C2M2 Overview

Brian Benestelli

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0633

Agenda

Introduction

Core Concepts

C2M2 Overview

Conducting a Self-Evaluation

Questions

About Me

Brian Benestelli
Cybersecurity Engineer
Acting Team Lead, Resilience Diagnostics

CERT Division
Software Engineering Institute

bdbenestelli@cert.org

Carnegie Mellon University | Software Engineering Institute | CERT

Software Engineering Institute (SEI)

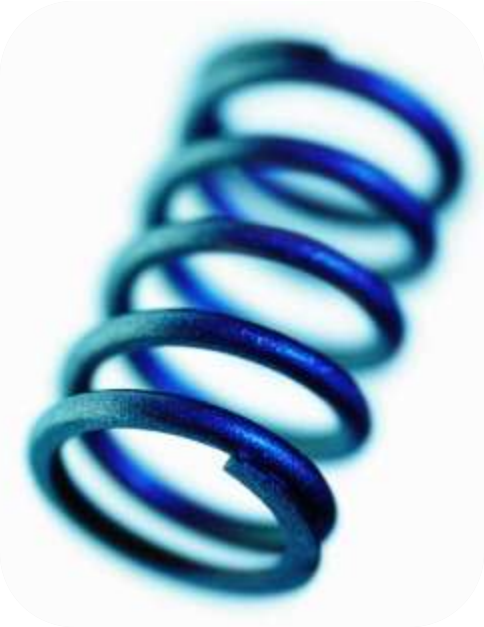
- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve their development, operation, and management of software-intensive and networked systems

CERT Division – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at the SEI
- Focused on information and cybersecurity, risk management, operational resilience, insider risk, governance, and security metrics

Core Concepts

What is Resilience?



"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

– Presidential Policy Directive – PPD 21
Critical Infrastructure Security and Resilience
February 12, 2013

This definition explicitly includes ***attacks, accidents, or naturally occurring threats or incidents,*** intentionally expanding resilience beyond a cyber definition.

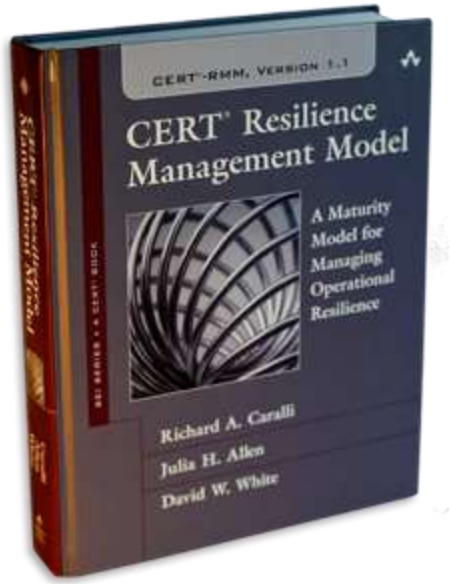
What Do We Mean by *Operational Resilience*?

***"Operational resilience:** the organization's ability to adapt to risk that affects its core operational capacities; the **emergent** property of an organization that can **continue to carry out its mission** after disruption that does not exceed its operational limit"*

– CERT-RMM

Operational resilience expands on the PPD 21 definition of resilience, which emphasizes the need to define operational limits while stressing the emergent nature of resilience.

What is the CERT-RMM?



The CERT Resilience Management Model (CERT-RMM) is a process improvement model for managing operational resilience.

It provides guidelines and practices for

- converging security, business continuity, disaster recovery, and IT ops
- implementing, managing, and sustaining operational resilience activities
- managing operational risk through process
- measuring and institutionalizing the resilience process

CERT-RMM provides a common vernacular and basis for planning, communicating, and evaluating improvements.

It is organized into 26 process areas.

