yield a more efficient evaluation. Participants can complete homework to practice the process of reviewing domains and objectives, then select completed practices and MILs. The evaluation sponsor and/or facilitator can determine whether to have all participants pre-select MILs for all objectives or to assign portions to specific participants (e.g., divide up the model by domain and ask divisions with responsibility or expertise in domain topics to pre-select actual and target MILs for those domains). The Maturity Level Selection Worksheet includes instructions for completing this homework.

2. Perform an Evaluation

Following the detailed planning and preparation discussed in Chapter 1, the sponsor, facilitator, and participants gather to conduct the evaluation in a workshop setting. The evaluation entails the participants' assessing cybersecurity maturity across ten cybersecurity domains (logical groupings of cybersecurity practices) and the discussion of results and next steps.

Sample Approaches

Important steps for performing a C2M2 evaluation include preparing the location where the evaluation will be conducted, facilitating the evaluation to identify and record cybersecurity practice maturity data, and reviewing the preliminary results generated by selecting MILs.

Finalize Preparation

Before the evaluation is conducted, the facilitator and any support staff ensure that the meeting space is adequately configured and provisioned for a productive evaluation. Appendix F provides a detailed checklist of final preparation tasks.

- Prepare Location Equipment: Prior to the evaluation, it is important to ensure management support for use of the organization's rooms, furniture, equipment, and other provisions that might be needed for the evaluation. These items can then be acquired and configured appropriately (e.g., setting up equipment and rearranging tables and chairs). Common evaluation equipment includes computers, projectors, screens, flip charts, and white boards. Primary considerations for setting up the meeting space include:
  - Sufficient seating is available for all expected participants and any observers.
  - The room is set up to facilitate dialogue among participants (i.e., boardroom, not classroom, format).
  - 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 visible.
  - Documents useful for the evaluation have been printed in advance.

Documents to Print for the Evaluation

- Evaluation Agenda
- Evaluation Attendance Sheet
- Dams-C2M2 Chapter 7. Model Domains
- Dams-C2M2 Glossary
- Appendix E. Maturity Level Selection Worksheet
- Appendix G. C2M2 Domains and Maturity Indicator Level Reference Sheet
- Appendix H. Maturity Profile Table
- Appendix I. Gap Mitigation Plan

- Balance Evaluation Tools: It is important to consider an appropriate balance of evaluation tools for the participants and the function to be evaluated. Depending on the function and the familiarity of participants, technology-based tools (e.g., computers and software, projectors and screens, and monitors) and manual tools (e.g., flip charts, white boards, notecards, and markers) might be employed. Generally, a variety of technological and manual tools should be available to encourage dialogue and discussion during the evaluation. To ensure the effective use of these evaluation aides, the tools (especially the technological tools) should be tested prior to the evaluation for proper operation.

Facilitate the Evaluation

Conducting the evaluation broadly involves opening with a welcoming statement and an overview of the C2M2 model, followed by progressing through the model to evaluate the maturity of cybersecurity practices for the function. The facilitator guides the participants through the model and discussion, and a member of the evaluation team records decisions and discussion points.

Sample Evaluation Agenda

- Welcome Remarks
- Opening Discussion
- MIL Selection for Domains, Objectives, Practices
  - Actual MILs
  - Target MILs
- Results
  - Maturity Profile
  - Successes
  - Gaps
- Next Steps
  - After-Action Report Development
  - Gap Analysis

- Welcome Remarks and Opening Discussion: The beginning of the evaluation is an opportune time to ensure that the participants are prepared for and comfortable during the evaluation. It is often useful to begin with comments from senior management to emphasize the importance of the C2M2 to the organization, identify the business drivers for a cybersecurity effort, and highlight the importance of active participation in the evaluation. Common topics that warrant emphasis in the opening discussion include:
  - C2M2 Definitions: Define key terms that will be used throughout the evaluation (e.g., function, domain, objective, MIL, levels of completeness).
  - C2M2 Process: Walk through the model, explain how the participants will review and select MILs, and describe the desired outcomes of the evaluation. Figure 2 in this document can be used to display and discuss the model.
  - Organization's Vocabulary: Identify consistency and conflicts between terms used by the organization and the C2M2.
  - Function and scope: Remind participants that the evaluation is being applied to a specific set of operations performed by the organization.
  - Organization's Environment: Discuss the organization's business and operating environment and/or show pictures of cyber components to add context to the description of the function being evaluated.
- Guide Participants through the Model: The facilitator leads the participants through each of the ten domains, associated objectives and practices, and MIL options. The following process is suggested to engage the participants in a discussion. The same process is used for identifying actual MILs and successes, immediately followed by identifying target MILs and gaps. The organization may discuss and select actual and target MILs separately, but this approach may take longer than one day to complete.
  - Display the Maturity Level Selection Worksheet (Appendix E) on the evaluation screen. This enables participants to efficiently review the practices included in each objective, select the appropriate MILs, and discuss these decisions. Chapter 7 of the Dams-C2M2 includes summary language that can be used to display and describe the domains and objectives, as well as tables inclusive of resources that can help select MILs and fill gaps. The Dams-C2M2 Glossary can be used to answer questions about definitions of domains, objectives, and cyber terminology.
  - Proceed progressively through the model's ten domains, each of which contains objectives that represent achievements to support the domain. Within each objective are up to four MILs (MIL0 through MIL3) containing a structured set of cybersecurity practices that represent the activities an organization can perform to establish and mature capability in the domain. See Figure 2 in the Introduction for a visual depiction of the model.
  - Display and read the objective, review the practices associated with each of the MILs, and ask the participants to confirm which practice(s) within the objective have been completed.

Participants can choose from four levels of completeness: Fully Complete, Largely Complete, Partially Complete, and Not Complete. The organization should define these terms prior to the evaluation (e.g., on a planning call), highlight them during the opening discussion, apply the definitions consistently across all objectives, and include the definition of each in the after-action report (AAR) summary. A sample approach to writing an AAR is provided below.

- Document the selection of completed practices using the check boxes included in the Maturity Level Selection Worksheet. Only practices noted as Fully Complete or Largely Complete should receive a checkmark. Partially Complete and Not Complete remain unchecked as an indication of gaps to be filled.
- Engage the participants in a discussion about specific actions the organization implemented to complete the practices and thereby achieve the actual MIL. Document these successes as evidence to support each completed practice selection in the notes column included in the Maturity Level Selection Worksheet. Examples of evidence include summarizing why the practice is fully or largely complete (including assumptions made), citing a specific document pertaining to that practice (e.g., a plan or strategy), summarizing the organization's specific actions pertaining to that practice (e.g., cyber exercises and training), and noting who is responsible for the actions.
- Ask participants to select the *actual* MIL that best represents the completed practices. To earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level(s). Note that a MIL of zero is indicated for an objective if any of the practices for MIL1 are not complete. Document this decision in the Maturity Level Selection Worksheet and Maturity Profile Table. See Figure 3 for a visual representation of these documents and tips for selecting MILs.
- Ask participants to select the *target* MIL that best represents the organization's desired state for that objective, based on the organization's priorities and/or which practices in higher-order MILs have been completed. Remind participants that striving to achieve the highest MIL in all domains may not be optimal. Practice performance and MIL achievement should align with the organization's business objectives and cybersecurity strategy. Document this decision in the Maturity Level Selection Worksheet and Maturity Profile Table.
- If the organization has not achieved the target MIL, engage the participants in a discussion identifying gaps between the actual and target MILs and actions the organization should implement to complete the additional practices needed to achieve the target. Document these gaps in the notes column of the Maturity Level Selection Worksheet. Examples of gaps include summarizing why the practice is partially or not complete (including assumptions made), citing a specific document to be updated to complete the practice, summarizing the organization's future actions to complete the practice, and noting who is responsible for the actions.
- Count the number of MILs and practices required to achieve the target MIL. Document these numbers on the Maturity Profile Table.
- Throughout the discussion, confirm with participants that they concur with the MIL determinations and ask whether they have additional input on successes and gaps. Help participants work through disagreements about MIL selections.

Interactive dialogue is important for the effectiveness of the C2M2, and participants are encouraged to ask questions, use visual aids (e.g., flip charts, white boards, and markers), and seek support from subject matter experts for clarification, depth, or nuance on the topics under discussion. At times the facilitator might remind participants to focus not on the specific phrasing of a practice, objective, or MIL but rather on the intent behind the term. Chapter 7 and the glossary in the Dams-C2M2 can be useful in supporting this understanding.

FIGURE 3. Maturity Level Selection and Documentation

Maturity Profile Table

Domain	Objective	Actual MIL	Target MIL	# of MILs to Meet Target	# of Practices to Meet Target
1. Risk Management	Establish Cybersecurity Risk Management Strategy				
	Manage Cybersecurity Risk				
	Management Activities				
2. Asset Identification, Change, and Configuration Management	Manage Asset Inventory				
	Manage Asset Configuration				
	Manage Changes to Assets				
	Management Activities				
3. Identity and Access Management	Establish and Maintain Identities				
	Control Access				
	Management Activities				

Maturity Level Selection Worksheet

Domain 1: Risk Management

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Establish Cybersecurity Risk-Management Strategy				
MIL1	No practices.			
MIL2	☐ a) There is a **documented** cybersecurity risk-management strategy. ☐ b) The strategy **provides an approach** for risk prioritization, including consideration of effect.			
MIL3	☐ c) Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on effect, tolerance for risk, and risk response approaches) are **defined and available**. ☐ d) The risk-management strategy is periodically **updated** to reflect the current threat environment. ☐ e) An organization-specific risk taxonomy is **documented** and is used in risk-management activities.			
2. Manage Cybersecurity Risk				
MIL1	☐ a) Cybersecurity risks are **identified**. ☐ b) Identified risks are **mitigated, accepted, tolerated, or transferred**.			

Four aspects of the MILs are important for understanding and applying the model:

- **The MILs apply independently to each objective.** As a result, an organization using the model may be operating at different MIL ratings for different objectives. For example, an organization could be operating at MIL1 for one objective, MIL2 for another objective, and MIL3 for a third objective.
- **The MILs are cumulative within each objective.** To earn an MIL for a given objective, an organization must perform all of the practices in that level and its predecessor level(s). For example, an organization must perform all of the objective practices in MIL1 and MIL2 to achieve MIL2 for the objective. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
- **Establishing a target MIL for each objective is an effective strategy for using the model to guide cybersecurity program improvement.** Organizations should become familiar with the practices in the model prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.
- **Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy.** Companies should evaluate the costs of achieving a specific MIL against potential benefits rather than focusing on achieving the highest MIL. However, the model was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

- Document Evaluation Decisions and Discussion: As shown in Figure 3, the Maturity Profile Table Template (Appendix H) and the Maturity Level Selection Worksheet Template (Appendix E) provide consistent and streamlined tools to collect evaluation data. While the facilitator is guiding participants through the C2M2, a member(s) of the evaluation team documents the decisions and discussion in the templates, as noted above in the section titled Guide Participants through the Model. Both templates are aligned to the C2M2's ten domains and associated objectives.
    - The Maturity Profile Table captures *decisions* about the actual and target MILs and the number of MILs and practices needed to achieve the target. If the organization chooses to reevaluate the function in the future (see Chapter 5), the results of the reevaluation can be compared to this table to demonstrate progress.
    - The Maturity Level Selection Worksheet captures the *discussion* of the evaluation, including evidence of successes leading to the actual MILs and gaps to be mitigated to achieve the target MILs. Documenting these details can help ensure future reviews of the evaluation results are understood, especially by a reviewer who was not an evaluation participant.

