C2M2 | Cybersecurity Capability Maturity Model

PNNL-31860

Step-By-Step Instructions for Using the Cybersecurity Capability Maturity Model (C2M2) Online Tool

C2M2 Version 2.0

August 2021

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

TABLE OF CONTENTS

LIST OF FIGURES

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This Cybersecurity Capability Maturity Model (C2M2) was developed through a collaborative effort between public- and private-sector organizations, sponsored by the United States Department of Energy (DOE) and supported by the Electricity Subsector Coordinating Council, and the Oil and Natural Gas Subsector Coordinating Council. The DOE thanks the organizations and individuals who provided their valuable input during the development of the C2M2.

The C2M2 online tool was developed by Pacific Northwest National Laboratory (PNNL) and is based on an online maturity modeling framework developed to support a number of projects that were sponsored by a variety of DOE programs and other federal agencies. Invaluable contributions to the tool were made by our industry partners.

The authors of this document are Robert Harrington, Cliff Glantz, Sri Nikhil Gourisetti, Grace McNally, Joseph Loftus, and Kade Cornelison.

The team at PNNL supporting the production of the C2M2 online tool included:

- Clifford Glantz (project manager)
- Paul Skare (principal investigator and energy sector coordinator)
- Sri Nikhil Gupta Gourisetti (online tool development task manager)
- Darlene Thorsen (mapping activity task manager)
- Easton Gervais
- Joseph Loftus
- Grace McNally
- Kade Cornelison
- Robert Harrington
- Jasmine McKenzie
- Sraddhanjoli Bhadra
- Claudia Hildebrand
- Carla Raymond
- Devan Farrell
- Aarne Nixon
- Jasmine Mckenzie
- Scott Mix

The authors are grateful for the assistance provided by Fowad Muneer (DOE Office of Cybersecurity, Energy Security, and Emergency Response) and his support team. We are also grateful for the invaluable technical contributors from other governmental and private sector organizations including, but certainly not limited to Jeanne Petty (Appligent), Alexander Petrilli (Carnegie Mellon University Software Engineering Institute), Lynna Estep (North American Transmission Forum), and Ed Ernst (North American Transmission Forum).

For questions on how to use the C2M2 tools, suggestions for tool improvements, or requests for assistance with assessments – please email C2M2@hq.doe.gov.

1. Introduction

The Cybersecurity Capability Maturity Model (C2M2) is used to conduct cybersecurity programmatic self-evaluations. It addresses the implementation and management of programmatic cybersecurity practices associated with information technology (IT) and operations technology (OT) and the environments where these assets operate. The C2M2 is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, the C2M2 is not part of any regulatory framework and is not intended for regulatory use. Rather, the C2M2 is intended to complement a comprehensive enterprise cybersecurity program. Although it is anticipated that entities subject to compliance requirements would use this model, compliance requirements are not altered in any way by this model. Please consult your compliance authority for any questions on regulatory compliance.

Since the last major update of the C2M2 in 2014, both technology and threat actors have become more sophisticated, creating new attack vectors and introducing new risks. Also, new cybersecurity standards have been developed and existing standards have been improved. The C2M2 Version 2.0 is intended to address these challenges. The C2M2 Version 2.0 incorporates enhancements to improve alignment with internationally recognized cyber standards and best practices, including the NIST Cybersecurity Framework Version 1.1 released in April 2018. In addition to technical model improvements, the usability of the C2M2 Version 2.0 is enhanced by the introduction of user-friendly online- and PDF-based tools for performing a C2M2 self-evaluation.

Background Information on the C2M2

The C2M2 Version 2.0 is organized into 10 domains:

1. Asset, Change, and Configuration Management (ASSET)
2. Threat and Vulnerability Management (THREAT)
3. Risk Management (RISK)
4. Identity and Access Management (ACCESS)
5. Situational Awareness (SITUATION)
6. Event and Incident Response, Continuity of Operations (RESPONSE)
7. Third-Party Risk Management (THIRD-PARTIES)
8. Workforce Management (WORKFORCE)
9. Cybersecurity Architecture (ARCHITECTURE)
10. Cybersecurity Program Management (PROGRAM)

Each domain is composed of two or more objectives. The objectives are target achievements that support the domain. The objectives are made up of a set of cybersecurity practices. Each practice is a specific activity that can be performed by an organization to support its cybersecurity program. Practices indicate performance at a given maturity indicator level (MIL). This C2M2 model structure is illustrated in Figure 1.1.