Maturity Models

"A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline." – C2M2 V2.1

Attributes define levels in a maturity model

- Capability progression: crawl, walk, run
- Process maturity: institutionalization (a.k.a., what makes it "stick")

Having measurable transitions between the levels enables an organization to use the scaling to:

- define its current state
- define its future, more "mature" state
- identify the attributes it must attain to reach that future state

Cybersecurity Capability Maturity Model (C2M2) Overview

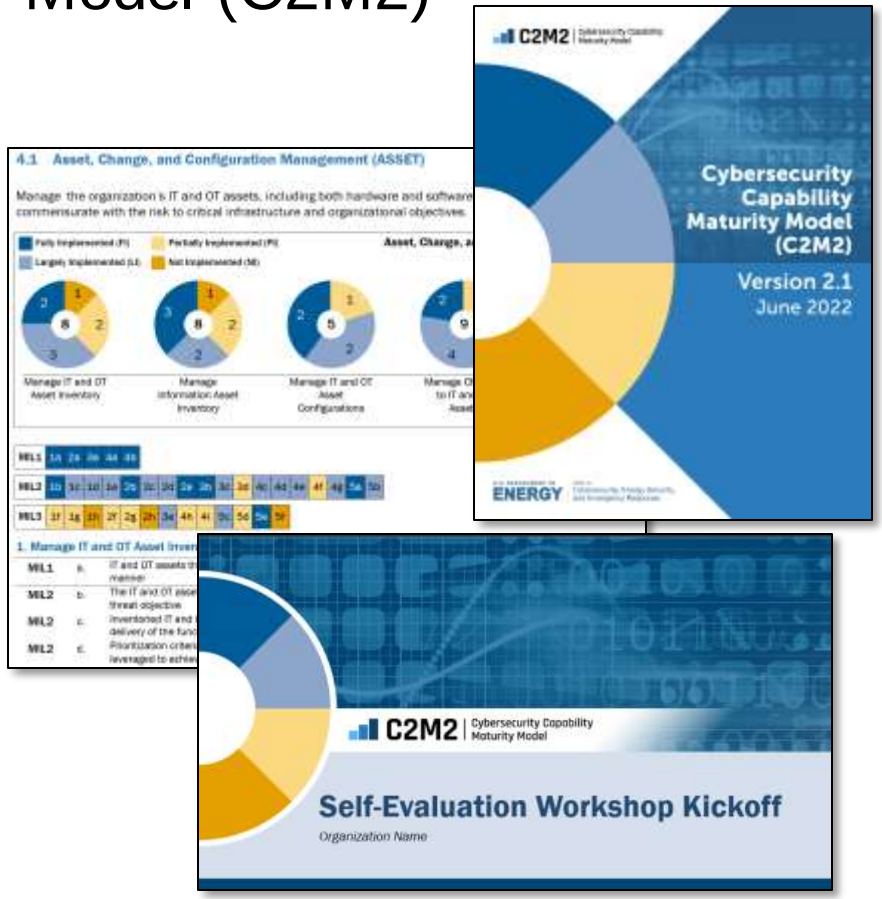
Cybersecurity Capability Maturity Model (C2M2)

Designed for any organization regardless of ownership, structure, size, or industry

It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

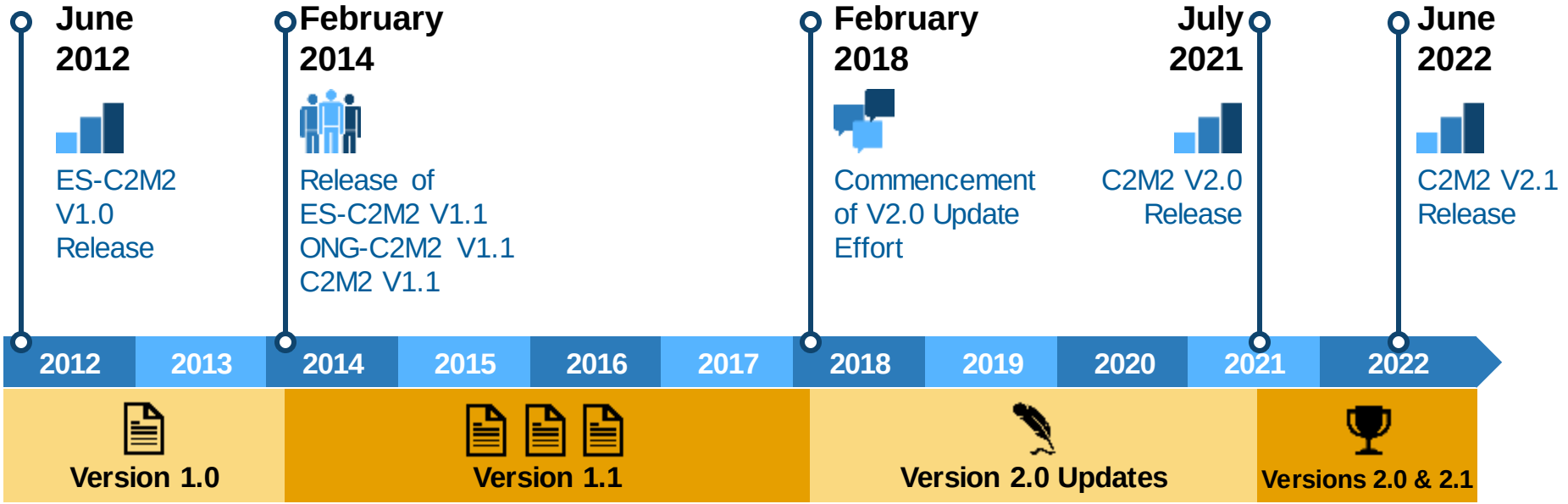
Developed through extensive public-private partnership with numerous government, industry, and academic organizations