  The completed Maturity Profile Table and Maturity Level Selection Worksheet become primary components of the gap mitigation process and an AAR as a consolidated and complete record of the C2M2 evaluation. A sample approach to writing an AAR is provided below.

- Information Security: The information discussed, documented, and shared among those participating in the C2M2 process may include sensitive information that the organization would wish to protect from unauthorized access. Therefore, organizations are encouraged to use their own established policies, designations, and document markings for information security (e.g., For Official Use Only, Business Sensitive, Internal Use, Privileged, Confidential, Private, or Secret). See Chapter 5 Information Security Practices of the *Dams Sector Security Guidelines* for more detail on information security and designation.

Discuss Preliminary Results and Next Steps

Following the selection of MILs across the ten domains and their recording in the Maturity Profile Table and Maturity Level Selection Worksheet, the participants discuss the results of that effort and next steps leading from the evaluation. The facilitator summarizes the selected MILs, successes, and gaps and leads a discussion to confirm the organization's cybersecurity maturity profiles. Participants review the current profile (i.e., actual MILs) and the capability profile (i.e., target MILs) and prepare for the examination of those profiles to identify, analyze, prioritize, and mitigate gaps.

- Summarize Results: After MILs for the tenth domain have been selected and recorded, the facilitator displays the Maturity Profile Table to highlight the target MIL and actual MIL for each objective of each domain and the number of MILs and practices needed to achieve the target MIL. The facilitator highlights primary successes and gaps offered during the evaluation and recorded on the Maturity Level Selection Worksheet. Participants are asked to reconfirm the MILs they selected, as well as provide any additional input on successes supporting actual MILs and gaps between actual and target MILs. If additional input or feedback is given, or MILs are changed, that information is added to the Maturity Profile Table and Maturity Level Selection Worksheet.

- Confirm Maturity Profiles: Displaying the Maturity Profile Table can allow for a clear and concise visual summary of MILs selected during the evaluation. The collection of actual MILs per objective and domain represents the organization's current profile. This is a snapshot in time of the maturity of the organization's cybersecurity practices for the function that was evaluated. Similarly, the collection of target MILs represents the organization's capability profile. The capability profile indicates the level of maturity the organization desires to achieve for the cybersecurity practices of the function. Together, these profiles, the Maturity Level Selection Worksheet, and/or the draft AAR form the basis for the organization to:

- Identify and analyze gaps between actual and target MILs (see Chapter 3).
- Prioritize the gaps and develop a plan to address them (see Chapter 4).
- Turn the plan into action and evaluate progress toward its completion (see Chapter 5).

The initial discussions of successes in actual MILs and gaps between actual and target MILs will prepare those who, post-evaluation, will work toward improving the cybersecurity maturity of the function.

- Write the After-Action Report: The AAR summarizes key information related to the evaluation and includes gap analysis, prioritization, and mitigation planning. The organization may choose when to draft the AAR: after the C2M2 evaluation is concluded but prior to the gap analysis or after both steps are completed. The length, format, and development timeframe of the AAR depend on the amount of discussion (about domains, objectives, MILs, successes, and gaps), the organization's preferred format, availability of the person responsible for drafting the document, and scheduling of the session to analyze the identified gaps. A typical AAR includes several components:
  - Overview: Basic evaluation information, such as the date(s), scope (the function evaluated), outcome(s), an overview of participants and how they were selected, and the name of the sponsor and point of contact. This information may be copied from the Evaluation Read-Ahead (Appendix D).
  - Executive Summary: Summary of additional details important for the organization to communicate about the evaluation, as a supplement to the full results. Options include the business case for implementing the C2M2, process used for the evaluation, methodology/assumptions used to select complete practices, criteria selected to identify meaningful gaps and prioritize gaps, overall results of the C2M2, gap prioritization and mitigation planning details, points of contact, and a scheduled or projected time for reevaluation. This summary could also be used in a stand-alone document for sharing the process, results, and next steps with others who are important to implementing the gap mitigation actions.
  - Results–Maturity Profile: A snapshot of the decisions made during the evaluation, including the target/actual MIL selections and the number of MILs and practices needed to reach target MILs. This may be copied from the Maturity Profile Table (Appendix H), which is used to document decisions during the evaluation.
  - Results–Supporting Evidence: Full details summarizing the discussion that supported the decisions made during the evaluation. Two templates are available to record this information, depending on the organization's preference (see Figure 4 for images of these options):
    - Worksheet Format: List of evidence supporting complete practices and gaps associated with incomplete practices, based on the Maturity Level Selection Worksheet (Appendix E) used during the evaluation. This format is appropriate for organizations that generally do not develop report-based documents, prefer a more direct progression from materials used during the evaluation to reporting results, and/or have less time and staff resources to translate the evaluation results into a report.
    - Report Format: Narrative-based report that highlights successes and gaps associated with each objective. The Microsoft Word template is available for download from the HSIN-CI Dams Portal or upon request from dams@hq.dhs.gov. This format is appropriate for organizations that regularly develop report-based documents, prefer a more analytical approach to summarizing the successes and gaps across MILs, and/or have time and staff resources available to translate the evaluation results into a report.

- Gap Mitigation Plan: Result of the Prioritize and Plan step in the C2M2 model (see Chapter 4 for more information on this step).
- Attendance List: A list of evaluation participants and their affiliations.

The draft AAR is provided to the evaluation sponsor, who distributes it to participants for review and validation that the content is complete and correct. The draft can be used to analyze gaps and prioritize mitigation actions, which are then entered into the Gap Mitigation Plan component of the AAR. Once the participants validate the content and the Gap Mitigation Plan is completed, the AAR is considered final as the official record of the C2M2.

FIGURE 4. After-Action Report Results Section: Format Options

Maturity Level Selection Worksheet

Domain 1: Risk Management

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Establish Cybersecurity Risk-Management Strategy				
MIL1	No practices.			
MIL2	☐ a) There is a **documented** cybersecurity risk-management strategy. ☐ b) The strategy **provides an approach** for risk prioritization, including consideration of effect.			
MIL3	☐ c) Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on effect, tolerance for risk, and risk response approaches) are **defined and available**. ☐ d) The risk-management strategy is periodically **updated** to reflect the current threat environment. ☐ e) An organization-specific risk taxonomy is **documented** and is used in risk-management activities.			
2. Manage Cybersecurity Risk				
MIL1	☐ a) Cybersecurity risks are **identified**. ☐ b) Identified risks are **mitigated, accepted, tolerated, or transferred**.			

Narrative After-Action Report

Domain 1: Risk Management

Objective 1: Establish Cybersecurity Risk Management Strategy

Successes

Meeting the target MIL can be attributed to the following successes:

Success 1: [Observation statement]

Success 2: [Observation statement]

Gaps to Mitigate

The following areas require improvement to achieve the target MIL:

Gap 1: [Clearly state the problem or gap. Reference relevant plans, policies, procedures, regulations, or laws. Provide a root cause analysis or summary of why the target MIL was not achieved.]

Gap 2: [Clearly state the problem or gap. Reference relevant plans, policies, procedures, regulations, or laws. Provide a root cause analysis or summary of why the target MIL was not achieved.]

Objective 2: Manage Cybersecurity Risk

Successes

Meeting the target MIL can be attributed to the following successes:

Success 1: [Observation statement]

Success 2: [Observation statement]

3. Analyze Identified Gaps

The completion of the C2M2 evaluation and the establishment of maturity profiles (current and capability) allow the organization analyze its cybersecurity maturity for the selected function. Through analysis of the evaluation results, gaps between where the organization currently stands in cybersecurity maturity and the desired level of maturity are readily identified. Once identified, the gaps are analyzed to provide the basis for determining which are meaningful and, of those, which should be prioritized.

Sample Approaches

Major steps to identifying and analyzing cybersecurity maturity gaps include selecting the appropriate group of personnel to identify and analyze the gaps in cybersecurity maturity, reviewing the results of the C2M2 evaluation to determine the gaps in cybersecurity maturity, and selecting those gaps most meaningful to the organization. The end result of this analysis is a collection of gaps that is used to guide the organization through the next step of the C2M2: prioritize and plan.

Identify Participants

After the participants have completed the C2M2 evaluation, a separate group of personnel (referred to as the post-evaluation group) coordinates the results of the evaluation and collaborates on identifying gaps between the organization's current and capability profiles. This group is generally smaller than the group of evaluation participants and includes key decision-makers relating to the objectives and practices of the function that was evaluated.

- Participant Responsibilities and Types: Those involved in identifying and analyzing gaps will make decisions that direct the organization's efforts to address cybersecurity maturity gaps. Generally, this group would include those personnel who are relevant to the evaluated function and who will be implementing the mitigation actions developed by the C2M2 process. Including both strategic and technical personnel is encouraged for a broad understanding of the objectives, practices, and gaps. Typical personnel types to consider include:
  - Senior-Level Management: Higher-level personnel (e.g., directors of divisions relating to the function or managers) can relate strategic issues and concepts to the identified gaps. Examples include top-level budget personnel or those occupying one step under top-level executives.
  - Operational Managers: Personnel with direct operational familiarity with the objectives and practices can be valuable for identifying and analyzing technically focused gaps. Examples include those overseeing divisions relating to the function or C2M2 domain and managers of the objectives and practices of the function.
  - Other Decision-Makers: Personnel with subject matter expertise and decision-making authority in other areas can provide deeper focus on some issues and alternative perspectives on others. Examples include supply chain, sourcing, or purchasing managers.

  Depending on its size, structure, and available resources, the organization may or may not employ all these suggested types of personnel. However, the organization can select the most appropriate personnel with similar attributes or duties.
- Facilitator: A facilitator for identifying and analyzing gaps might not be needed. The smaller group involved in this step is likely to navigate discussions and decisions without additional guidance. An external facilitator could actually prove an encumbrance, as the discussions of gaps and their importance could involve sensitive or proprietary information that the organization would not want to expose to outside parties. Requiring the facilitator to complete a non-disclosure agreement may alleviate this concern.

Senior leadership in the organization might require justification for committing personnel (likely some of the same personnel from the evaluation) to spend additional time on the C2M2. Rationales for this work include the relevance of gap analysis to strategic priorities, critical business functions, or regulatory compliance.

Review Results

Once the post-evaluation group has been selected to continue through the steps of the model, the evaluation results review can take place. The group might prefer to convene in a workshop setting immediately following the evaluation or may wish to conduct this step over time through multiple meetings. The primary sources of information to review are the Maturity Profile Table (Appendix H) and the Maturity Level Selection Worksheet (Appendix E), which will have been populated with all the relevant information from the evaluation. Reviewing these documents will allow the post-evaluation group to become familiar with the decisions and supporting discussion from the evaluation. Other documents to review include the list of strategic documents and reference material relating to the C2M2 objectives (Appendix C. Pre-Evaluation Reference Checklist).

- Review Maturity Profiles: As described in Chapter 2, the collection of actual MILs per objective and domain represents the organization's current profile, and the collection of target MILs represents the organization's capability profile. These are clearly displayed in the Maturity Profile Table. The post-evaluation group can readily compare the profiles to identify gaps, as well as review the number of MILs and practices required to achieve the target MIL (for those objectives in which the target MIL has not been met). The group might also identify the relevant reference material per objective to support the identification and analysis of gaps.
- Review Successes and Gaps: The discussions from the evaluation on successes supporting MIL acheivement and the gaps in paractices required to reach unmet MILs provide valuable context to the group's identification and analysis. This information will have been recorded in the Maturity Level Selection Worksheet.