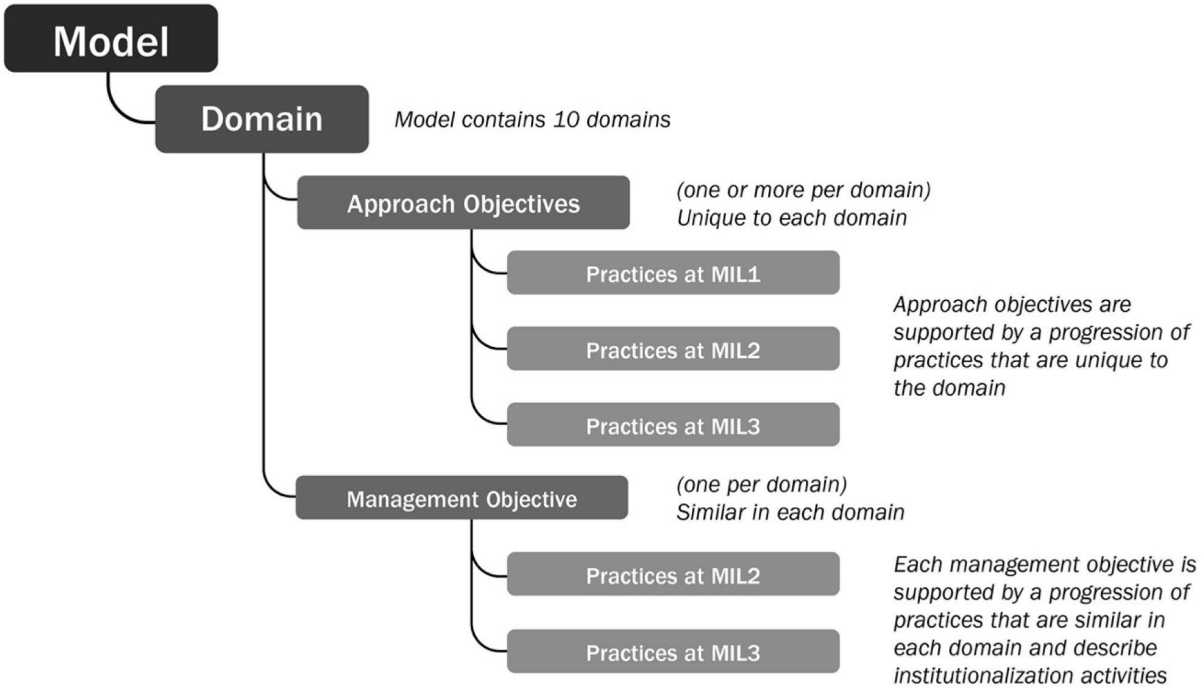

Model
Domain
Model contains 10 domains
Approach Objectives
(one or more per domain)
Unique to each domain
Practices at MIL1
Practices at MIL2
Practices at MIL3
Approach objectives are supported by a progression of practices that are unique to the domain
Management Objective
(one per domain)
Similar in 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

Figure 1.1. C2M2 Model Structure

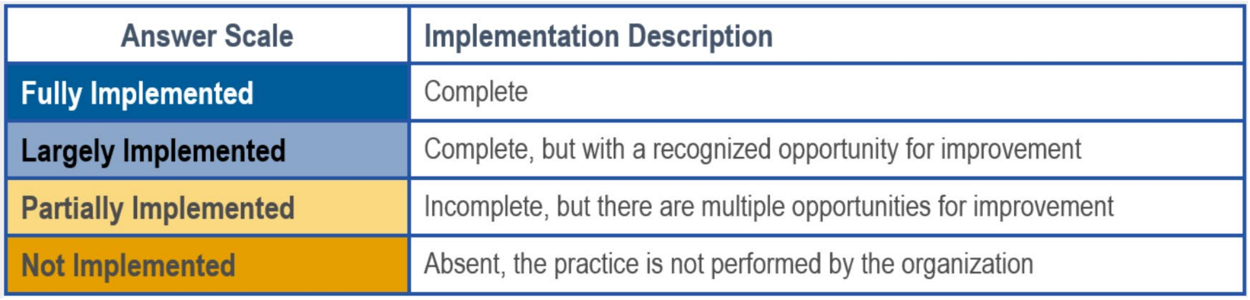
The model defines three MILs (1 through 3) that indicate a progression of maturity. Practices are assigned a MIL (either MIL1, MIL2, or MIL3) that corresponds to the level of programmatic maturity associated with that practice:

- **MIL1** represents initial activities that may be performed in an informal or ad hoc manner.
- **MIL2** activities are designed to be more complete than at MIL1, with more regular and reliable performance. Often, formal documentation is required.
- **MIL3** activities are designed to be highly mature, stable, institutionalized, and well-managed. They are often guided by high-level organizational directives, such as policy.

If all the MIL1 practices are not achieved for a specific domain or an objective, the organization is assumed to be functioning at a **MIL0** for that domain or objective.

MILs are cumulative within each domain. To earn a MIL in a given domain, an organization must perform all the practices in that level and its predecessor level(s). For example, an organization must perform all the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization must perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3. The MILs apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings in different domains.

The implementation of each practice is evaluated with a four-point answer scale (Figure 1.2). Fully and largely implemented scores indicate a "passing" level of performance for the activity; partially and not implemented scores indicate the practice does not achieve its corresponding MIL.



Answer Scale	Implementation Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete, but there are multiple opportunities for improvement
Not Implemented	Absent, the practice is not performed by the organization

Figure 1.2. The Four Point-Scale Used for Assigning a Practice Implementation Score

What Does This Document Cover?

The guidance provided in this publication is intended to provide step-by-step instructions for users of the C2M2 Version 2.0 online tool. It should be particularly helpful for first-time users of the C2M2 – including those using the tool to provide input for a self-evaluation and those who are using the tool's reporting features to assess their organization's programmatic maturity. This document includes instructions for using the tool, including:

- Finding and running the C2M2 online tool from the tool's website (https://c2m2.doe.gov).
- Navigating through the tool's pages to enter data (or review existing data) for C2M2 practices.
- Filling out the "Organization Information" page which records the scope of the self-evaluation, its date, and the key technical contributors performing the evaluation.
- Accessing each practice, viewing "help text", viewing definitions of key terms, entering practice implementation scores, and recording notes to document the rationale for practice scores.
- Reviewing summary results for the practices that make up each Objective.
- Saving input data, loading previous data files, and resetting the tool.
- Generating an output report.

This document also includes instructions for viewing and downloading a report documenting the results of an assessment. It reviews the:

- Introductory text that summarizes the model's architecture including a description of each of the domains, MILs, and implementation scoring for the practices.
- Summary results by domain, including a description of tool-generated donut diagrams and clickable features to support data analytics and data visualization.
- A summary of crosscutting management practices.
- Detailed evaluation result – including providing results for each objective in a domain.
- A detailed table containing all assessment information – including each practice statement, self-evaluation notes, and the implementation status for each practice.

