Carnegie Mellon University
Software Engineering Institute

[Distribution Statement A] Approved for public release and unlimited distribution.

C2M2 Overview

Brian Benestelli

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2022 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-0633

Agenda

Introduction

Core Concepts

C2M2 Overview

Conducting a Self-Evaluation

Questions

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

About Me

Brian Benestelli
Cybersecurity Engineer
Acting Team Lead, Resilience Diagnostics

CERT Division
Software Engineering Institute

bdbenestelli@cert.org

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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.

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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”*

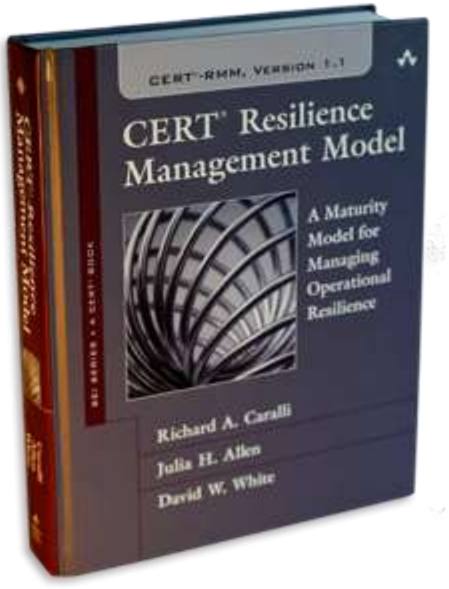
– CERT-RMM

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.

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

What is the CERT-RMM?


CERT-RMM, VERSION 1.1
CERT Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White

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

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

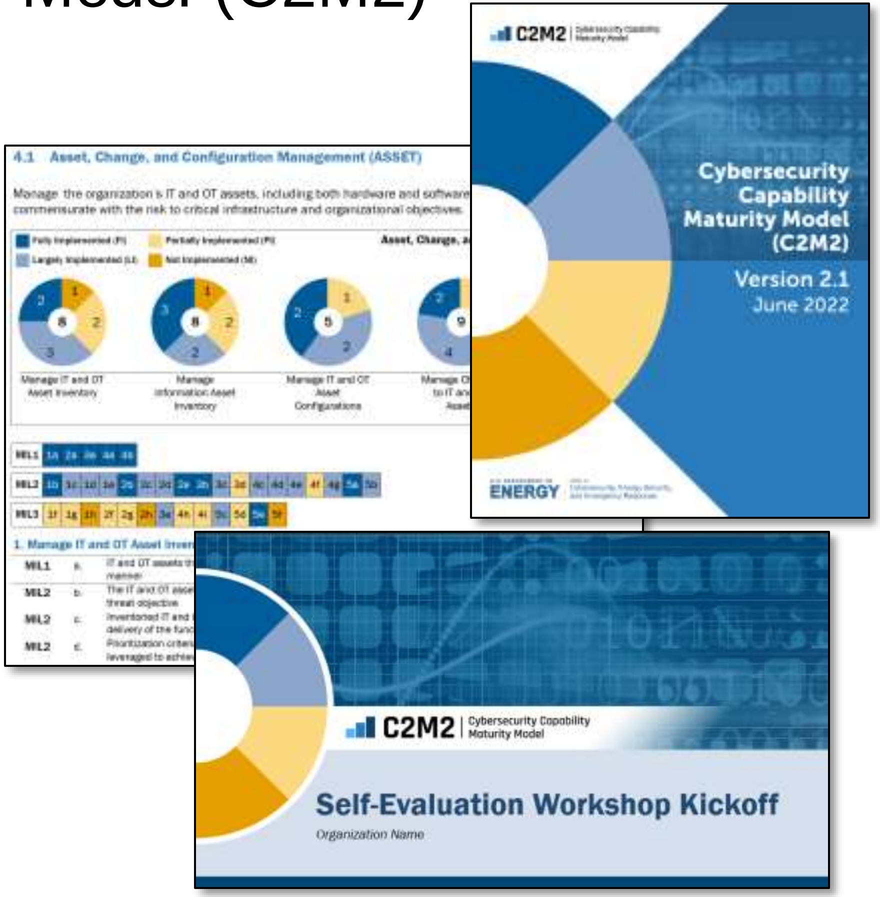
Cybersecurity Capability Maturity Model (C2M2)