Identify Meaningful Gaps

The current and capability profiles provide the fundamental basis for the identification and analysis of gaps. Specifically, the gaps exist where the actual MIL falls short of the target MIL. Selecting meaningful gaps from the full list of gaps is a practical step in narrowing the organization's focus on those gaps to prioritize for mitigation. Several options, ranging from simple to complex, are available to analyze the gaps and determine their approximate significance. An organization may choose to apply existing processes to identify meaningful gaps, or they can select from the options listed below. Reviewing and choosing the selection criteria prior to the evaluation may save time during the analysis of the evaluation results. The criteria are summarized in the AAR summary to document and explain this key decision of implementing the C2M2.

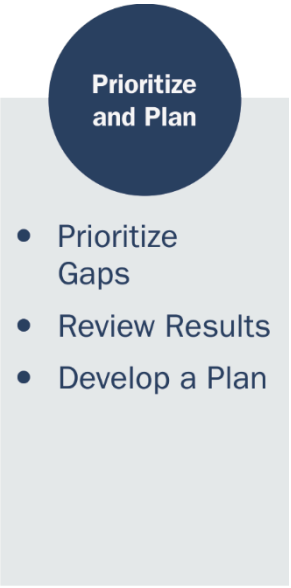
- Common Themes: Leveraging common themes from the evaluation discussion may be a simple and effective method to determine which gaps are meaningful to the organization. The facilitator can help to identify these themes and select gaps that cross multiple domains and/or objectives (e.g., training, exercises, or documenting plans).
- Domain-Level Selection: The organization may focus on gaps within domains that are deemed of highest importance by the post-evaluation group. Considerations for selecting specific domains include:
    - Domains with the most number of practices to complete before achieving the target MIL
    - Domains with the least number of practices to complete before achieving the target MIL
    - Domains that prompted the most discussion during the evaluation
    - Domains that the group deems important based on their understanding of their organization (e.g., alignment with strategies and plans, affecting critical business or operational functions, regulatory requirements, known threats or vulnerabilities)

- Practice-Level Selection: For organizations with additional time and resources to devote to gap analysis, reviewing the full list of practices yet to be completed (i.e., gaps) and applying more rigorous criteria may be an effective method to determine which gaps are meaningful to the organization. Considerations for selecting specific practices include:
    - Strategic Focus: A strategic analysis of gaps based on incomplete practices tied to the organization's risk management or cybersecurity strategies and plans, leadership priorities, or initiatives.
    - Technical Focus: Technical or operational practices relevant to specific risks (including threats, vulnerabilities, and consequences) that are deemed important to complete. Operational standards and guidelines will be important references for analyzing the practices to prepare for gap prioritization.
    - Low Level of Effort: In some cases, the organization may need to complete one or two practices to achieve their target MIL. In addition, some practices may be completed with existing people, processes, and technologies. Completion of these practices may easily achieve the target MIL for that objective.
    - High Level of Effort: The identified gaps might span many incomplete practices and/or multiple MILs (e.g., an actual MIL of zero for an objective with a target MIL of three). Such gaps may be especially important to complete if they relate to the cybersecurity of high-profile topics such as critical business operations, executive strategic priorities, or regulatory requirements.

Regardless of the analysis method, the resulting list of meaningful gaps should be documented in the Gap Mitigation Plan (Appendix I) for use in progressing through the next steps in the C2M2. A member of the post-evaluation group would record this information in the first four columns in the Gap Mitigation Plan Template. This identification and analysis of gaps is only the first step toward addressing the gaps and improving on current performance. Prioritization and planning (covered in Chapter 4) and implementation (covered in Chapter 5) are required to mature the organization's cybersecurity capabilities.

4. Prioritize and Plan

Organizations prioritize the gaps between their current and capability profiles in order to plan targeted mitigation actions to address those gaps. Limited time and resources require intelligent choices about which actions to pursue first to ensure deployment of a mature, robust cybersecurity management strategy. Prioritization that aligns with business objectives and understanding of risk informs the choices about actions. Planning actions improves the likelihood of effective implementation of new practices. Documentation, rationale, and ownership of projects can help build consensus and support for closing priority gaps.



Sample Approaches

Organizations are encouraged to use existing strategic planning processes to prioritize gaps and plan mitigation actions if those processes are already in place. If not, multiple commonly used options are available; these can be tailored to fit the organization's unique operations, personnel, risk environment, and business objectives. Whichever method for prioritization is used, a Gap Mitigation Plan guides the implementation of the selected priority gaps and mitigation actions.

Prioritize Gaps

Identifying the meaningful gaps, as outlined in the previous chapter, isolates significant issues an organization faces. Prioritizing these gaps helps an organization to make informed decisions about where and when to apply limited resources to mature cybersecurity capabilities. Organizations may choose to apply existing internal strategic planning processes to prioritize gaps, or they can select from the options below, which range from simple to complex. As with identifying meaningful gaps, reviewing and selecting this prioritization criteria prior to the evaluation may save time on this step. The option(s) selected is summarized in the AAR summary to document and explain this key decision of implementing the C2M2.

- Importance: Gaps may be organized into the categories of high, medium, and low by their perceived importance. The organization might consider impact on business objectives, impact on cybersecurity objectives, risk to critical infrastructure or equipment, and/or other factors significant to the business.
- Timeframe: Gaps may be organized by implementation timeframe by considering how rapidly the gap needs to be and can be resolved. For example, gaps could be organized as short-, mid-, and long-term.
- Quadrant: Examining both importance and timeframe might be more insightful than either criterion alone, as gaps can fall into one of four quadrants (i.e., high–short, high–long, low–short, low–long).
- Cost–Benefit Analysis: A cost–benefit analysis (CBA) takes a detailed look at the capital costs of potential actions and estimated benefits gained to compare actions by their predicted effect on future revenues. A CBA might be appropriate for organizations accustomed to using such analysis in regular business decisions.
- Weighted Analysis: An organization can develop quantifiable measures to assign numerical weights to the importance of addressing a gap. To gauge gaps using these criteria, organizations may want to identify the activities and resources needed to address the gaps to create a more robust data set for analysis.

The resulting classification of gaps for prioritization should be recorded in the "Prioritization" column of the Gap Mitigation Plan Template (Appendix I). These results are helpful inputs to the process of selecting gaps to mitigate.

Review Results

Reviewing the prioritization results in the Gap Mitigation Plan allows the organization to organize, sort, select, or highlight specific gaps or groups of gaps that are higher or lower in priority. This step may include sorting or rearranging the list of gaps into ordered categories. The ultimate aim is to select those for further development in the C2M2. At this point in the prioritization process, it may be useful for the organization to also review the list or groupings of gaps and priority categories to ensure that the results are congruent with the organization's expectations for the C2M2.

- Select Prioritized Gaps: Following the review of the prioritization results, the organization can choose those gaps with the highest priority to mitigate. The organization's available personnel and resources, as well as its strategic or executive goals, may be considered when raising or lowering the relative priority of gaps. Further, the judgment of senior management involved in the C2M2 might be the major driver of which gaps are selected as the highest priority. The selection of highest-priority gaps should be documented in the Gap Mitigation Plan.

Develop a Plan

The development of a Gap Mitigation Plan can be useful for articulating and addressing the prioritized gaps and, ultimately, for managing the maturation of the organization's cybersecurity capabilities. The organization may choose to incorporate the process of developing a Gap Mitigation Plan into its established strategic planning process. If one does not exist at the organization, or if the C2M2 model is run outside of the usual planning cycle, the process outlined in this Implementation Guide may be used. The primary components to consider include brainstorming and confirming mitigation actions that would address the selected gaps, determining key information needed to implement the actions (e.g., milestones, staff assignments, and resources), and designating an owner of the plan to track progress. The Gap Mitigation Plan Template (Appendix I) can be used to record this information. Regardless of the process used—an established strategic planning process or this Implementation Guide process—key information is recorded in the AAR to document this key decision of implementing the C2M2.

- Identify Mitigation Actions: The first step is to brainstorm at least one distinct mitigation action (or project) for gaps identified in the previous step as priorities. Each mitigation action ties directly to completing a practice/practices that enable the achievement of the target MIL. Depending on the prioritization categories used (e.g., high/medium/low or short-/mid-/long-term), the group can select which gaps will receive mitigation actions (e.g., only high-priority or short- and mid-term). Additional mitigation actions can be identified at a later date for lower-priority or longer-term gaps.
- Determine Milestones: A milestone is a significant event in a mitigation action that occurs at a point in time. For the purposes of the Gap Mitigation Plan, a start and end date for each mitigation action can be used to visualize the sequencing of the actions. In addition, the group may select a milestone for the plan itself, which would help signal the start of the reevaluation cycle. Plans can span a period of weeks, months, or years, depending on the extent of improvements needed to close the selected gaps and achieve the target MIL.
- Confirm Staff Assignments: Identifying the appropriate personnel required to implement each mitigation action contributes to the estimate of resources and facilitates gaining approval from the manager/managers for time allocated to the action.
- Estimate Cost: Based on the time and staff resources needed to implement the mitigation action, plus any capital investments required, a rough order of magnitude (or preliminary) cost estimate can be generated. The plan may also note the high-priority gaps for which resources are not yet available. While this estimate will most likely be adjusted as the plan is implemented, the collection of cost estimates for all actions can be valuable in sequencing activities based on realistic expectations and in communicating with management about the need for funding.

- Designate a Plan Owner: The plan owner is typically responsible for tracking progress, reporting to management, and initiating the reevaluation cycle (see Chapter 5). Selection of an appropriate staff member to fill this role is dependent on the organization's structure and/or the mitigation actions included in the Gap Mitigation Plan. If the organization created the plan through an established strategic planning process, the program management office or other planning office may be selected to manage plan implementation. Alternatively, the evaluation sponsor may find it valuable to manage the entire C2M2 process. Finally, if all mitigation actions are assigned to one division of the organization, the division manager may be designated to directly tie plan progress to division mitigation actions.

5. Implement Plans and Periodically Reevaluate

Organizations can implement the Gap Mitigation Plan developed to address the gaps identified and planned for in previous steps of the C2M2. Plan implementation improves the organization's cybersecurity capabilities and helps drive the evaluated function toward achieving the capability profile (i.e., target MILs). Tracking implementation of the Gap Mitigation Plan is an important step to ensure that the desired outcomes can be met on time and on budget. Periodic reevaluation is useful in allocating limited remaining resources and reviewing overall progress to keep the organization focused and on track.

Sample Approaches

Organizations with established frameworks for project management can utilize those existing processes to implement, track, and reevaluate the mitigation actions listed in the Gap Mitigation Plan. All organizations have several options for implementing and tracking plans, but these fundamentally rely on allocating the necessary resources—budget, personnel, and time—to successfully carry out requisite actions. A defined review period for the overall plan establishes a clear time for reevaluation of the progress made, while other factors may trigger earlier reevaluation.

Implement the Plan

The implementation of the Gap Mitigation Plan may proceed through an established strategic planning process. If the organization does not have a formal process or the C2M2 evaluation occurs outside the usual planning cycle, the process outlined in this Implementation Guide may be used. Key factors to consider when implementing the plan include allocating adequate and appropriate resources, communicating the desired milestones and outcomes to assigned staff, and managing the implementation process (e.g., setting schedules, establishing reporting formats, and communicating with both implementing staff and interested supervisory roles such as senior management or the board of directors).