Enables consistent evaluation of cybersecurity practices and tracking of progress over time



[DOE C2M2 Program Page]

C2M2 Model Evolution

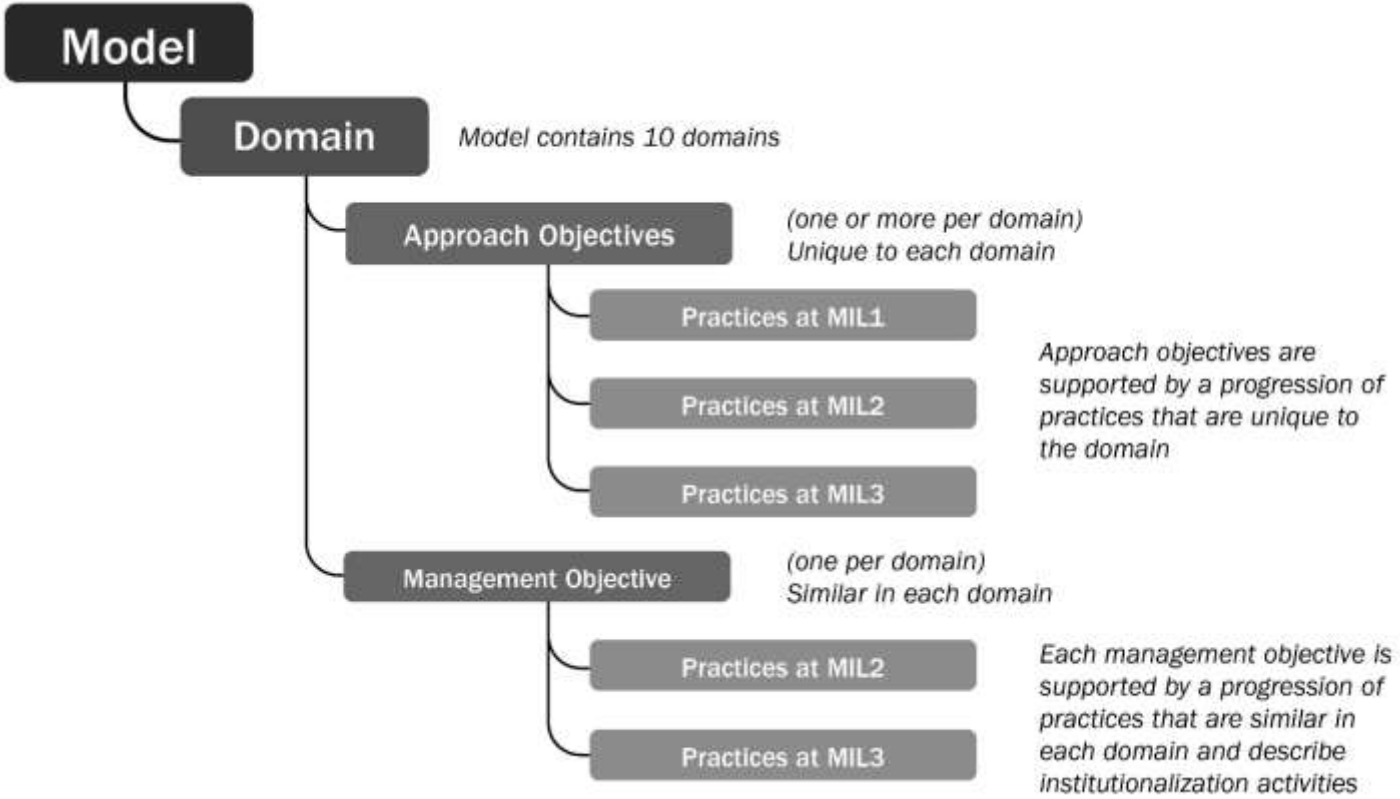


Model Includes 10 Domains

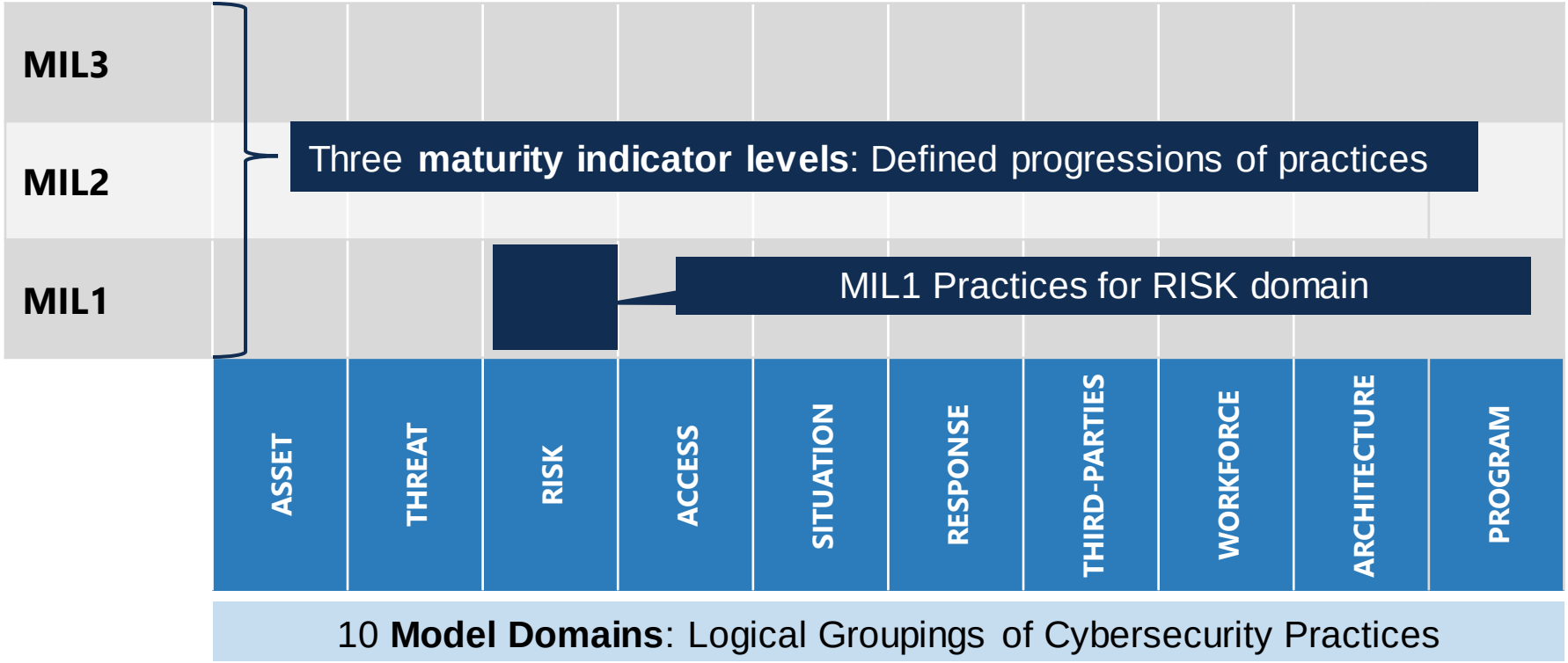
ASSET	Asset, Change, and Configuration Management
THREAT	Threat and Vulnerability Management
RISK	Risk Management
ACCESS	Identity and Access Management
SITUATION	Situational Awareness
THIRD-PARTIES	Third-Party Risk Management
RESPONSE	Event and Incident Response, Continuity of Operations
ARCHITECTURE	Cybersecurity Architecture
WORKFORCE	Workforce Management
PROGRAM	Cybersecurity Program Management

- Domains are logical groupings of cybersecurity practices
- Each domain has a short name for ease of reference