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



4.1 Asset, Change, and Configuration Management (ASSET)

Manage the organization s IT and OT assets, including both hardware and software commensurate with the risk to critical infrastructure and organizational objectives.

C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2)

Version 2.1
June 2022

ENERGY

Self-Evaluation Workshop Kickoff

Organization Name

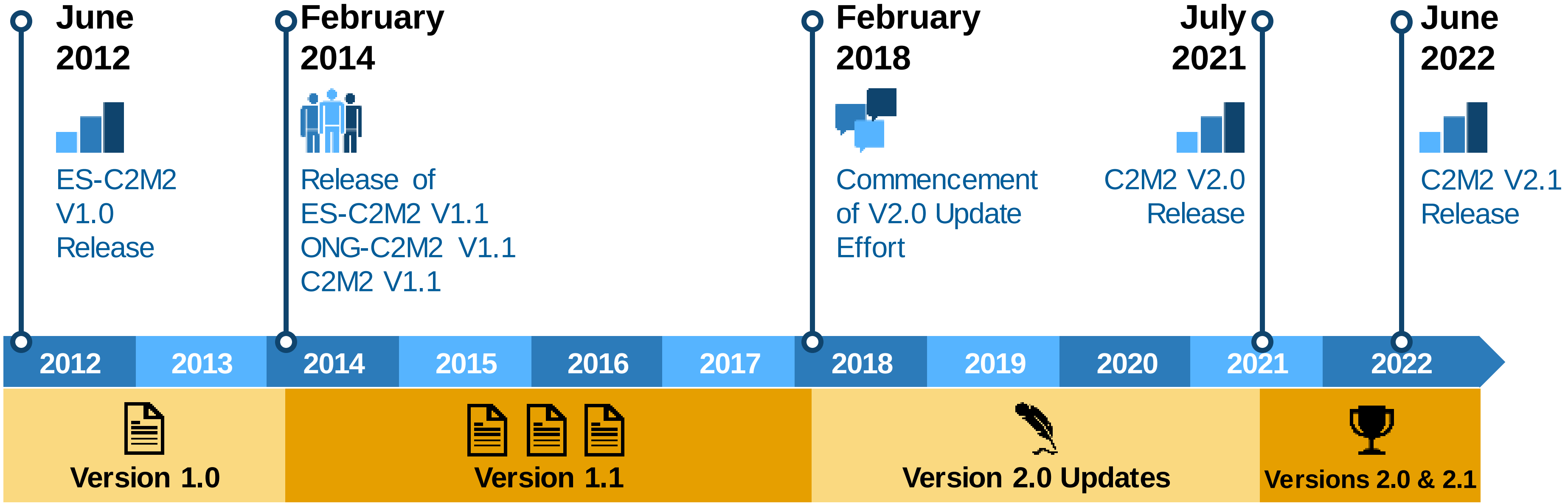
Fully Implemented (FI)
Partially Implemented (PI)
Largely Implemented (LI)
Not Implemented (NI)
Manage IT and OT Asset Inventory
Manage Information Asset Inventory
Manage IT and OT Asset Configurations
MIL1
MIL2
MIL3

[DOE C2M2 Program Page](#)

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

C2M2 Model Evolution



June 2012

ES-C2M2 V1.0 Release

February 2014

Release of ES-C2M2 V1.1 ONG-C2M2 V1.1 C2M2 V1.1

February 2018

Commencement of V2.0 Update Effort

July 2021

C2M2 V2.0 Release

June 2022

C2M2 V2.1 Release

2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

Version 1.0

Version 1.1

Version 2.0 Updates

Versions 2.0 & 2.1

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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