- Allocate Resources: A detailed budget, proportioned to reach specific milestones, can clarify plan implementation. Human resources are equally important to successful implementation. Personnel with requisite skills will need sufficient time and support to complete practices. The organization can leverage a rough cost estimate, if one was developed along with the Gap Mitigation Plan (see Chapter 4 for additional information on this step). Otherwise, organizations may develop detailed timelines, identify staffing requirements, and identify any procurement requirements that would contribute to the project in order to better estimate overall project costs.
- Document Mitigation Action Details: Clearly defined parameters or boundaries of the mitigation action can help to communicate the ultimate objective of its implementation as well as to inform the staff that will participate in implementation. Limiting the focus and avoiding dilution of efforts (e.g., objectives expanding as the project progresses) can help prevent budget and schedule overruns.
- Manage Implementation: As discussed in the approach to Develop a Plan in Chapter 4, organizations have several options when selecting a plan owner. The primary responsibilities of the plan owner are to communicate with implementing staff about milestones, resources, and documentation and to report progress of all activities to senior management or the board of directors as needed. Regular communication with these supervisory roles can help to maintain buy-in and support throughout the implementation cycle. Finally, the plan owner may establish the timeline for a reevaluation of the plan or trigger such a reevaluation mid-cycle if deemed necessary.

Track Implementation

Tracking implementation of mitigation actions helps to ensure that progress is made towards the desired capability profile and allows an organization to course-correct before major issues arise. Well-defined milestones can be helpful in checking that implementation of mitigation actions remains on schedule and on budget. Frequent communication with implementing staff to gather status reports or review actions undertaken and regular reporting to senior management on overall progress may also be helpful in identifying and addressing barriers. Organizations may implement project tracking practices already in place, but any organization could consider the approaches outlined below.

- Baseline: The Gap Mitigation Plan (including milestones, timelines, and other details) may act as a baseline against which to compare actual progress during implementation. The plan owner can readily compare current status reported by implementing staff to the original plan to highlight deviation.
- Metrics: In general, the plan owner may define metrics for progress, such as resources expended to date, milestones met, or number of practices within an objective that have been completed. Leveraging the organization's existing project metrics and formats for reporting status (e.g., graphical displays or dashboards) can help to clearly communicate progress to interested stakeholders. Relating project metrics to the organization's strategic vision, mission, or plans can bolster continued senior management support.
- Documentation: As mitigation actions within the Gap Mitigation Plan are completed, documentation of new practices, capabilities, and tools to address gaps will be useful input during any reevaluation. The organization may choose where to document this information (e.g., in the Gap Mitigation Plan or the supporting evidence document in the AAR). Acknowledging successes in completing practices can keep the team focused and engaged in further improving the organization's cybersecurity capabilities.

Reevaluate

Defining and conducting routine reviews to reevaluate gap mitigation implementation status is a common project management practice for maintaining effectiveness of the mitigation actions and helping to keep the organization's efforts on track, on schedule, and on budget. The reevaluation of the Gap Mitigation Plan or the current and capability profiles allows the organization to adjust its gap mitigation priorities, resource allocations, and metrics to align with current conditions. Such flexibility through reevaluation is a valuable aspect of the C2M2 process. Accordingly, reevaluations should also be considered in response to major changes in the business or risk environments to continue on the path of matching the organization's current profile to its desired state of cybersecurity maturity.

- Reevaluation Focus: Common options for reevaluation focus include reviewing progress the organization has made to address priority gaps or reviewing the current and capability profiles for changes in gaps previously identified and prioritized. Gap Mitigation Plan progress can be reevaluated based on the metrics defined by the plan owner, as well as merely by assessing which mitigation actions have or have not been completed. The current and capability profiles may be reevaluated to adjust actual or target MILs (which might affect the priority levels of gaps).
- Reevaluation Timing: Once the focus of the reevaluation has been identified, the organization can review gap mitigation implementation or current and capability profile changes within or outside of planned review cycles.
    - In-Cycle Reviews: Periodic reviews based on established milestones, deadlines, or timeframes would be considered in-cycle reviews. For example, the organization might decide to review the implementation status of a particular gap mitigation action monthly, quarterly, or annually; or the organization might choose to review the status of the entire Gap Mitigation Plan implementation or the current and capability profiles annually, biannually, or at another interval deemed appropriate.

- Out-of-Cycle Reviews: Changes in the organization or its operating environment may necessitate a review of the Gap Mitigation Plan outside of a planned review interval. Factors that would encourage such out-of-cycle reviews include changes in:
    - Status (i.e., availability, functionality, or viability) of assets or systems relating to the function of the C2M2 evaluation
    - Risk (including threats or vulnerabilities) to the organization or function
    - Technology or industry developments that affect operations relating to the function
    - Organization, such as new executive leadership, new or updated strategic plans, or personnel changes
    - Scope, schedule, or budget of the Gap Mitigation Plan

The C2M2 process described in this document is intended to be iterative and flexible; as the organization implements and completes the actions it set out to accomplish in the Gap Mitigation Plan, it can choose to return to previous steps of the model to identify new gaps, assign new priorities, adjust the current or capability profile, or conduct a new C2M2 evaluation. Because the C2M2 is focused on the maturity of the organization's cybersecurity capabilities, a static end state to the process is not indicated. Rather, the model is a tool to support the continual improvement of the organization's cybersecurity program in response to changing risk, business, and technology environments.

Appendix A. Acronyms and Terms

AAR	After-Action Report
ACM	Asset Identification, Change, and Configuration Management
C2M2	Cybersecurity Capability Maturity Model
CBA	Cost–Benefit Analysis
CISCP	Cyber Information Sharing and Collaboration Program
COP	Common Operating Procedure
CPM	Cybersecurity Program Management
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
E-ISAC	Electricity Information Sharing & Analysis Center
FERC	Federal Energy Regulatory Commission
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
IAM	Identity and Access Management
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IR	Event and Incident Response, Continuity of Operations, and Service Restoration
ISC	Information Sharing and Communications
IT	Information Technology
MIL	Maturity Indicator Level
MS-ISAC	Multi-State Information Sharing and Analysis
OT	Operational Technology
RM	Risk Management
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SA	Situational Awareness
SAR	Standards Authorization Request
TVM	Threat and Vulnerability Management
US-CERT	United States Computer Emergency Readiness Team
VOIP	Voice Over Internet Protocol
VSM	Vendor Security Management
WM	Workforce Management

Appendix B. Roles of Evaluation Participants

This list of roles and descriptions of evaluation participants is modified from the U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2) Facilitator Guide (Version 1.1 February 2014).

Sponsor: The sponsor should have a broad understanding of the status and components of the function for which the evaluation is being completed. A sponsor is commonly part of the senior management team, a respected executive, and acknowledged by the staff members as being in charge of their efforts and responsible for results. General responsibilities include:

- Deciding whether the organization should participate in the C2M2 evaluation process
- Selecting an individual to serve as the facilitator
- Ensuring that the necessary resources for the C2M2 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

Participants: All individuals whose presence and active participation is critical during the evaluation (e.g., sponsor, facilitator, SMEs) are referred to as participants. The facilitator should ensure all participants are available for the duration of the evaluation.

Subject Matter Experts (SMEs): SMEs provide input to the evaluation that best represents the organization's current cybersecurity capabilities in relation to the function being evaluated. SMEs are commonly:

- Closely involved in the planning, implementation, or management of the function being evaluated
- Able to understand or speak about one or more of these 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

Observers: All individuals whose presence and active participation are optional during the evaluation are referred to as observers. Attendance of observers should be approved by the sponsor.

Facilitator: The facilitator is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the C2M2 evaluation. General responsibilities include:

- Completing the activities of a typical C2M2 evaluation process
- Ensuring that all activities in the evaluation process are executed efficiently and effectively
- Working with the organization to ensure the evaluation produces high-quality results
- Facilitating the C2M2 evaluation
- Recording responses and comments during the C2M2 evaluation
- Reviewing the detailed outcomes with the sponsor and designees
- Assisting in the planning of follow-up activities

Support Staff: In collaboration with the sponsor, the facilitator should identify all other individuals whose support is necessary during the C2M2 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 evaluation as necessary)

- Technology support staff (to provide and set up all necessary IT and non-IT hardware and software required for the evaluation)
- Site security staff (to issue visitor badges and enable proper physical access by the visitors)

Evaluation Team: All individuals responsible for planning and conducting the C2M2 evaluation comprise the team. At a minimum, this includes the sponsor, facilitator, and support staff.

Appendix C. Pre-Evaluation Reference Checklist

The Dams-C2M2 identifies specific practices across ten domains to be evaluated for an organization's cybersecurity maturity. Many of these practices have associated reference material—plans, strategies, requirements, standards, or guidelines—that might currently exist at facilities or within organizations. Gathering and reviewing available documents in advance of conducting the C2M2 evaluation can help owners and operators progress through the C2M2 evaluation in a timely and efficient manner. During the planning stage, the evaluation team can use this checklist of C2M2 evaluation reference materials. The checklist is organized by C2M2 domain.

Domain 1: Risk Management

- ☐ Enterprise/cybersecurity risk management strategy
- ☐ Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches)
- ☐ Risk taxonomy
- ☐ Risk register (a structured repository of identified risks)
- ☐ Stakeholders list for risk management activities
- ☐ Documented practices, standards, and guidelines for risk management activities

Domain 2: Asset Identification, Change, and Configuration Management

- ☐ Inventory of OT and IT assets (including asset criticality)
- ☐ Configuration baselines
- ☐ Stakeholders list for asset identification, change, and configuration management activities
- ☐ Documented practices, standards, and guidelines for asset identification, change, and configuration management activities

Domain 3: Identity and Access Management

- ☐ Identity and credential type repository
- ☐ Requirements (e.g., access, logging, monitoring, and analysis)
- ☐ Stakeholders list for identity and access management activities
- ☐ Documented practices, standards, and guidelines for identity and access management activities

Domain 4: Threat and Vulnerability Management

- ☐ Information sources for threats and vulnerabilities, communications methods for current cybersecurity state (e.g., from E-ISAC, ICS-CERT, US-CERT, InfraGard, industry associations, other public–private partnerships, vendors, Federal briefings, internal assessments)
- ☐ Threat profile for the function
- ☐ Results of risk and vulnerability assessments
- ☐ Stakeholders list for threat and vulnerability management activities
- ☐ Documented practices, standards, and guidelines for threat and vulnerability management activities

Domain 5: Situational Awareness

- ☐ Logging requirements for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])
- ☐ Aggregated log data
- ☐ Monitoring and analysis requirements (e.g., alarms, alerts, anomalous activity indicators)

- ☐ Common operating picture (monitoring data aggregated to provide an understanding of the operational state of the function)
- ☐ Predefined states (manual or automated process) based on the common operating picture
- ☐ Stakeholders list for situational awareness activities
- ☐ Documented practices, standards, and guidelines for situational awareness activities

Domain 6: Information Sharing and Communications

- ☐ Individuals/organizations identified for information sharing (e.g., HSIN-CI Dams Portal, ICS-CERT, US-CERT, MS-ISAC, E-ISAC, CISCP)
- ☐ Cybersecurity reporting responsibilities by personnel type and audience (e.g., internal reporting, FERC SAR, DOE Form OE-417, law enforcement)
- ☐ Technical sources for cybersecurity issues
- ☐ Information-sharing requirements per the function
- ☐ Stakeholders list for information-sharing activities
- ☐ Documented practices, standards, and guidelines for information-sharing activities

Domain 7: Event and Incident Response, Continuity of Operations, and Service Restoration

- ☐ Point(s) of contact for event reporting
- ☐ Cybersecurity event detection criteria (e.g., what constitutes an event, where to look for events)
- ☐ Cybersecurity event logs and repository
- ☐ Cybersecurity event escalation criteria
- ☐ Cybersecurity event and incident response plans and associated exercises (e.g., table top, simulated incidents)
- ☐ Cybersecurity event and incident lessons learned and associated repository
- ☐ Continuity plans (including minimum requirements for the function, recovery time objectives, and recovery point objectives)
- ☐ Business impact analyses
- ☐ Stakeholders list for event/incident response, continuity of operations, and service restoration activities
- ☐ Documented practices, standards, and guidelines for event/incident response, continuity of operations, and service restoration activities