- A summary table that provides information for each practice that has an appreciable implementation gap (i.e., an implementation score of “not implemented” or “partially implemented”).

Broader Document Context and Companion Information

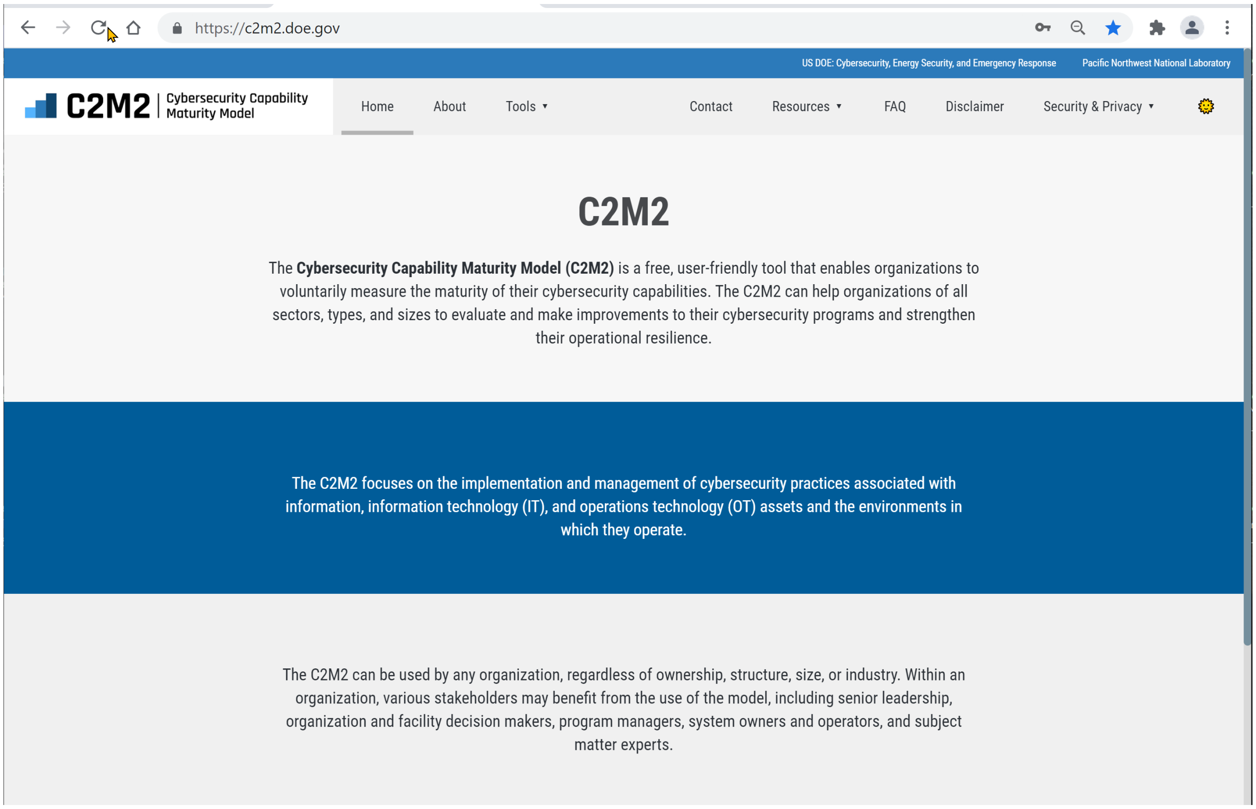
This document is a supplement to the larger C2M2 Version 2.0 guidance document (available at https://c2m2.doe.gov/resources/ and other locations). That document describes the C2M2’s main structure and content. It includes the following:

- Descriptions of core concepts that are important for interpreting the content and structure of the C2M2.
- Descriptions of the architecture of the C2M2.
- Guidance on how to use the model.
- Information on the domains, objectives, and practices used in the model.

2. Accessing the Online Tool and Entering Data

Accessing the Online C2M2 Tool

The online C2M2 tool is accessible at https://c2m2.doe.gov (Figure 2.1). The model was developed and extensively tested using Google Chrome and other internet browsers (e.g., Mozilla Firefox, Microsoft Edge) are also fully supported.


https://c2m2.doe.gov
US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾

C2M2

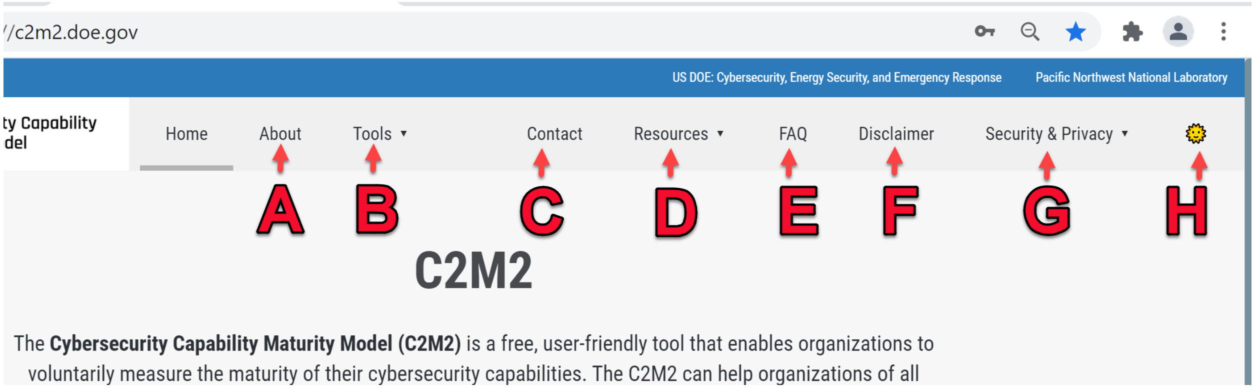
The **Cybersecurity Capability Maturity Model (C2M2)** is a free, user-friendly tool that enables organizations to voluntarily measure the maturity of their cybersecurity capabilities. The C2M2 can help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience.