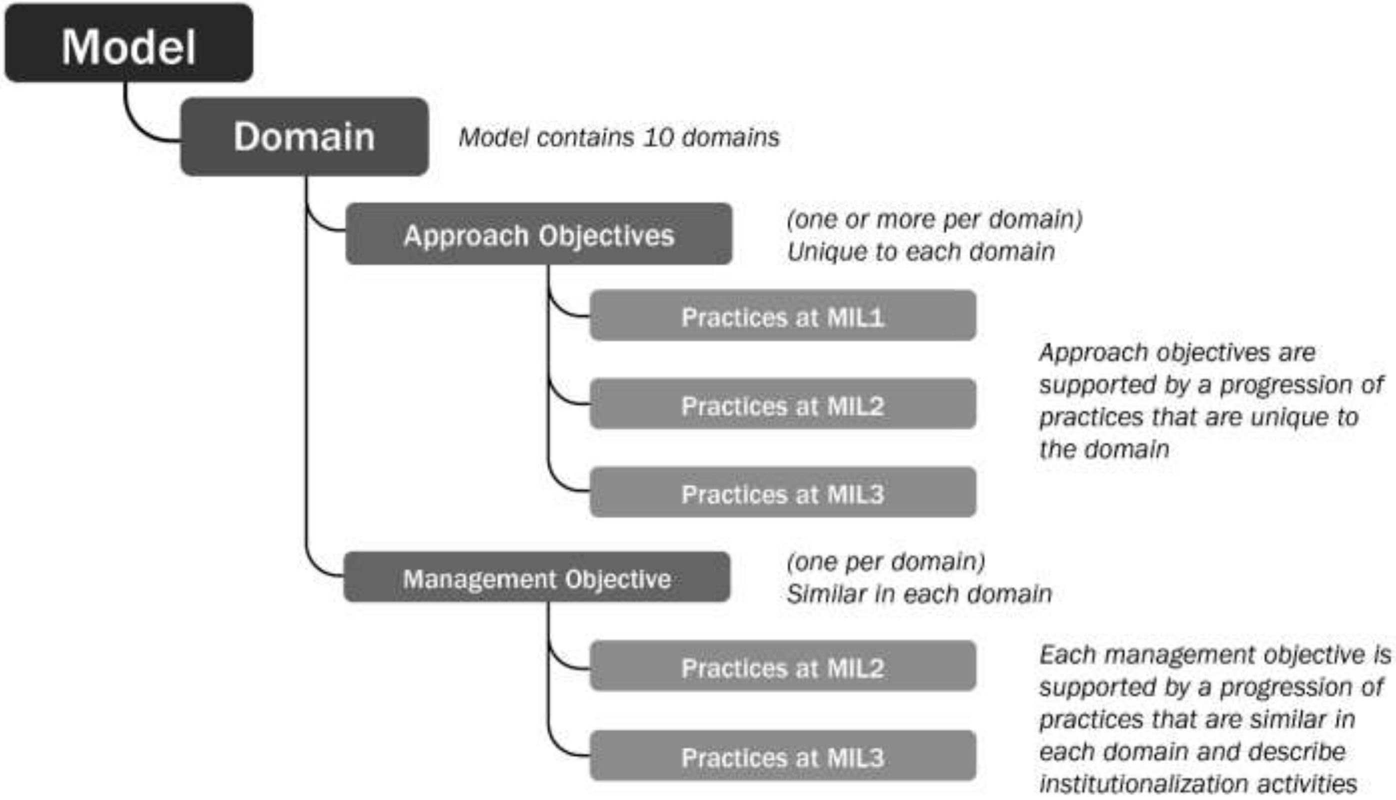
ARCHITECTURE Cybersecurity Architecture

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

Domain

Model contains 10 domains

Approach Objectives

(one or more per domain)
Unique to each domain

Practices at MIL1

Practices at MIL2

Practices at MIL3

Approach objectives are supported by a progression of practices that are unique to the domain

