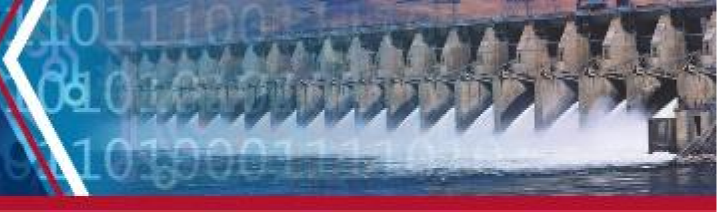
Dams Sector Cybersecurity Capability Maturity Model

Frequently Asked Questions



What is the Dams Sector Cybersecurity Capability Maturity Model?

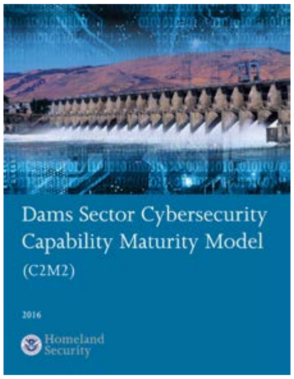
The Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2) advances the practice of cybersecurity risk management across the Dams Sector by providing all owners and operators, regardless of size or type, with a flexible tool to help them evaluate, prioritize, and improve their own cybersecurity capabilities. Once implemented, the Dams-C2M2 can be used by an organization to evaluate its cybersecurity capabilities consistently, communicate its capability levels in meaningful terms, and inform the prioritization of its cybersecurity investments.

Why should my organization implement the Dams-C2M2?

Numerous cyber intrusions across critical infrastructure sectors have demonstrated the urgent need for improved cybersecurity in the United States. Because cyber threats are continuing to grow and represent some of the most serious operational risks facing modern organizations, strong cybersecurity is essential for organizations that use cyber systems to manage or control critical physical processes.

Where do I start with implementation? What are the first steps?

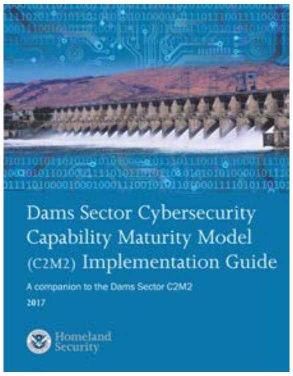
Important first steps to take when implementing the Dams-C2M2 include reviewing important C2M2 materials (e.g., the Dams-C2M2 and the Implementation Guide), determining what function to evaluate (i.e., a subset of operations of a facility or organization) and when to conduct the evaluation (e.g., in time to influence the organization's budget), and obtaining buy-in from management to dedicate time to the process and use the results. Cybersecurity and risk management discussions with internal divisions or personnel can help to make these early decisions.



Dams Sector Cybersecurity Capability Maturity Model (C2M2)

2016

Homeland Security



Dams Sector Cybersecurity Capability Maturity Model (C2M2) Implementation Guide

A companion to the Dams Sector C2M2

2017

Homeland Security

Is the Dams-C2M2 required under a regulatory framework?

No, implementation of the Dams-C2M2 is voluntary, based on an organization's needs and priorities. The model and implementation process leverage and build upon existing efforts and best practices and are aligned with the *National Institute of Standards and Technology (NIST) Cybersecurity Framework* and the *Roadmap to Secure Control Systems in the Dams Sector*. The C2M2 also supports implementation of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636).

What is included in the Dams-C2M2?

The Dams-C2M2 includes a model and implementation process. The *model* is organized into 10 domains, each containing a logical grouping of cybersecurity objectives and practices. There are 37 objectives across the domains, and each objective has associated practices. How many and which cybersecurity practices the organization implements, as well as the consistency of their application, indicate the maturity level for that objective. The *implementation process* includes five major steps centered on a discussion-based evaluation:

- **Prepare to Use the Model:** The organization plans for the model's effective and efficient implementation, including selecting what to evaluate, choosing evaluation participants, and organizing evaluation logistics.
- **Evaluate Maturity:** During the evaluation, participants measure the cybersecurity maturity of the function by using a scale of maturity indicator levels (MILs), 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.
- **Analyze Gaps:** Participants determine which gaps are meaningful and important to address, i.e., whether closing these gaps would best enable the organization to meet its business objectives and cybersecurity strategy.
- **Prioritize Gaps:** Participants prioritize the most meaningful gaps and identify activities/actions to fully implement the practices needed to achieve the target capability in specific domains.
- **Plan to Fill Gaps:** Post-evaluation, the organization develops a plan to address the selected gaps and tracks implementation of the plan.

The Dams-C2M2 model and implementation process look complicated. Is the process difficult to complete?

The model is organized into 10 logical cybersecurity domains and associated objectives and practices. Because the model provides descriptive, not prescriptive, guidance to help organizations improve their cybersecurity capabilities, the model practices tend to be abstract so they can be easily adapted by facilities and organizations of various structures, functions, and sizes. The implementation process is systematic and repeatable so that an organization can apply the model step by step and progress through preparation, evaluation, analysis, prioritization, and implementation.

Who should participate in the Dams-C2M2 evaluation?

Selecting the appropriate personnel to participate in the evaluation is a key early step in implementing the model. 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 included in the model. In general, personnel selected to participate in the evaluation should include operations, management, and any others who could provide useful information about the organization's cybersecurity practices. The Implementation Guide provides more specific examples of suitable participants.

How long will the Dams-C2M2 process take to complete?

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 effectiveness of the facilitator, and whether homework was assigned and completed. Implementation process actions in advance of the evaluation (e.g., preparing) and post-evaluation (e.g., gap analysis and plan implementation) will require additional time. The total time to complete the C2M2 implementation process depends on how broad the scope of the C2M2 is, how extensive the gaps and mitigation actions are, and the availability of personnel dedicated to the process.

What support is available to my organization to implement the Dams-C2M2?

The Dams Sector-Specific Agency (SSA) is available to answer questions about the model or implementation process and can provide Dams Sector owners and operators access to all C2M2 materials. In addition, the SSA will host a C2M2 informational webinar for organizations interested in implementing the Dams-C2M2. Please email dams@hq.dhs.gov with questions or requests. A complete suite of documents has been developed by the Dams Sector Joint Council, including the C2M2 model, Implementation Guide, and templates to document results of implementing the C2M2.

- **The Dams-C2M2** introduces the complete maturity model—including core concepts, model architecture, and domains—and describes how the model relates to the Dams Sector cyber landscape and risk management.
- **The Implementation Guide** highlights approaches to implementing both the administrative and substantive elements of the model. 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.
- **Templates** aid in data collection, analysis, and decision documentation. They can be tailored by the organization based on its structure, resources, and current processes.

What happens to the results of my organization's Dams-C2M2?

The organization retains all results from implementing the Dams-C2M2. The results help improve an organization's cybersecurity maturity not only by identifying needs and solutions, but also by providing evidence to support budget requests and long-term strategy. As resources become available, they can be applied to fill gaps. Results include a maturity profile listing actual and target MILs, evidence supporting MIL selection, a mitigation plan inclusive of prioritized gaps and associated mitigation actions, and an official record of the C2M2 (an after-action report) that combines all of the results into a single document. Results can be used for other purposes, such as informing or contributing to strategic planning, or justifying updates to facilities and systems.

Suggestions for improvement on the Dams-C2M2 implementation process may be submitted to the Dams SSA by email to dams@hq.dhs.gov.