The C2M2 focuses on the implementation and management of cybersecurity practices associated with information, information technology (IT), and operations technology (OT) assets and the environments in which they operate.

The C2M2 can be used by any organization, regardless of ownership, structure, size, or industry. Within an organization, various stakeholders may benefit from the use of the model, including senior leadership, organization and facility decision makers, program managers, system owners and operators, and subject matter experts.

Figure 2.1. The C2M2.doe.gov Homepage

Navigation through the website is facilitated using the navigation menu located at the top of the webpage (Figure 2.2).



C2M2

The **Cybersecurity Capability Maturity Model (C2M2)** is a free, user-friendly tool that enables organizations to voluntarily measure the maturity of their cybersecurity capabilities. The C2M2 can help organizations of all

Figure 2.2. Close-Up of the Top-Line Navigation Menu with Added Labeling

The navigation menu provides access to C2M2 webpages where the user can:

("A") learn more about the C2M2

("B") access the C2M2 online tool or request the C2M2 PDF tool

("C") obtain contact information for the C2M2 team

("D") access additional C2M2 tool information resources

("E") examine frequently asked questions

("F") examine the standard legal disclaimer for the C2M2

("G") read about how the C2M2 ensures the security and privacy of user data

("H") toggle the website between its standard "light mode" and an optional "dark mode." The dark mode has the same functionality as the default "light mode," but it employs a dark background color that some users may prefer.

To access the C2M2 model, click the "Tools" button in the navigation menu (labeled "B" in Figure 2.2). This will open a drop-down menu as shown in Figure 2.3. Click the "C2M2 Online Tool" to begin using the online tool. Clicking the "C2M2 PDF-Based Tool" will open a webpage that will provide instructions for requesting the C2M2 project office to email this PDF-based tool to you.

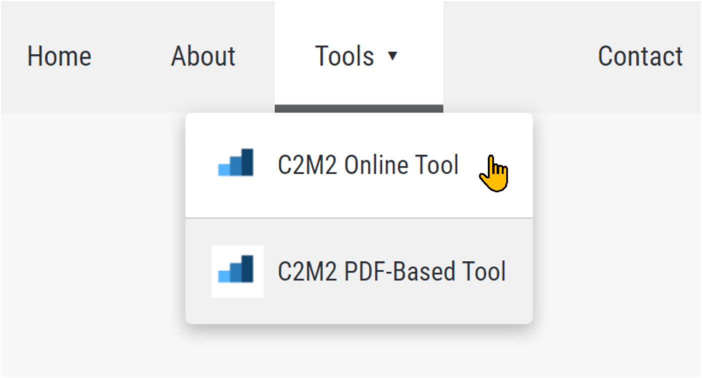
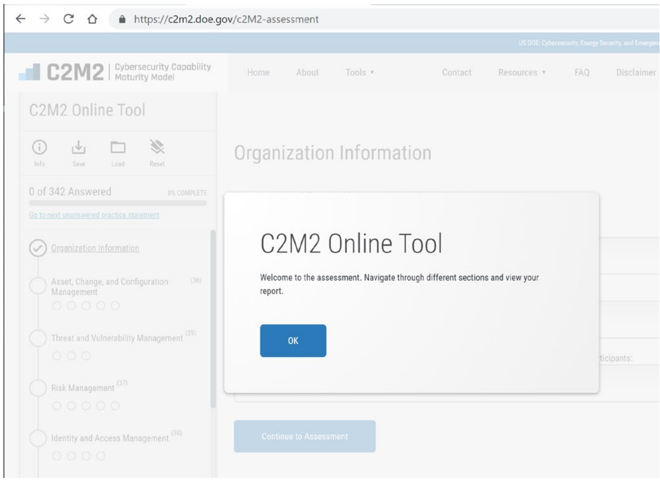


Figure 2.3. Tool Drop-Down Menu

After clicking the "C2M2 Online Tool" option, Figure 2.4 is displayed. Click OK to enter the tool.


https://c2m2.doe.gov/c2M2-assessment
US DOE: Cybersecurity, Energy Security, and Emergen
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools ▼
Contact
Resources ▼
FAQ
Disclaimer
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Organization Information
ticipants:
OK
Continue to Assessment