Organization of a Domain



Model at a Glance



Maturity Indicator Levels

Level	Description
MIL0	Practices are not performed
MIL1	Initial practices are performed but may be ad hoc (performance depends largely on the initiative and experience of the individual or team)
MIL2	**Management Characteristics** ▪ Practices are documented ▪ Adequate resources are provided to support the process **Approach Characteristic** ▪ Practices are more complete or advanced than at MIL1
MIL3	**Management Characteristics** ▪ Activities are guided by policies (or other organizational directives) ▪ Responsibility, accountability, and authority for performing the practices are assigned ▪ Personnel performing the practices have adequate skills and knowledge ▪ The effectiveness of activities in the domain is evaluated and tracked **Approach Characteristic** ▪ Practices are more complete or advanced than at MIL2

Using the Model

Perform a Self-Evaluation: determine the implementation of cybersecurity activities within the organization

Analyze Identified Gaps: determine whether the gaps are meaningful and important and should be addressed

Prioritize and Plan: prioritize the actions needed to fully implement the practices to achieve the desired capability

Implement Plan: implement the plans defined in the previous step to address the identified gaps

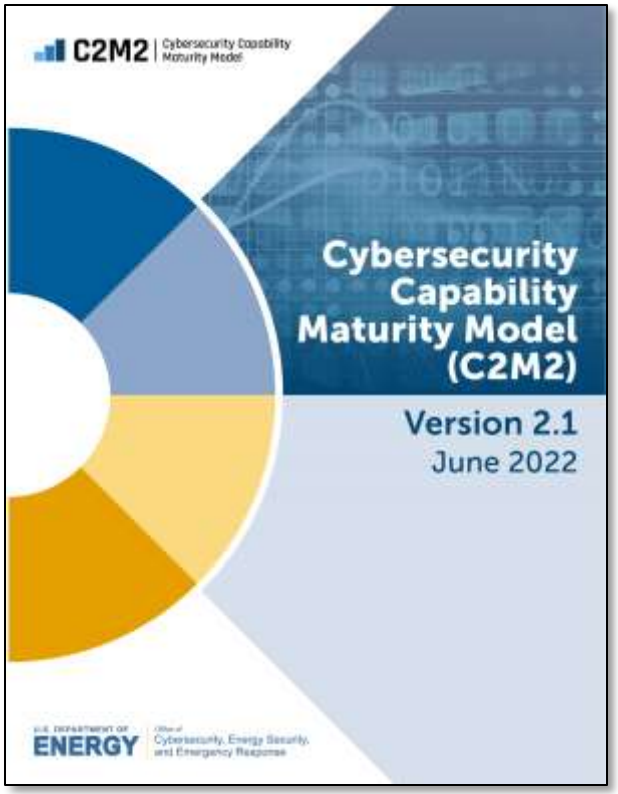
C2M2 Resources

Model Document

Foundational document

Sections

- Core concepts
- Model architecture
- Using the model
- Model domains



Self-Evaluation Tools

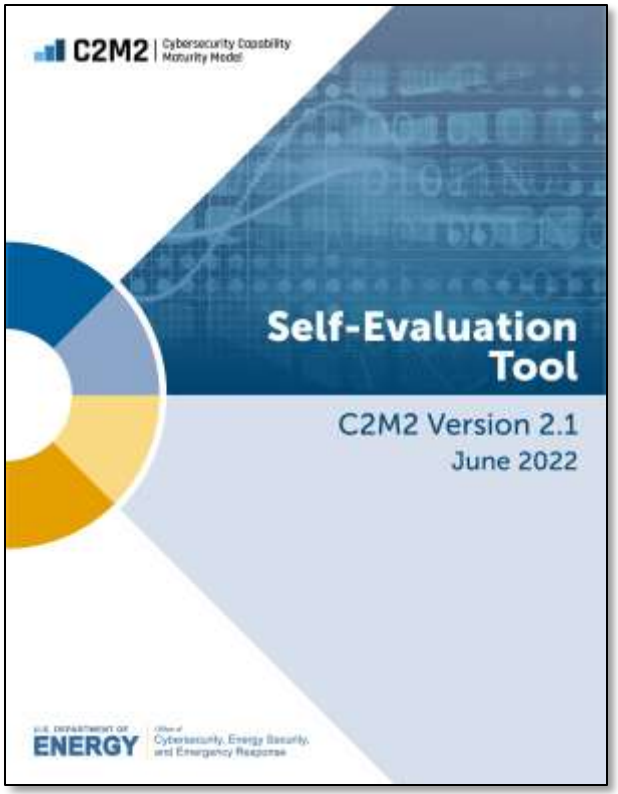
Two tools are available

- PDF-Based
- HTML-Based

Organizations can use these tools to conduct a self-evaluation

They can also be used to compare the results of up to five self-evaluations

Designed to be interoperable

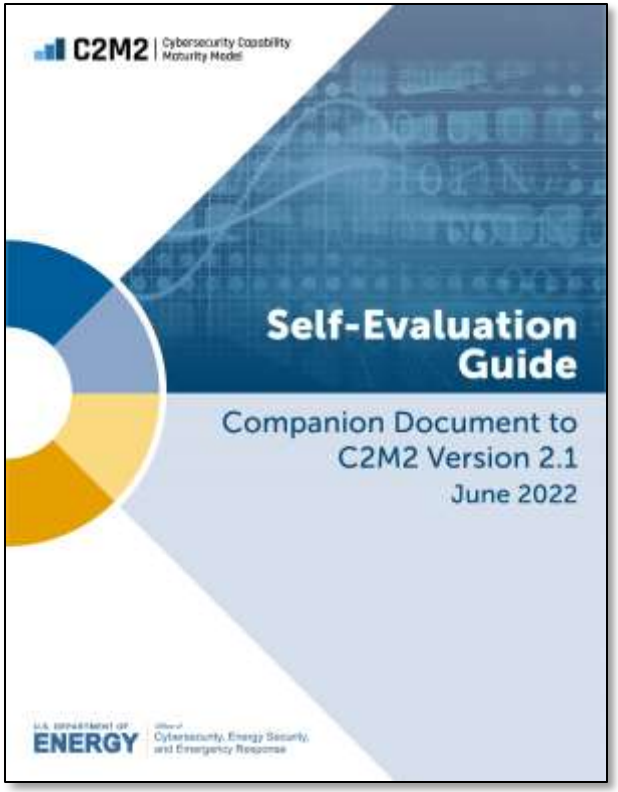


Self-Evaluation Guide

Guidance for organizations preparing to hold a self-evaluation workshop

- Preparation
- Conducting the workshop
- Follow-up activities

Additional information in appendices



C2M2 Model Practices (Excel File)

Domain	MIL	Practice	Practice Text	Help Text