Domain 8: Vendor Security Management

- ☐ Important IT and OT supplier dependencies (external parties, including operating partners, on which the delivery of the function depends)
- ☐ Important customer dependencies (external parties, including operating partners, on which the delivery of the function depends)
- ☐ Single-source and other essential dependencies
- ☐ Significant cybersecurity risks due to suppliers and other dependencies
- ☐ Supplier cybersecurity requirements
- ☐ Information sources to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services)
- ☐ Stakeholders list for vendor security management activities
- ☐ Documented practices, standards, and guidelines for vendor security management activities

Domain 9: Workforce Management

- ☐ Cybersecurity responsibilities for the function (assigned to personnel types, or roles, including external service providers)
- ☐ Personnel vetting, transferring, and termination procedures
- ☐ Formal accountability process (disciplinary actions for personnel who fail to comply with established security policies and procedures)
- ☐ Cybersecurity training and awareness programs and objectives
- ☐ Stakeholders list for workforce management activities
- ☐ Documented practices, standards, and guidelines for workforce management activities

Domain 10: Cybersecurity Program Management

- ☐ Cybersecurity program strategy (including priorities, objectives, governance, policies, and standards)
- ☐ Program resources (people, tools, funding, senior management sponsorship)
- ☐ IT/OT architectural segmentation/isolation strategy
- ☐ Stakeholders list for cybersecurity program management activities
- ☐ Documented practices, standards, and guidelines for cybersecurity program management activities

Appendix D. Evaluation Read-Ahead Template

Prior to performing the C2M2 evaluation, all participants should become familiar with the C2M2 components and process. This template is provided to help communicate with participants in advance of the evaluation. The template can be modified to include information specific to the organization conducting the evaluation.

Cybersecurity Capability Maturity Model Evaluation	
Evaluation Logistics	*Insert date, time (start and end), and location of the evaluation*
Agenda	▪ Welcome (Sponsor) ▪ Evaluation Overview (Facilitator or Evaluation Team Lead) ▪ C2M2 Evaluation ▪ Review Results: Identify Gaps ▪ Next Steps: Prioritize and Plan to Address the Gaps
Function to be Evaluated	*Insert name of department, line of business, facility, common system, or technology to be evaluated for cybersecurity maturity*
Participants	*Insert titles of personnel expected to participate (personnel names may not be necessary)*
Points of Contact	Sponsor – *Insert name and contact information* Evaluation Team Lead – *Insert name and contact information* Facilitator – *Insert name and contact information*

What is the Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2)?

Cyber threats continue to grow and represent some of the most serious operational risks facing modern organizations. Strong cybersecurity is particularly essential for organizations that use cyber systems to manage or control critical physical processes. The Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2) helps Dams Sector organizations self-evaluate their cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and prioritize cybersecurity investments. The evaluation includes:

- **Evaluate Maturity:** The model is organized into ten domains, each containing a logical grouping of structured objectives and cybersecurity practices. During the evaluation, participants will measure the organization's progression using a scale of maturity indicator levels (MILs) 0–3, with a set of attributes defining each level. This allows the organization to define its current/actual state, determine its future/target state, and identify the gaps that must be filled to attain the future/target state.
- **Review Results:** Upon completion of the evaluation, a summary table is generated that shows MIL results for each domain and identifies gaps in the performance of model practices. Participants will briefly discuss the successes that led to attaining the current/actual state and gaps that must be filled to attain the future/target state.
- **Analyze Gaps:** Participants will determine whether the gaps identified are meaningful and important for the organization to address. This will be based on a target MIL rating for each objective that best enables the organization to meet its business objectives and cybersecurity strategy.
- **Prioritize Gaps:** Participants will prioritize the most meaningful gaps and brainstorm activities/actions to fully implement the practices needed to achieve the desired capability in specific domains. This will be based on relative importance and the time needed to fill the gap.

Post-evaluation, the organization will develop a plan to address the selected gaps and track implementation of the plan.

Why is [ORGANIZATION NAME] Implementing the Dams-C2M2?

Insert the reason the organization is implementing the C2M2, including why the specific function was selected for evaluation, the intended value to the organization, and expected outcome(s).

How Should Participants Prepare for the Dams-C2M2 Evaluation?

1. Read Chapters 5 and 7 of the Dams-C2M2 to understand the model's structure, terminology, and process.
2. Utilize the tables in Appendix E. Maturity Level Selection Worksheet to practice using the model by pre-selecting MILs to assess cybersecurity maturity of the evaluated function. Instructions for using the worksheet are included in Appendix E.

Appendix E. Maturity Level Selection Worksheet

The selection of actual and target maturity indicator levels (MILs) for the function being evaluated forms the primary results of the C2M2. This worksheet template (which is based on Chapter 7 of the Dams-C2M2) may be used in multiple ways to support the organization's implementation of the model.

- **Homework:** Prior to the evaluation, participants will become familiar with the C2M2 by practicing the process of reviewing domains and objectives, then selecting completed practices and MILs.
- **Evaluation Guidance:** During the evaluation, participants follow along with the facilitator as the C2M2 domains, objectives, and practices are discussed.
- **Evaluation Documentation:** While the facilitator is guiding participants through the C2M2, a member(s) of the evaluation team documents the decisions about MILs and discussions supporting MIL selection.
- **After-Action Report Development:** The evaluation results (including MIL selection and supporting information) recorded in the worksheet can be used in the development of an after-action report.

Worksheet Instructions

1. Review the objective (rows shaded blue) and practices associated with each MIL.
2. For each practice, identify whether the practice is:
    - Fully complete – *Insert the organization's definition of fully complete*
    - Largely complete – *Insert the organization's definition of largely complete*
    - Partially complete – *Insert the organization's definition of partially complete*
    - Not complete – *Insert the organization's definition of not complete*
3. Document the selection of completed practices by using the check boxes. Only practices noted as fully complete or largely complete should receive a checkmark. Partially complete and not complete remain unchecked as an indication of gaps to be filled.
4. Document the evidence to support each completed practice selection in the notes column. Examples of evidence include summarizing why the practice is fully or largely complete (including assumptions made), citing a specific document pertaining to that practice, summarizing the organization's specific actions pertaining to that practice, and noting who is responsible for the actions.
5. Select the *actual* MIL associated with the number of practices your organization has completed (and checkmarked) for that domain/objective. MILs are cumulative within each objective.
    - MIL0 (or MIL1 if the objective shows that there are no practices for MIL1): No practices are completed for that objective.
    - MIL1: All practices listed for MIL1 are completed.
    - MIL2: All practices listed for MIL1 and MIL2 are completed.
    - MIL3: All practices listed for MIL1, MIL2, and MIL3 are completed.
    - If all practices for MIL 1 and some of the practices for MIL2 are completed, select MIL1 as the actual MIL.
6. Select the *target* MIL associated with the desired level of maturity for that objective. Striving to achieve the highest MIL in all objectives may not be the optimal course of action for all organizations.
7. Document the actions the organization should implement to complete the additional practices needed to achieve the target MIL in the notes column. Examples of these gaps include summarizing why the practice is partially or not complete (including assumptions made), citing a specific document to be updated to complete the practice, summarizing the organization's future actions to complete the practice, and noting who is responsible for the actions.