Management Objective

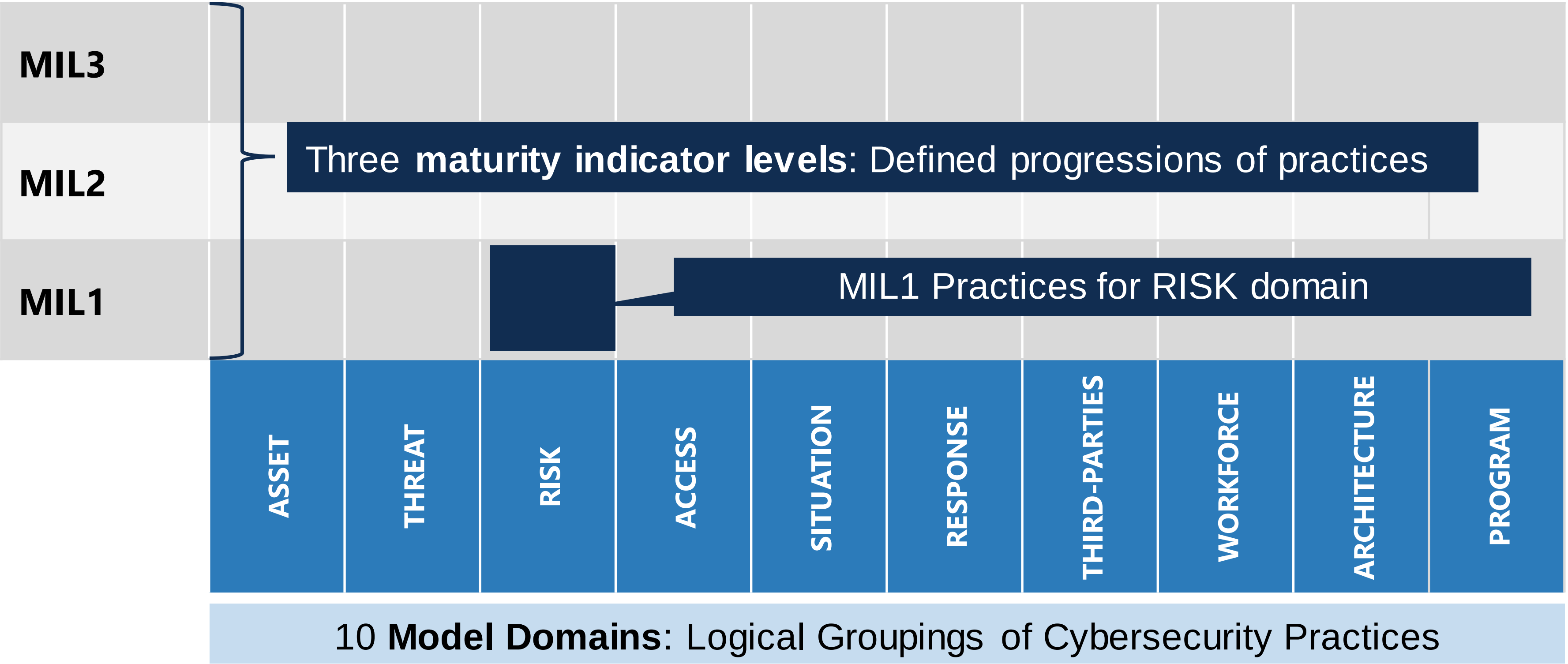
(one per domain)
Similar in each domain

Practices at MIL2

Practices at MIL3

Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

Model at a Glance



Three **maturity indicator levels**: Defined progressions of practices

MIL1 Practices for RISK domain

10 **Model Domains**: Logical Groupings of Cybersecurity Practices

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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