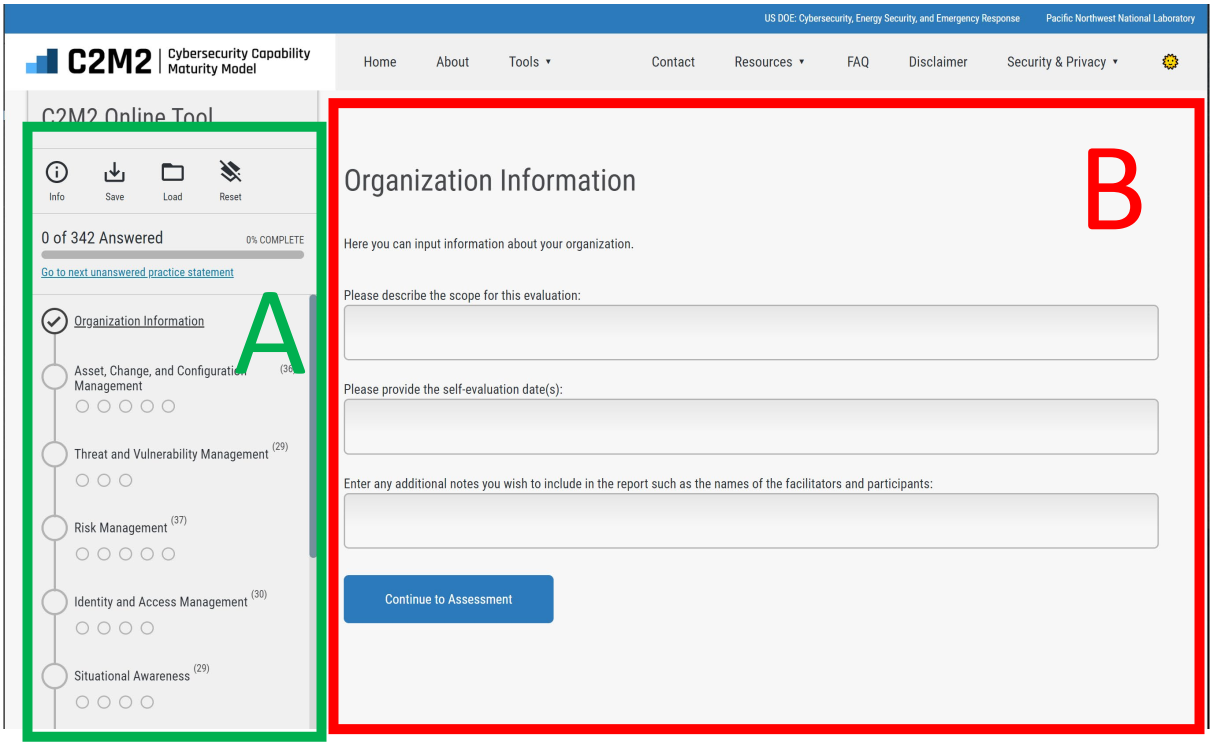
C2M2 Online Tool

Welcome to the assessment. Navigate through different sections and view your report.

Figure 2.4. Initial Display of the C2M2 Online Tool

Accessing the Online C2M2 Tool

After clicking OK, the user is now ready to start using the tool. In addition to the previously described website navigation information at the top of the webpage, Figure 2.5 shows the two main areas on the screen: the tool navigation/status/management area on the left ("A") and the data entry area ("B").


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Situational Awareness (29)
A
B
Continue to Assessment

Organization Information

Here you can input information about your organization.

Please describe the scope for this evaluation:

Please provide the self-evaluation date(s):

Enter any additional notes you wish to include in the report such as the names of the facilitators and participants:

Figure 2.5. The Work Areas within the Tool

The left area ("A" In Figure 2.5, also called the "navigation pane") contains buttons to save, load, or reset the assessment data. Beneath these buttons is a progress bar that displays the number of answered practice statements for the assessment and the total number of practices. The navigation menu displayed beneath the progress bar can be used to navigate to any domain or objective that the user wants to access. As the user completes sections of the assessment, the icons for domains and objectives in the navigation menu are displayed as "checked" to acknowledge their completion. This navigation menu can be used to allow the user to choose their preferred order for addressing the domains and objectives in their self-evaluation.

The right area ("B" In Figure 2.5) is for data entry. This portion of the screen information is used to enter "organization information" (i.e., information on the scope of the assessment and the people performing the assessment), display descriptions of each domain, enter practice implementation scores, enter practice notes, and display messages to the user.

The Navigation Pane

Figure 2.6 provides a close-up display of the navigation pane.

The "Save" button is labeled as "A". It allows the user to download their current assessment data to their computer. Data are saved to a file using a JavaScript Object Notation (JSON) format. JSON is a standard data interchange format that is primarily used for transmitting data between a web application and a server.

The “Load” button is labeled as “B”. It allows the user to load a saved assessment by dragging a saved JSON format data file and dropping it in the load window.

The “Reset” button is labeled as “C”. Clicking it gives the user the option to clear the answered practice statements and start with a clean (i.e., blank) assessment.

The Save, Load, and Reset functions are described in more detail in Section 3.

Clicking the “Go to next unanswered practice statement” button (labeled as “D”) will navigate the assessment to the next unanswered practice. This is quite useful when working with a partially completed assessment and there is a need to quickly jump to unanswered practices.

Clicking the circle to the left of a domain name (examples are labeled as “E” and “G”), takes the user to the corresponding domain. Domains for which all the practices are assessed are denoted with a checkmark (as shown by E”). A bolded circle indicates the current domain (as shown by “G”). If a circle is unchecked (as shown by “G”), practices in the domain are not yet fully assessed.