Dams-C2M2 Maturity Level Selection Documentation

Evaluation Date: _____

Organization: _____

Note-Taker Name and Contact Info: _____

Domain 1: Risk Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Establish Cybersecurity Risk-Management Strategy					
MIL1		No practices.			
MIL2	☐	a) There is a **documented** cybersecurity risk-management strategy.			
	☐	b) The strategy **provides an approach** for risk prioritization, including consideration of effect.			
MIL3	☐	c) Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on effect, tolerance for risk, and risk response approaches) are **defined and available**.			
	☐	d) The risk-management strategy is periodically **updated** to reflect the current threat environment.			
	☐	e) An organization-specific risk taxonomy is **documented** and is used in risk-management activities.			
2. Manage Cybersecurity Risk					
MIL1	☐	a) Cybersecurity risks are **identified**.			
	☐	b) Identified risks are **mitigated, accepted, tolerated, or transferred**.			
MIL2	☐	c) Risk assessments are performed to **identify risks** in accordance with the risk-management strategy.			
	☐	d) Identified risks are **documented**.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ e) Identified risks are **analyzed** to prioritize response activities in accordance with the risk-management strategy. ☐ f) Identified risks are **monitored** in accordance with the risk-management strategy. ☐ g) Risk analysis is **informed** by network (IT and/or OT) architecture.			
MIL3	☐ h) The risk-management program **defines and operates** risk-management policies and procedures that implement the risk-management strategy. ☐ i) A current cybersecurity architecture is used to **inform** risk analysis. ☐ j) A risk register (a structured repository of identified risks) is used to **support** risk-management activities.			
3. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for risk-management activities. ☐ b) Stakeholders for risk-management activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support risk-management activities. ☐ d) Standards and/or guidelines have been **identified** to inform risk-management activities.			
MIL3	☐ e) Risk-management activities are **guided by** documented policies or other organizational directives. ☐ f) Risk-management policies **include** compliance requirements for specified standards and/or guidelines. ☐ g) Risk-management activities are periodically **reviewed** to ensure conformance with policy. ☐ h) Responsibility and authority for the performance of risk-management activities are **assigned** to personnel.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	i) Personnel performing risk-management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 2: Asset Identification, Change, and Configuration Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Manage Asset Inventory					
MIL1	☐	a) There is an **inventory** of OT and IT assets that are important to the delivery of the function.			
	☐	b) There is an **inventory** of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data).			
MIL2	☐	c) Inventory attributes **include** information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, criticality of the asset, service dependencies, service-level agreements, and conformance of assets to relevant industry standards).			
	☐	d) Inventoried assets are **prioritized** based on their importance to the delivery of the function.			
MIL3	☐	e) There is an **inventory** for all connected IT and OT assets related to the delivery of the function.			
	☐	f) The asset inventory **is current** (as defined by the organization).			
2. Manage Asset Configuration					
MIL1	☐	a) Configuration baselines are **established** for inventoried assets where it is desirable to ensure that multiple assets are configured similarly.			
	☐	b) Configuration baselines are used to **configure** assets at deployment.			
MIL2	☐	c) The design of configuration baselines **includes** cybersecurity objectives.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐ d) Configuration of assets is **monitored** for consistency with baselines throughout the assets' life cycle. ☐ e) Configuration baselines are **reviewed and updated** at an organizationally defined frequency.			
3. Manage Changes to Assets				
MIL1	☐ a) Changes to inventoried assets are **evaluated** before being implemented. ☐ b) Changes to inventoried assets are **logged**.			
MIL2	☐ c) Changes to assets are **tested** prior to being deployed, whenever possible. ☐ d) Change management practices **address** the full life cycle of assets (i.e., acquisition, deployment, operation, retirement).			
MIL3	☐ e) Changes to assets are **tested** for cybersecurity effect prior to being deployed. ☐ f) Change logs **include** information about modifications that affect the cybersecurity requirements of assets (availability, integrity, confidentiality).			
4. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for asset inventory, configuration, and change management activities. ☐ b) Stakeholders for asset inventory, configuration, and change management activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support asset inventory, configuration, and change management activities. ☐ d) Standards and/or guidelines have been **identified** to inform asset inventory, configuration, and change management activities.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	e) Asset inventory, configuration, and change management activities are **guided** by documented policies or other organizational directives.			
	☐	f) Asset inventory, configuration, and change management policies **include** compliance requirements for specified standards and/or guidelines.			
	☐	g) Asset inventory, configuration, and change management activities are periodically **reviewed** to ensure conformance with policy.			
	☐	h) Responsibility and authority for the performance of asset inventory, configuration, and change management activities are **assigned** to personnel.			
	☐	i) Personnel performing asset inventory, configuration, and change management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 3: Identity and Access Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Establish and Maintain Identities					
MIL1	☐	a) Identities are **provisioned** for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities).			
	☐	b) Credentials are **issued** for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys).			
	☐	c) Identities are **deprovisioned** when no longer required.			
MIL2	☐	d) Identity repositories are periodically **reviewed and updated** to ensure validity (i.e., to ensure that the identities still need access).			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ e) Credentials are periodically **reviewed** to ensure they are associated with the correct person or entity. ☐ f) Identities are **deprovisioned** within organizationally defined time thresholds when no longer required.			
MIL3	☐ g) Requirements for credentials are **informed** by the organization's risk criteria (e.g., multifactor credentials for higher risk access).			
2. Control Access				
MIL1	☐ a) Access requirements, including those for remote access, are **determined** (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters). ☐ b) Access is **granted** to identities based on requirements. ☐ c) Access is **revoked** when no longer required.			
MIL2	☐ d) Access requirements **incorporate** least-privilege and separation-of-duties principles. ☐ e) Access requests are **reviewed and approved** by the asset owner. ☐ f) Root privileges, administrative access, emergency access, and shared accounts **receive** additional scrutiny and monitoring.			
MIL3	☐ g) Access privileges are **reviewed and updated** to ensure validity, at an organizationally defined frequency. ☐ h) Access to assets is **granted** by the asset owner based on risk to the function. ☐ i) Anomalous access attempts are **monitored** as indicators of cybersecurity events.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
3. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** to establish and maintain identities and control access. ☐ b) Stakeholders for access and identity management activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support access and identity management activities. ☐ d) Standards and/or guidelines have been **identified** to inform access and identity management activities.			
MIL3	☐ e) Access and identity management activities are **guided** by documented policies or other organizational directives. ☐ f) Access and identity management policies **include** compliance requirements for specified standards and/or guidelines. ☐ g) Access and identity management activities are periodically **reviewed** to ensure conformance with policy. ☐ h) Responsibility and authority for the performance of access and identity management activities are **assigned** to personnel. ☐ i) Personnel performing access and identity management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 4: Threat and Vulnerability Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Identify and Respond to Threats					
MIL1	☐	a) Information sources to support threat management activities are **identified** (e.g., E-ISAC, ICS-CERT, US-CERT, InfraGard, industry associations, other public-private partnerships, vendors, Federal briefings).			
	☐	b) Cybersecurity threat information is **gathered and interpreted** for the function.			
	☐	c) Threats considered important to the function are **addressed** (e.g., implement mitigating controls, monitor threat status).			
MIL2	☐	d) A threat profile for the function is **established** that includes characterization of likely intent, capability, and target of threats to the function.			
	☐	e) Threat information sources that address all components of the threat profile are **prioritized and monitored**.			
	☐	f) Identified threats are **analyzed and prioritized**.			
	☐	g) Threats are **addressed** according to the assigned priority.			
MIL3	☐	h) The threat profile for the function is **validated** at an organization-defined frequency.			
	☐	i) Analysis and prioritization of threats are **informed** by the function's (or organization's) risk criteria.			
	☐	j) Threat information is **added** to the risk register.			
2. Monitoring and Mitigating Cybersecurity Vulnerabilities					
MIL1	☐	a) Information sources to support cybersecurity vulnerability discovery are **identified** (e.g., E-ISAC, ICS-CERT, US-CERT, InfraGard, industry associations, vendors, Federal briefings, internal assessments).			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL1	☐ b) Cybersecurity vulnerability information is **gathered and interpreted** for the function. ☐ c) Cybersecurity vulnerabilities that are considered important to the function are **addressed** (e.g., implement mitigating controls, apply cybersecurity patches).			
MIL2	☐ d) Cybersecurity vulnerability information sources that address all assets important to the function are **monitored**. ☐ e) Cybersecurity vulnerability assessments are **performed** (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools). ☐ f) Identified cybersecurity vulnerabilities are **analyzed and prioritized** (e.g., NIST Common Vulnerability Scoring System could be used for patches; internal guidelines could be used to prioritize other types of vulnerabilities). ☐ g) Cybersecurity vulnerabilities are **addressed** according to the assigned priority. ☐ h) Operational effect to the function is **evaluated** prior to deploying cybersecurity patches.			
MIL3	☐ i) Cybersecurity vulnerability assessments are **performed** for all assets important to the delivery of the function, at an organization-defined frequency. ☐ j) Cybersecurity vulnerability assessments are **informed** by the function's (or organization's) risk criteria. ☐ k) Cybersecurity vulnerability assessments are **performed** by parties that are independent of the operations of the function. ☐ l) Analysis and prioritization of cybersecurity vulnerabilities are **informed** by the function's (or organization's) risk criteria. ☐ m) Cybersecurity vulnerability information is **added** to the risk register.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐ n) Risk-monitoring activities **validate** the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities).			
3. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for threat and vulnerability management activities. ☐ b) Stakeholders for threat and vulnerability management activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support threat and vulnerability management activities. ☐ d) Standards and/or guidelines have been **identified** to inform threat and vulnerability management activities.			
MIL3	☐ e) Threat and vulnerability activities are **guided** by documented policies or other organizational directives. ☐ f) Threat and vulnerability management policies **include** compliance requirements for specified standards and/or guidelines. ☐ g) Threat and vulnerability management activities are periodically **reviewed** to ensure conformance with policy. ☐ h) Responsibility and authority for the performance of threat and vulnerability management activities are **assigned** to personnel. ☐ i) Personnel performing threat and vulnerability management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 5: Situational Awareness

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Perform Logging					
MIL1	☐	a) Logging is **occurring** for assets important to the function where possible.			
MIL2	☐	b) Logging requirements have been **defined** for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability]).			
	☐	c) Log data are being **aggregated** within the function.			
MIL3	☐	d) Logging requirements are **based** on the risk to the function.			
	☐	e) Log data **support** other business and security processes (e.g., incident response, asset management).			
2. Perform Monitoring					
MIL1	☐	a) Cybersecurity monitoring activities are **performed** (e.g., regular/daily reviews of log data).			
	☐	b) Operational environments are **monitored** for anomalous behavior that may indicate a cybersecurity event.			
MIL2	☐	c) Monitoring and analysis requirements have been **defined** for the function and address timely review of event data.			
	☐	d) Alarms and alerts are **configured** to aid in the identification of cybersecurity events.			
	☐	e) Indicators of anomalous activity have been **defined and are monitored** across the operational environment.			
	☐	f) Monitoring activities are **aligned** with the function's threat profile.			
MIL3	☐	g) Monitoring requirements are **based** on the risk to the function.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	h) Monitoring is **integrated** with other business and security processes (e.g., incident response, asset management).			
	☐	i) Continuous monitoring is **performed** across the operational environment to identify anomalous activity.			
	☐	j) Risk register content is used to **identify** indicators of anomalous activity.			
	☐	k) Alarms and alerts are **configured** according to indicators of anomalous activity.			
3. Establish and Maintain a Common Operating Procedure (COP)					
MIL1		No practices.			
MIL2	☐	a) Methods of communicating the current state of cybersecurity for the function are **established and maintained**.			
	☐	b) Monitoring data are **aggregated** to provide an understanding of the operational state of the function (i.e., a COP; a COP may or may not include visualization or be presented graphically).			
	☐	c) Information from across the organization is **available** to enhance the COP.			
MIL3	☐	d) Monitoring data are **aggregated** to provide near-real-time understanding of the cybersecurity state for the function to enhance the COP.			
	☐	e) Information from outside the organization is **collected** to enhance the COP.			
	☐	f) Predefined states of operation are **defined and invoked** (manual or automated process) based on the COP.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
4. Management Activities					
MIL1		No practices.			
MIL2	☐	a) Documented practices are **followed** for logging, monitoring, and COP activities.			
	☐	b) Stakeholders for logging, monitoring, and COP activities are **identified and involved**.			
	☐	c) Adequate resources (people, funding, and tools) are **provided** to support logging, monitoring, and COP activities.			
	☐	d) Standards and/or guidelines have been **identified** to inform logging, monitoring, and COP activities.			
MIL3	☐	e) Logging, monitoring, and COP activities are **guided** by documented policies or other organizational directives.			
	☐	f) Logging, monitoring, and COP policies **include** compliance requirements for specified standards and/or guidelines.			
	☐	g) Logging, monitoring, and COP activities are periodically **reviewed** to ensure conformance with policy.			
	☐	h) Responsibility and authority for the performance of logging, monitoring, and COP activities are **assigned** to personnel.			
	☐	i) Personnel performing logging, monitoring, and COP activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 6: Information Sharing and Communications

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Share Cybersecurity Information					
MIL1	☐	a) Information is **collected from and provided** to selected individuals and/or organizations as applicable to the organization, considering regulatory reporting			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL1		obligations and voluntary sharing among industry associations.			
	☐	b) Responsibility for cybersecurity reporting obligations (e.g., internal reporting, Federal Energy Regulatory Commission [FERC] Standards Authorization Request [SAR], DOE Form OE-417, law enforcement) is **assigned** to personnel.			
MIL2	☐	c) Information-sharing stakeholders are **identified** based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities).			
	☐	d) Information is **collected from and provided** to identified information-sharing stakeholders.			
	☐	e) Technical sources are **identified** that can be consulted on cybersecurity issues.			
	☐	f) Provisions are **established and maintained** to enable secure sharing of sensitive or classified information.			
	☐	g) Information-sharing practices **address** both standard operations and emergency operations.			
MIL3	☐	h) Information-sharing stakeholders are **identified** based on shared interest in and risk to critical infrastructure.			
	☐	i) The function or the organization **participates** with information-sharing and analysis centers.			
	☐	j) Information-sharing requirements have been **defined** for the function **and address** timely dissemination of cybersecurity information.			
	☐	k) Procedures **are in place** to analyze and de-conflict received information.			
	☐	l) A network of internal and external trust relationships (formal and/or informal) has been **established** to vet and validate information about cyber events.			
2. Management Activities					
MIL1		No practices.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ a) Documented practices are **followed** for information-sharing activities. ☐ b) Stakeholders for information-sharing activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support information-sharing activities. ☐ d) Standards and/or guidelines have been **identified** to inform information-sharing activities.			
MIL3	☐ e) Information-sharing activities are **guided** by documented policies, subject matter experts, or other organizational directives. ☐ f) Information-sharing policies **include** compliance requirements for specified standards and/or guidelines. ☐ g) Information-sharing activities are periodically **reviewed** to ensure conformance with policy. ☐ h) Responsibility and authority for the performance of information-sharing activities are **assigned** to personnel. ☐ i) Personnel performing information-sharing activities **have the skills and knowledge** needed to perform their assigned responsibilities. ☐ j) Information-sharing policies **address** protected information and ethical use and sharing of information, including sensitive and classified information as appropriate.			