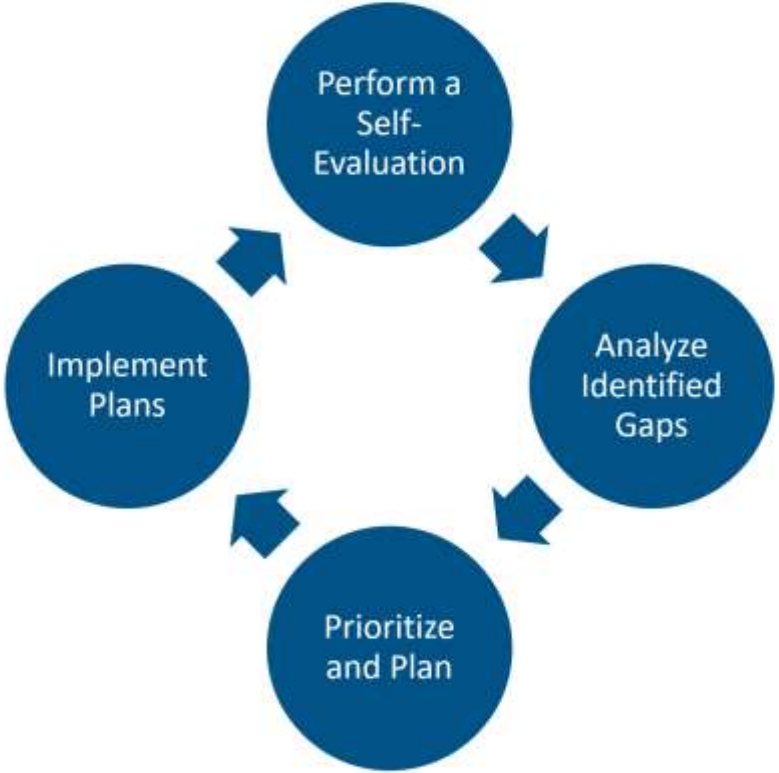
Using the Model

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



© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

C2M2 Resources

© 2022 Carnegie Mellon University

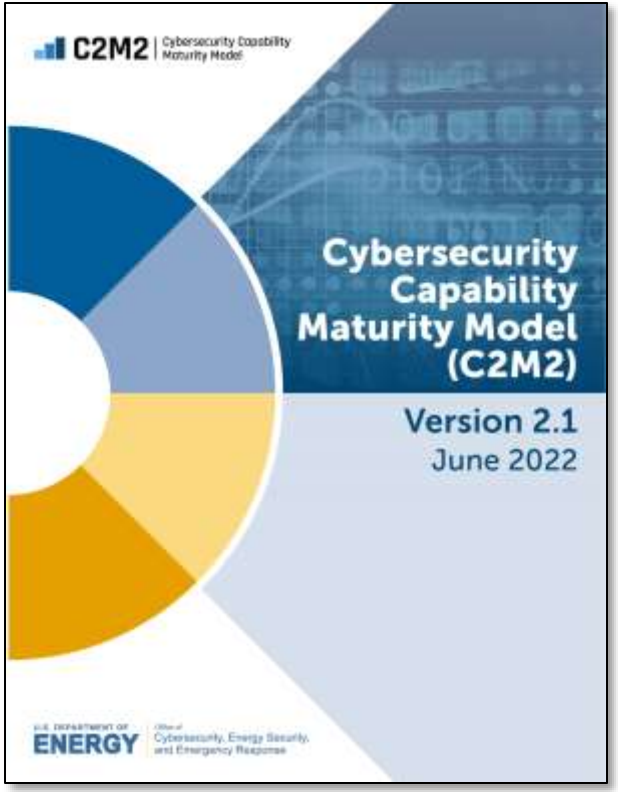
[Distribution Statement A] Approved for public release and unlimited distribution.