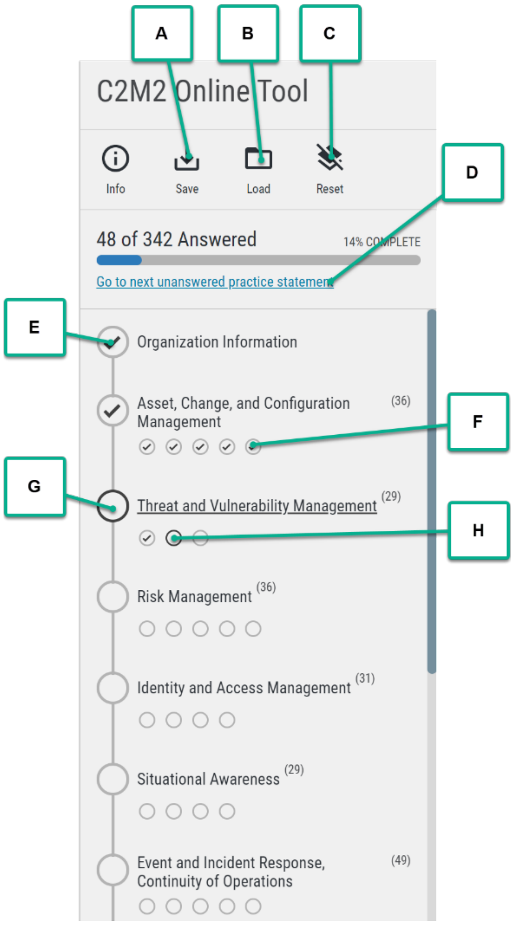

A
B
C
D
E
F
G
H
C2M2 Online Tool
Info
Save
Load
Reset
48 of 342 Answered
14% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (36)
Identity and Access Management (31)
Situational Awareness (29)
Event and Incident Response, Continuity of Operations (49)

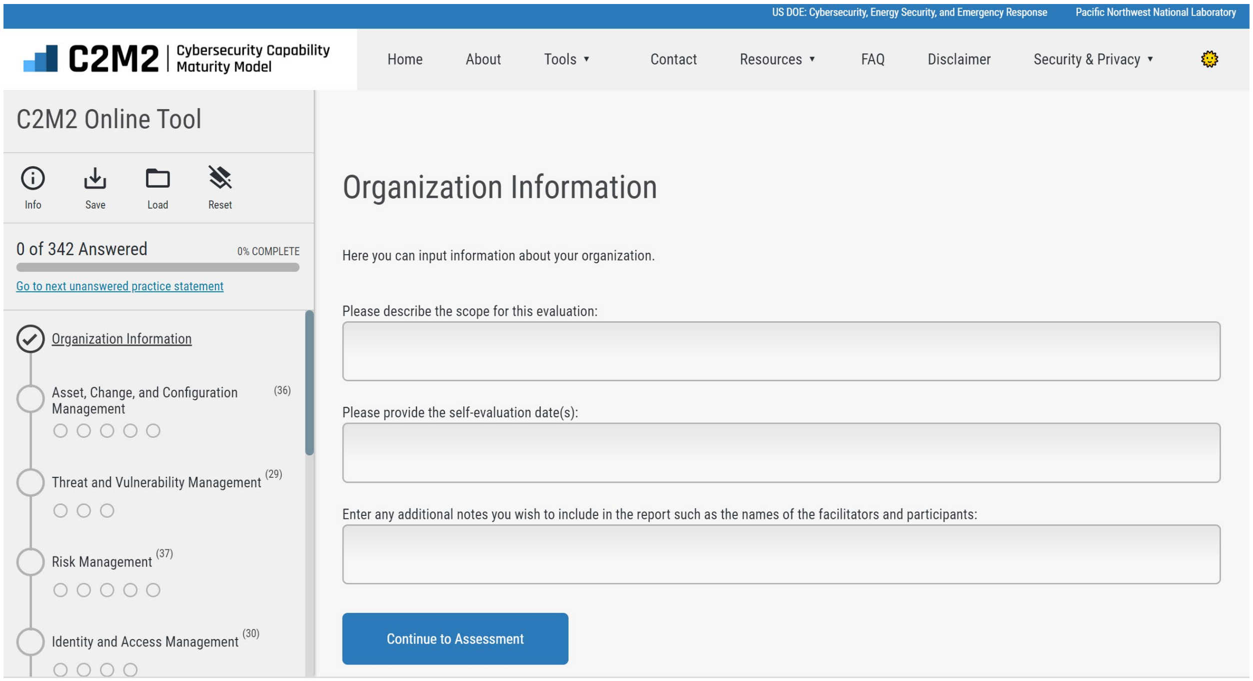
Figure 2.6. Navigation Pane

Below the domain names are smaller circle icons. These represent each of the objectives in the domain. Clicking a circle icon takes the user to that objective. A checkmark in an objective circle icon indicates all the practices in the objective are scored (as shown by “F”). A slightly bolded circle indicates the current objective being assessed (as shown by “H”).

A slider bar on the right side of the left navigation pane allows the user to move the display up and down within the pane. Below the last of the domains is a circle for “Results”. Clicking “Results” takes the user to a screen from which they can automatically generate an assessment report. In this version of the tool, results cannot be displayed until all the C2M2 practices are scored.

Entering Data

Figure 2.7 presents the introductory screen for the assessment. The user should use this screen to enter details on the scope of the organization’s C2M2 self-evaluation. The scope may be quite broad or narrowly focused. For example, it may focus on the overall organization, a department or function (e.g., the information technology group, power transmission, hydroelectric power generation, substation operation), a specific facility or group of facilities (e.g., the Alpha Power Generation Station, the Beta Energy Control Center), or a region of concern (e.g., Gamma Power Company‘s Northern State region).


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Continue to Assessment

Organization Information

Here you can input information about your organization.