Domain 7: Event and Incident Response, Continuity of Operations, and Service Restoration

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Detect Cybersecurity Events				
MIL1	☐ a) There **is a point of contact** (person or role) to whom cybersecurity events could be reported. ☐ b) Detected cybersecurity events are **reported**. ☐ c) Cybersecurity events are **logged and tracked**.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ d) Criteria are **established** for cybersecurity event detection (e.g., what constitutes an event, where to look for events). ☐ e) **There is a repository** where cybersecurity events are logged based on the established criteria.			
MIL3	☐ f) Event information is **correlated** to support incident analysis by identifying patterns, trends, and other common features. ☐ g) Cybersecurity event detection activities are **adjusted** based on information from the organization's risk register and threat profile to help detect known threats and monitor for identified risks. ☐ h) The common operating picture for the function is **monitored** to support the identification of cybersecurity events.			
2. Escalate Cybersecurity Events and Declare Incidents				
MIL1	☐ a) Criteria for cybersecurity event escalation are **established**, including cybersecurity incident declaration criteria. ☐ b) Cybersecurity events are **analyzed** to support escalation and the declaration of cybersecurity incidents. ☐ c) Escalated cybersecurity events and incidents are **logged and tracked**.			
MIL2	☐ d) Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are **established** based on the potential effect to the function. ☐ e) Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are **updated** at an organization-defined frequency. ☐ f) **There is a repository** where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	g) Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are **adjusted** according to information from the organization's risk register and threat profile.			
	☐	h) Escalated cybersecurity events and declared cybersecurity incidents **inform** the common operating picture for the function.			
	☐	i) Escalated cybersecurity events and declared incidents are **correlated** to support the discovery of patterns, trends, and other common features.			
3. Respond to Incidents and Escalated Cybersecurity Events					
MIL1	☐	a) Cybersecurity event and incident response personnel are **identified** and roles are **assigned**.			
	☐	b) Responses to escalated cybersecurity events and incidents are **implemented** to limit effects to the function and to restore normal operations.			
	☐	c) Reporting of escalated cybersecurity events and incidents is **performed** (e.g., internal reporting, DOE Form OE-417, E-ISAC, ICS-CERT).			
MIL2	☐	d) Cybersecurity event and incident response is **performed** according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure).			
	☐	e) Cybersecurity event and incident response plans are **exercised** at an organization-defined frequency.			
	☐	f) Cybersecurity event and incident response plans **address** OT and IT assets important to the delivery of the function.			
	☐	g) Training is **conducted** for cybersecurity event and incident response teams.			
MIL3	☐	h) Cybersecurity event and incident root-cause analysis and lessons-learned activities are **performed**, and corrective actions are taken.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	i) Cybersecurity event and incident responses are **coordinated** with law enforcement and other government entities as appropriate, including support for evidence collection and preservation.			
	☐	j) Cybersecurity event and incident response personnel **participate** in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents).			
	☐	k) Cybersecurity event and incident response plans are **reviewed and updated** at an organization-defined frequency.			
	☐	l) Cybersecurity event and incident response activities are **coordinated** with relevant external entities.			
	☐	m) Cybersecurity event and incident response plans are **aligned** with the function's risk criteria and threat profile.			
	☐	n) Policy and procedures for reporting cybersecurity event and incident information to designated authorities **conform** to applicable laws, regulations, and contractual agreements.			
	☐	o) Restored assets are **configured** appropriately and inventory information is updated following execution of response plans.			
4. Plan for Continuity					
MIL1	☐	a) The activities necessary to sustain minimum operations of the function are **identified**.			
	☐	b) The sequence of activities necessary to return the function to normal operation is **identified**.			
	☐	c) Continuity plans are **developed** to sustain and restore operation of the function.			
MIL2	☐	d) Business impact analyses **inform** the development of continuity plans.			
	☐	e) Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are **incorporated** into continuity plans.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ f) Continuity plans are **evaluated and exercised**.			
MIL3	☐ g) Business impact analyses are periodically **reviewed and updated**. ☐ h) RTO and RPO are **aligned** with the function's risk criteria. ☐ i) The results of continuity plan testing and/or activation are **compared** to recovery objectives, and plans are **improved** accordingly. ☐ j) Continuity plans are periodically **reviewed and updated**. ☐ k) Restored assets are **configured** appropriately, and inventory information is **updated** following execution of continuity plans.			
5. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for cybersecurity event and incident response, as well as continuity of operations activities. ☐ b) Stakeholders for cybersecurity event and incident response, as well as continuity of operations activities, are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support cybersecurity event and incident response, as well as continuity of operations activities. ☐ d) Standards and/or guidelines have been **identified** to inform cybersecurity event and incident response, as well as continuity of operations activities.			
MIL3	☐ e) Cybersecurity event and incident response, as well as continuity of operations activities, are **guided** by documented policies or other organizational directives. ☐ f) Cybersecurity event and incident response, as well as continuity of operations policies, **include** compliance requirements for specified standards and/or guidelines.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	g) Cybersecurity event and incident response, as well as continuity of operations activities, are periodically **reviewed** to ensure conformance with policy.			
	☐	h) Responsibility and authority for the performance of cybersecurity event and incident response, as well as continuity of operations activities, are **assigned** to personnel.			
	☐	i) Personnel performing cybersecurity event and incident response, as well as continuity of operations activities, **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 8: Vendor Security Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Identify Dependencies					
MIL1	☐	a) Important IT and OT supplier dependencies are **identified** (i.e., external parties on which the delivery of the function depends, including operating partners).			
	☐	b) Important customer dependencies are **identified** (i.e., external parties that are dependent on the delivery of the function including operating partners).			
MIL2	☐	c) Supplier dependencies are **identified** according to established criteria.			
	☐	d) Customer dependencies are **identified** according to established criteria.			
	☐	e) Single-source and other essential dependencies are **identified**.			
	☐	f) Dependencies are **prioritized**.			
MIL3	☐	g) Dependency prioritization and identification are **based** on the function's or organization's risk criteria.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
2. Manage Dependency Risk					
MIL1	☐	a) Significant cybersecurity risks due to suppliers and other dependencies are **identified and addressed**.			
	☐	b) Cybersecurity requirements are **considered** when establishing relationships with suppliers and other third parties.			
MIL2	☐	c) Identified cybersecurity dependency risks are **entered** into the risk register.			
	☐	d) Contracts and agreements with third parties **incorporate** sharing of cybersecurity threat information.			
	☐	e) Cybersecurity requirements are **established** for suppliers according to a defined practice, including requirements for secure software development practices where appropriate.			
	☐	f) Agreements with suppliers and other external entities **include** cybersecurity requirements.			
	☐	g) Evaluation and selection of suppliers and other external entities **includes** consideration of their ability to meet cybersecurity requirements.			
	☐	h) Agreements with suppliers **require** notification of cybersecurity incidents related to the delivery of the product or service.			
	☐	i) Suppliers and other external entities are periodically **reviewed** for their ability to continually meet the cybersecurity requirements.			
MIL3	☐	j) Cybersecurity risks due to external dependencies are **managed** according to the organization's risk-management criteria and process.			
	☐	k) Cybersecurity requirements are **established** for supplier dependencies based on the organization's risk criteria.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	l) Agreements with suppliers **require** notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products.			
	☐	m) Acceptance testing of procured assets **includes** testing for cybersecurity requirements.			
	☐	n) Information sources are **monitored** to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services).			
3. Management Activities					
MIL1		No practices.			
MIL2	☐	a) Documented practices are **followed** for managing dependency risk.			
	☐	b) Stakeholders for managing dependency risk are **identified and involved**.			
	☐	c) Adequate resources (people, funding, and tools) are **provided** to support dependency risk-management activities.			
	☐	d) Standards and/or guidelines have been **identified** to inform managing dependency risk.			
MIL3	☐	e) Dependency risk-management activities are **guided** by documented policies or other organizational directives.			
	☐	f) Dependency risk-management policies **include** compliance requirements for specified standards and/or guidelines.			
	☐	g) Dependency risk-management activities are periodically **reviewed** to ensure conformance with policy.			
	☐	h) Responsibility and authority for the performance of dependency risk management are **assigned** to personnel.			
	☐	i) Personnel performing dependency risk management **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 9: Workforce Management

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Assign Cybersecurity Responsibilities				
MIL1	☐ a) Cybersecurity responsibilities for the function are **identified**. ☐ b) Cybersecurity responsibilities are **assigned** to specific people.			
MIL2	☐ c) Cybersecurity responsibilities are **assigned** to specific roles, including external service providers. ☐ d) Cybersecurity responsibilities are **documented** (e.g., in position descriptions).			
MIL3	☐ e) Cybersecurity responsibilities and job requirements are **reviewed and updated** as appropriate. ☐ f) Cybersecurity responsibilities are **included** in job performance evaluation criteria. ☐ g) Assigned cybersecurity responsibilities are **managed** to ensure adequacy and redundancy of coverage.			
2. Control the Workforce Life Cycle				
MIL1	☐ a) Personnel vetting (e.g., background checks, drug tests) is **performed** at hire for positions that have access to the assets required for delivery of the function. ☐ b) Personnel termination procedures **address** cybersecurity.			
MIL2	☐ c) Personnel vetting is **performed** at an organization-defined frequency for positions that have access to the assets required for delivery of the function. ☐ d) Personnel transfer procedures **address** cybersecurity.			
MIL3	☐ e) Risk designations are **assigned** to all positions that have access to the assets required for delivery of the function. ☐ f) Vetting is **performed** for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	g) Succession planning is **performed** for personnel based on risk designation.			
	☐	h) A formal accountability process that includes disciplinary actions is **implemented** for personnel who fail to comply with established security policies and procedures.			
3. Develop Cybersecurity Workforce					
MIL1	☐	a) Cybersecurity training is **made available** to personnel with assigned cybersecurity responsibilities.			
MIL2	☐	b) Cybersecurity knowledge, skill, and ability gaps are **identified**.			
	☐	c) Identified gaps are **addressed** through recruiting and/or training.			
	☐	d) Cybersecurity training is **provided** as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training).			
MIL3	☐	e) Cybersecurity workforce management objectives that support current and future operational needs are **established and maintained**.			
	☐	f) Recruiting and retention are **aligned** to support cybersecurity workforce management objectives.			
	☐	g) Training programs are **aligned** to support cybersecurity workforce management objectives.			
	☐	h) The effectiveness of training programs is **evaluated** at an organization-defined frequency, and improvements are made as appropriate.			
	☐	i) Training programs **include** continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.			
4. Increase Cybersecurity Awareness					
MIL1	☐	a) Cybersecurity awareness activities **occur**.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ b) Objectives for cybersecurity awareness activities are **established and maintained**. ☐ c) Cybersecurity awareness content is **based** on the organization's threat profile.			
MIL3	☐ d) Cybersecurity awareness activities are **aligned** with the predefined states of operation. ☐ e) The effectiveness of cybersecurity awareness activities is **evaluated** at an organization-defined frequency, and improvements are made as appropriate.			
5. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for cybersecurity workforce management activities. ☐ b) Stakeholders for cybersecurity workforce management activities are **identified and involved**. ☐ c) Adequate resources (people, funding, and tools) are **provided** to support cybersecurity workforce management activities. ☐ d) Standards and/or guidelines have been **identified** to inform cybersecurity workforce management activities.			
MIL3	☐ e) Cybersecurity workforce management activities are **guided** by documented policies or other organizational directives. ☐ f) Cybersecurity workforce management policies **include** compliance requirements for specified standards and/or guidelines. ☐ g) Cybersecurity workforce management activities are periodically **reviewed** to ensure conformance with policy. ☐ h) Responsibility and authority for the performance of cybersecurity workforce management activities are **assigned** to personnel.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL3	☐	i) Personnel performing cybersecurity workforce management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Domain 10: Cybersecurity Program Management

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
1. Establish Cybersecurity Program Strategy					
MIL1	☐	a) The organization **has a cybersecurity program strategy**.			
MIL2	☐	b) The cybersecurity program strategy **defines** objectives for the organization's cybersecurity activities.			
	☐	c) The cybersecurity program strategy and priorities are **documented and aligned** with the organization's strategic objectives and risk to critical infrastructure.			
	☐	d) The cybersecurity program strategy **defines** the organization's approach to provide program oversight and governance for cybersecurity activities, including policies and standards.			
	☐	e) The cybersecurity program strategy **defines** the structure and organization of the cybersecurity program.			
	☐	f) The cybersecurity program strategy is **approved** by senior management.			
MIL3	☐	g) The cybersecurity program strategy—including policies and standards—is **updated** to reflect business changes, changes in the operating environment and changes in the threat profile.			
2. Sponsor Cybersecurity Program					
MIL1	☐	a) Resources (people, tools, and funding) are **provided** to support the cybersecurity program.			
	☐	b) Senior management **provides** sponsorship for the cybersecurity program.			