Model Document

Foundational document

Sections

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



C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2)

Version 2.1
June 2022

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Self-Evaluation Tools

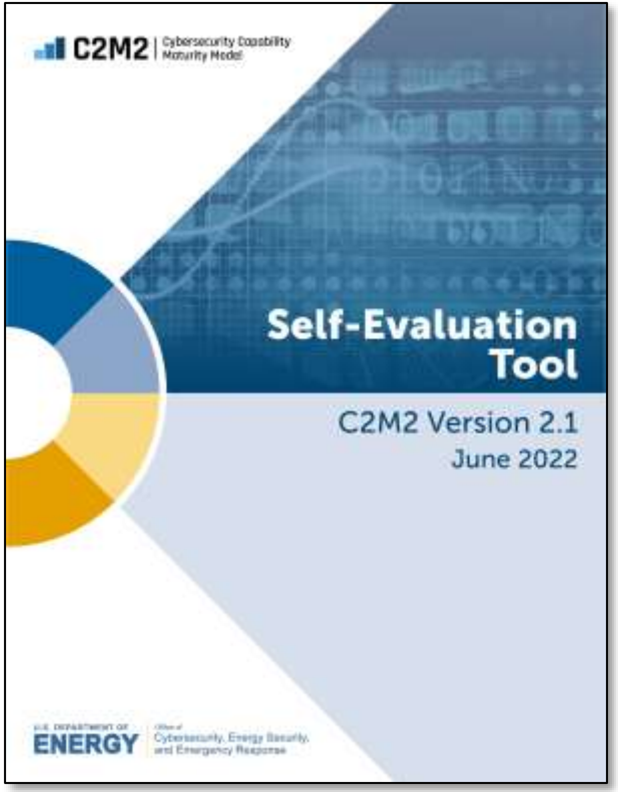
Two tools are available

- 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



C2M2 | Cybersecurity Capability Maturity Model

Self-Evaluation Tool

C2M2 Version 2.1

June 2022

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

© 2022 Carnegie Mellon University

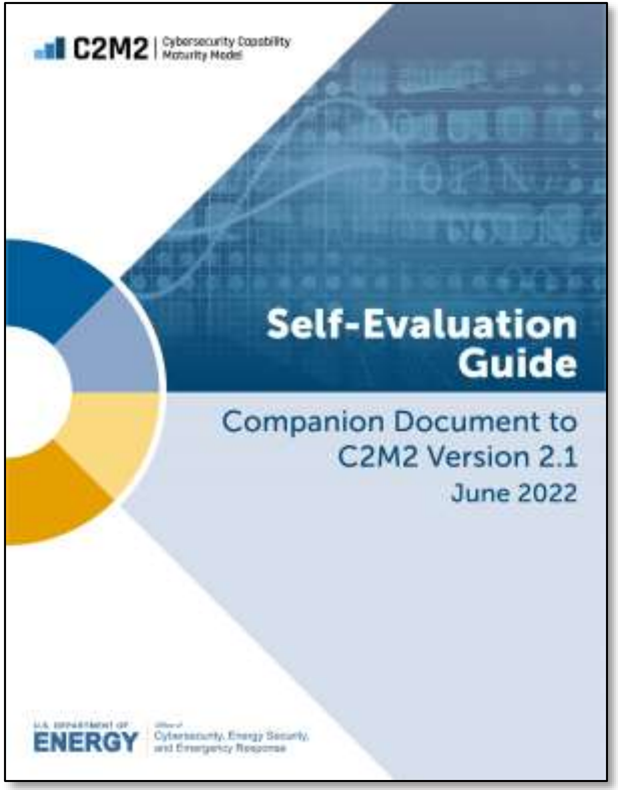
[Distribution Statement A] Approved for public release and unlimited distribution.