Please describe the scope for this evaluation:

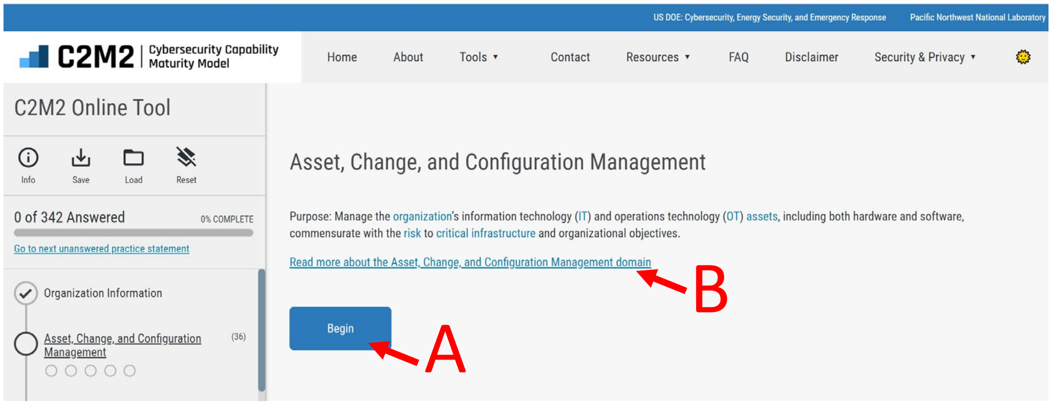
Please provide the self-evaluation date(s):

Enter any additional notes you wish to include in the report such as the names of the facilitators and participants:

Figure 2.7. The “Organization Information” Screen

A field is provided to specify the date or date range of the self-evaluation. This information is particularly useful if the self-evaluation is periodically repeated to monitor progress toward cybersecurity maturity goals. Finally, a field is provided to enter additional descriptive information about the evaluation. We recommend including the name and contact information for the self-evaluations facilitator and the names of the subject matter experts who provide input for the model domain.

After completing this “Organization Information” form, clicking “Continue to Assessment” will navigate to the first domain. The resulting screen (Figure 2.8) displays the title of the first domain and its purpose. Click the “Begin” button (as shown by “A”) to start the assessment of this domain. Before doing that, an option is provided to “read more about…” this domain (as shown by “B”).


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Begin
A
B

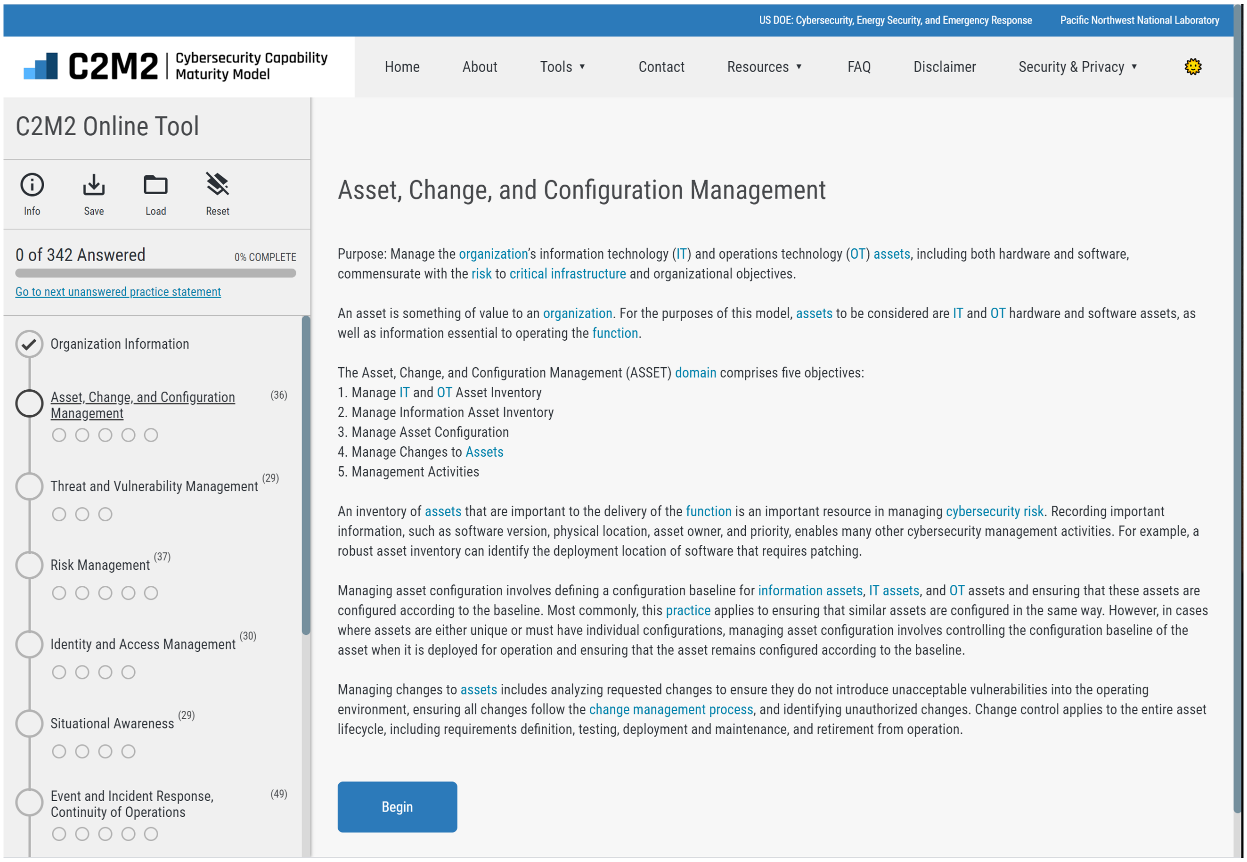
Asset, Change, and Configuration Management

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

Read more about the Asset, Change, and Configuration Management domain

Figure 2.8. The Initial Display of the First Domain

If this option is clicked, Figure 2.9 is displayed. It provides more descriptive information about the domain and lists each of the domain's objectives.



US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
✓ Organization Information
Asset, Change, and Configuration Management (36)
○ ○ ○ ○ ○
Threat and Vulnerability Management (29)
○ ○ ○
Risk Management (37)
○ ○ ○ ○ ○
Identity and Access Management (30)
○ ○ ○ ○
Situational Awareness (29)
○ ○ ○ ○
Event and Incident Response, Continuity of Operations (49)
○ ○ ○ ○ ○

Asset, Change, and Configuration Management

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

An asset is something of value to an organization. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.