Objective and Practices			Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐	c) The cybersecurity program is **established** according to the cybersecurity program strategy.			
	☐	d) Adequate funding and other resources (i.e., people and tools) are **provided** to establish and operate a cybersecurity program aligned with the program strategy.			
	☐	e) Senior management sponsorship for the cybersecurity program is **visible and active** (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management).			
	☐	f) If the organization develops or procures software, secure software development practices are **sponsored** as an element of the cybersecurity program.			
	☐	g) The development and maintenance of cybersecurity policies is **sponsored**.			
	☐	h) Responsibility for the cybersecurity program is assigned to a role with requisite authority.			
MIL3	☐	i) The performance of the cybersecurity program is **monitored** to ensure it aligns with the cybersecurity program strategy.			
	☐	j) The cybersecurity program is independently **reviewed** (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives.			
	☐	k) The cybersecurity program **addresses** and enables the achievement of regulatory compliance as appropriate.			
	☐	l) The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives.			
3. Establish and Maintain Cybersecurity Architecture					
MIL1	☐	a) A strategy to architecturally isolate the organization's IT systems from OT systems is **implemented**.			
MIL2	☐	b) A cybersecurity architecture is **in place** to enable segmentation, isolation, and other requirements that support the cybersecurity strategy.			

Objective and Practices		Actual MIL	Target MIL	Notes (Evidence Supporting MIL Selection)
MIL2	☐ c) Architectural segmentation and isolation are **maintained** according to a documented plan.			
MIL3	☐ d) Cybersecurity architecture is **updated** at an organization-defined frequency to keep it current.			
4. Perform Secure Software Development				
MIL1	No practices.			
MIL2	☐ a) Software to be deployed on assets that are important to the delivery of the function is **developed** using secure software development practices.			
MIL3	☐ b) Policies **require** that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices.			
5. Management Activities				
MIL1	No practices.			
MIL2	☐ a) Documented practices are **followed** for cybersecurity program management activities. ☐ b) Stakeholders for cybersecurity program management activities are **identified and involved**. ☐ c) Standards and/or guidelines have been **identified** to inform cybersecurity program management activities.			
MIL3	☐ d) Cybersecurity program management activities are **guided** by documented policies or other organizational directives. ☐ e) Cybersecurity program management activities are periodically **reviewed** to ensure conformance with policy. ☐ f) Personnel performing cybersecurity program management activities **have the skills and knowledge** needed to perform their assigned responsibilities.			

Appendix F. Evaluation Preparation Checklist

This checklist highlights the tasks for the facilitator and support staff to perform in preparation for the C2M2 evaluation. It is adapted from the U.S. Department of Energy C2M2 Facilitator Guide Appendix A, available at www.emannergy.gov/oe/downloads/cybersecurity-capability-maturity-model-facilitator-guide-february-2014.

Four Weeks Prior to Evaluation

- ☐ Obtain the latest version of the Dams-C2M2 and Implementation Guide (this document)
- ☐ Become familiar with the Dams-C2M2 and Implementation Guide
- ☐ Meet with the sponsor and other stakeholders
- ☐ Determine function and scope of the evaluation
- ☐ Identify participants and support personnel
- ☐ Identify date for the evaluation
- ☐ Send invitations to participants (such as through a calendar appointment)
- ☐ Determine the need to request that participants complete homework prior to the evaluation
- ☐ Draft the C2M2 Evaluation Read-Ahead (Appendix D)
- ☐ Identify and reserve appropriate meeting space for the evaluation
- ☐ Make travel arrangements (if necessary)
- ☐ Establish non-disclosure agreements (if necessary)
- ☐ Meet with local point of contact

Two Weeks Prior to Evaluation

- ☐ Send the C2M2 Evaluation Read-Ahead to participants as homework to prepare for the evaluation
- ☐ Ensure there are sufficient confirmed participants to conduct the evaluation
- ☐ Communicate IT system requirements to IT support staff
- ☐ Communicate non-IT system requirements to support staff
- ☐ Identify staff to scribe/take notes
- ☐ Arrange for catering (if necessary)
- ☐ Arrange for building access for those visiting
- ☐ Touch base with local point of contact

One Week Prior to Evaluation

- ☐ Test all the tools (hardware and software) ahead of time
- ☐ Touch base with local point of contact
- ☐ Ensure support staff will provide supplies for the room

The Day Before Evaluation

- ☐ Ensure the meeting room has been set up properly
- ☐ Ensure the required technology (e.g., computers, projectors) is present and functioning
- ☐ Load the necessary files onto the designated computers and test
- ☐ Confirm catering (if necessary)

The Day of Evaluation

- ☐ Arrive at the meeting room at least 30 minutes prior to the start of the evaluation
- ☐ After completion of the evaluation, collect all printed sensitive material
- ☐ Copy necessary files from the room computer onto two other locations/media; delete all evaluation files from the room computers

Within One Week After Evaluation

- ☐ Collect notes from the scribe/note-taker
- ☐ Organize all other inputs needed to draft the After-Action Report (e.g., Evaluation Read-Ahead, Maturity Profile, Gap Mitigation Plan)
- ☐ Determine who will draft the After-Action Report and milestones for drafting, reviewing, and finalizing
- ☐ Meet with the sponsor to assist the organization with planning follow-up actions

Appendix G. C2M2 Domains and Maturity Indicator Level Reference Sheet

The lists below consolidate descriptions of C2M2 domains and maturity indication levels (MILs) for easy reference for those involved in the C2M2 evaluation. It is adapted from the U.S. Department of Energy C2M2 Facilitator Toolkit Reference Cheat Sheet, available upon request from ES-C2M2@hq.doe.gov.

Domains

Risk Management (RM): Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Asset Identification, Change, and Configuration Management (ACM): Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

Identity and Access Management (IAM): Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

Threat and Vulnerability Management (TVM): Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

Situational Awareness (SA): Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture.

Information Sharing and Communications (ISC): Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

Event and Incident Response, Continuity of Operations, and Service Restoration (IR): Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

Vendor Security Management (VSM): Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

Workforce Management (WM): Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Cybersecurity Program Management (CPM): Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

Maturity Indicator Level Definitions

MIL 0: No Practices

- Practices are not performed.

MIL 1: Initiated

- Initial practices are performed but may be ad hoc.

MIL 2: Performed

- Practices are documented.
- Stakeholders are identified and involved.
- Adequate resources are provided to support the process.
- Standards or guidelines are used to guide practice implementation.

MIL 3: Managed

- Activities are guided by policy (or other directives) and governance.
- Policies include compliance requirements for specified standards or guidelines.
- Activities are periodically reviewed for conformance to policy.
- Responsibility and authority for practices are assigned to personnel.
- Personnel performing the practice have adequate skills and knowledge.

Appendix H. Maturity Profile Table Template

Domain	Objective	Actual MIL	Target MIL	# of MILs to Meet Target	# of Practices to Meet Target
1. Risk Management	Establish Cybersecurity Risk Management Strategy				
	Manage Cybersecurity Risk				
	Management Activities				
2. Asset Identification, Change, and Configuration Management	Manage Asset Inventory				
	Manage Asset Configuration				
	Manage Changes to Assets				
	Management Activities				
3. Identity and Access Management	Establish and Maintain Identities				
	Control Access				
	Management Activities				
4. Threat and Vulnerability Management	Identify and Respond to Threats				
	Reduce Cybersecurity Vulnerabilities				
	Management Activities				
5. Situational Awareness	Perform Logging				
	Perform Monitoring				
	Establish and Maintain a Common Operating Picture				
	Management Activities				
6. Information Sharing and Communications	Share Cybersecurity Information				
	Management Activities				
7. Event and Incident Response, Continuity of Government, and Service Restoration	Detect Cybersecurity Events				
	Escalate Cybersecurity Events and Declare Incidents				
	Respond to Incidents and Escalated Cybersecurity Events				
	Plan for Continuity				
	Management Activities				
8. Vendor Security Management	Identify Dependencies				
	Manage Dependency Risk				
	Management Activities				
9. Workforce Management	Assign Cybersecurity Responsibilities				
	Control the Workforce Life Cycle				
	Develop Cybersecurity Workforce				
	Increase Cybersecurity Awareness				
	Management Activities				
10. Cybersecurity Program Management	Establish Cybersecurity Program Strategy				
	Sponsor Cybersecurity Program				
	Establish and Maintain Cybersecurity Architecture				
	Perform Secure Software Development				
	Management Activities				

Appendix I. Gap Mitigation Plan Template

Gap Mitigation Plan

This gap mitigation plan has been developed specifically for *[Organization]* as a result of the Cybersecurity Capability Maturity Model evaluation conducted on *[date of evaluation].* For questions regarding the gap mitigation plan, please contact the owner of the plan, *[Person responsible for the plan].*

Domain	Objective	Practice	Gap Summary	Prioritization	Mitigation Action	Milestones	Responsible Party	Cost Estimate
[From Dams-C2M2]	*[From Dams-C2M2]*	*[From Dams-C2M2]*	*[Organization-specific details or needs to complete the practice]*	*[High/low, short-/mid-/long-term]*	*[Project or activity to address the gap]*	*[Significant event for the action (deadlines or timeframe)]*	*[Person responsible for implementing the mitigation action]*	*[Approximate cost of the mitigation action]*

Appendix J. Source Documents

Sector Documents

Dams Sector Cybersecurity Capability Maturity Model (C2M2), Washington, D.C.: U.S. Department of Energy, 2016

Dams Sector: Cybersecurity Framework Implementation Guidance, Washington, D.C.: U.S. Department of Homeland Security, 2015

Dams Sector Cybersecurity Program Guidance, Washington, D.C.: U.S. Department of Homeland Security, 2016

Dams Sector Security Guidelines, Washington, D.C.: U.S. Department of Homeland Security, 2015

Dams Sector-Specific Plan: An Annex to the NIPP 2013, Washington, D.C.: U.S. Department of Homeland Security, 2015

Federal Agency Guidelines

Cybersecurity Capability Maturity Model (C2M2), Version 1.1, Washington, D.C.: U.S. Department of Energy and U.S. Department of Homeland Security, 2014

Cybersecurity Capability Maturity Model (C2M2) Facilitator Guide, Version 1.1, Washington, D.C.: U.S. Department of Energy and U.S. Department of Homeland Security, 2014

Cybersecurity Capability Maturity Model (C2M2) Toolkit, Version 1.1, Washington, D.C.: U.S. Department of Energy and U.S. Department of Homeland Security, 2014

Electricity Subsector Cybersecurity Capability Maturity Model (C2M2), Version 1.1, Washington, D.C.: U.S. Department of Energy & U.S. Department of Homeland Security, 2014

Electricity Subsector Cybersecurity Risk Management Process, Washington, D.C.: U.S. Department of Energy, 2012

Energy Sector Cybersecurity Framework Implementation Guidance, Washington, D.C.: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2015

Homeland Security Exercise and Evaluation Program (HSEEP), Washington, D.S.: U.S. Department of Homeland Security, 2013

Security Guideline for the Electricity Sector: Protecting Sensitive Information, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2012

Homeland Security