ASSET	1	ASSET-1a	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	Assets derive their value and importance through their association with the aspects of the function's operations controls. At MIL1, the inventory may be produced in an ad hoc manner. Organizations should consider the differ · virtualized assets · regulated assets · assets managed by a third party · software · bring your own device (BYOD) assets · cloud assets (public, hybrid, or private service, software as a service, platform as a service, and infrastructure as · mobile assets · field assets · assets connected through different networks or communications technologies (e.g., telephone modem, cellular · network and communications assets · backup, spare, and redundant assets, including dormant virtualized assets · non-operational assets, assets undergoing repair, assets undergoing maintenance · assets reliant on specific infrastructure such as wireless networks, positioning navigation and timing services, an · assets that may be considered to be part of the Internet of things or industrial Internet of things · assets that have the potential to be untracked, unclaimed, or otherwise overlooked, such as legacy assets, comm An inventory is not meant to imply that a single list is required; multiple repositories, documents, or systems may consolidated to avoid potential risks related to managing multiple repositories. **Related Practices** · *Progression* : This practice is part of a practice progression. Practice progressions are groups of related practices ASSET-1a, ASSET-1b, ASSET-1f, ASSET-1g

Self-Evaluation Kickoff Presentation

Resource for facilitators who are conducting a self-evaluation

Provides an overview of C2M2

Details the self-evaluation process

Explains how to interpret reporting

Self-Evaluation Tool User Guides

User guides that provide step-by-step instructions on how to use both self-evaluation tools

In-Development Resources

C2M2 Overview Presentation

Self-Evaluation Cheat Sheet

Sample Threat Profile

C2M2-CMMC Supplemental Guidance

Mappings

- C2M2 V1.1 to C2M2 V2.1
- C2M2 V2.0 to C2M2 V2.1
- C2M2 V2.1 to CSF, CSF to C2M2 V2.1

Tool Demo

Thank you!

Questions?