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 | Cybersecurity Capability Maturity Model

Self-Evaluation Guide

Companion Document to C2M2 Version 2.1

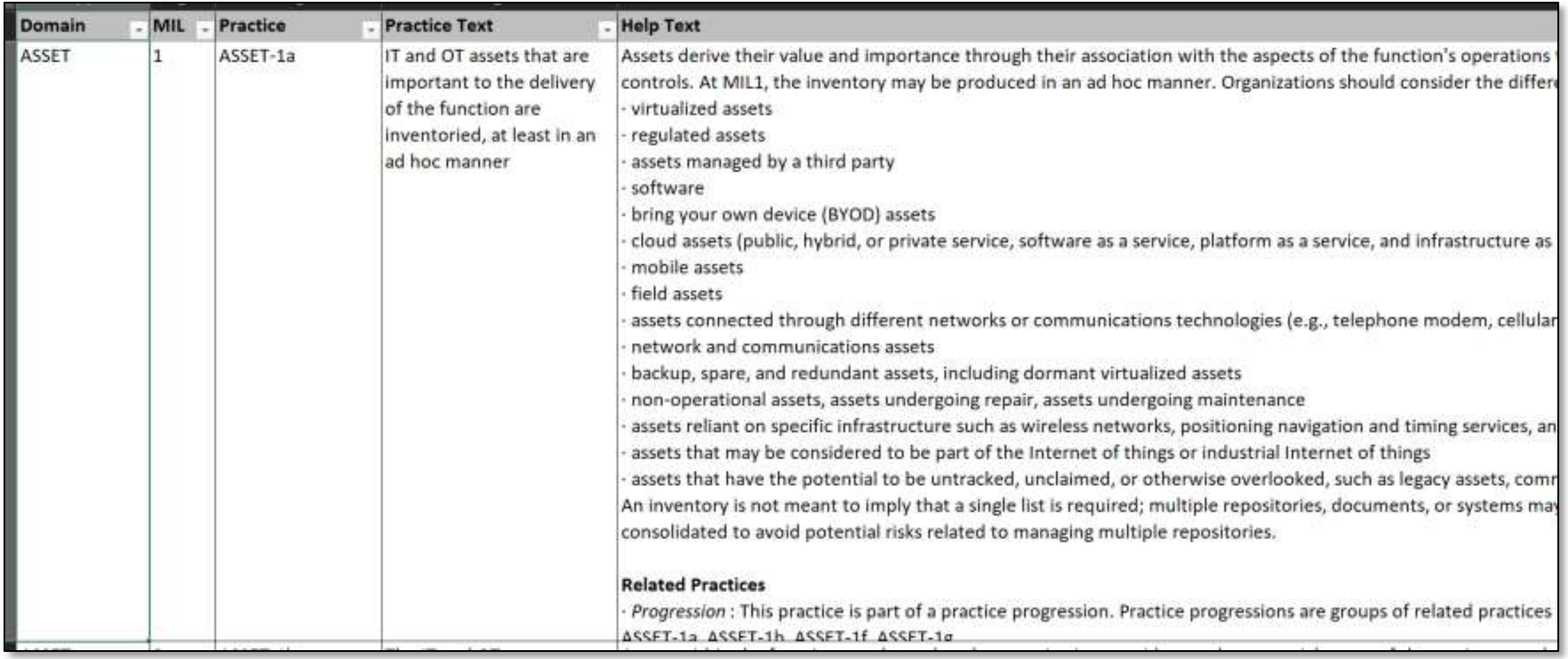
June 2022

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

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 differe - 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, comr 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

C2M2 | Cybersecurity Capability Maturity Model

Self-Evaluation Workshop Kickoff

Organization Name

Self-Evaluation Tool User Guides

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

C2M2 | Cybersecurity Capability Maturity Model

PDF-Based To
User Gu

User Guide fo
PDF-
Self-Evaluati
C2M2 Ve

U.S. Department of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

C2M2 | Cybersecurity Capability Maturity Model

HTML-Based Tool
User Guide

User Guide for the
HTML-Based
Self-Evaluation Tool
C2M2 Version 2.1
June 2022

U.S. Department of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

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

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Tool Demo

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Thank you!

Questions?

© 2022 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.