The Asset, Change, and Configuration Management (ASSET) domain comprises five objectives:
1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage Asset Configuration
4. Manage Changes to Assets
5. Management Activities

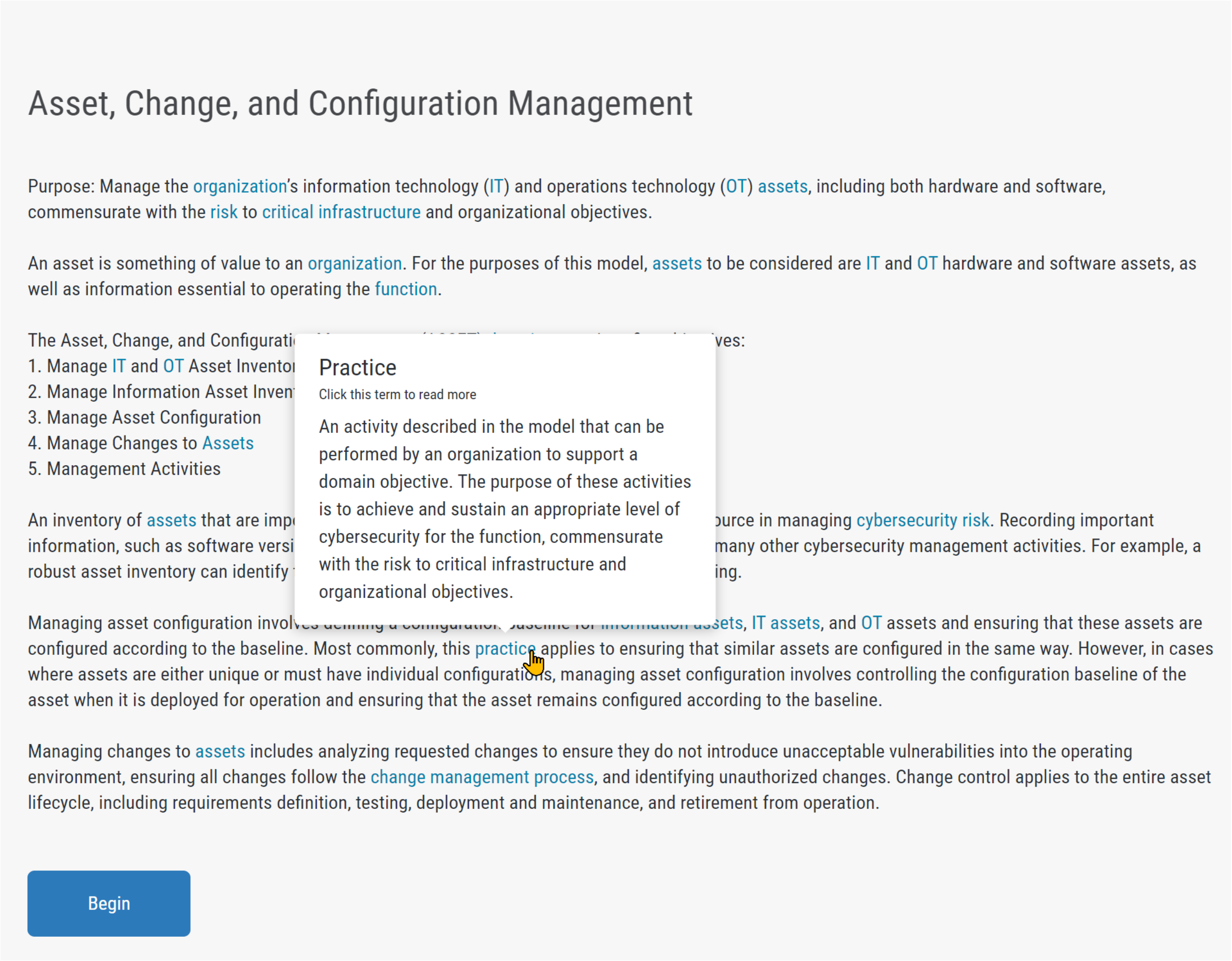
An inventory of assets that are important to the delivery of the function is an important resource in managing cybersecurity risk. Recording important information, such as software version, physical location, asset owner, and priority, enables many other cybersecurity management activities. For example, a robust asset inventory can identify the deployment location of software that requires patching.

Managing asset configuration involves defining a configuration baseline for information assets, IT assets, and OT assets and ensuring that these assets are configured according to the baseline. Most commonly, this practice applies to ensuring that similar assets are configured in the same way. However, in cases where assets are either unique or must have individual configurations, managing asset configuration involves controlling the configuration baseline of the asset when it is deployed for operation and ensuring that the asset remains configured according to the baseline.

Managing changes to assets includes analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes. Change control applies to the entire asset lifecycle, including requirements definition, testing, deployment and maintenance, and retirement from operation.

Figure 2.9. Detailed Presentation of Domain Descriptive Information

Note the text shown on this page (Figure 2.9), and throughout the tool, displays some words or phrases in a light blue font. Mousing over these words provides a pop-up definition (Figure 2.10).



Asset, Change, and Configuration Management

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

An asset is something of value to an organization. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.

The Asset, Change, and Configurati ves:
1. Manage IT and OT Asset Inventor
2. Manage Information Asset Inven
3. Manage Asset Configuration
4. Manage Changes to Assets
5. Management Activities

Practice
Click this term to read more
An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organizational objectives.

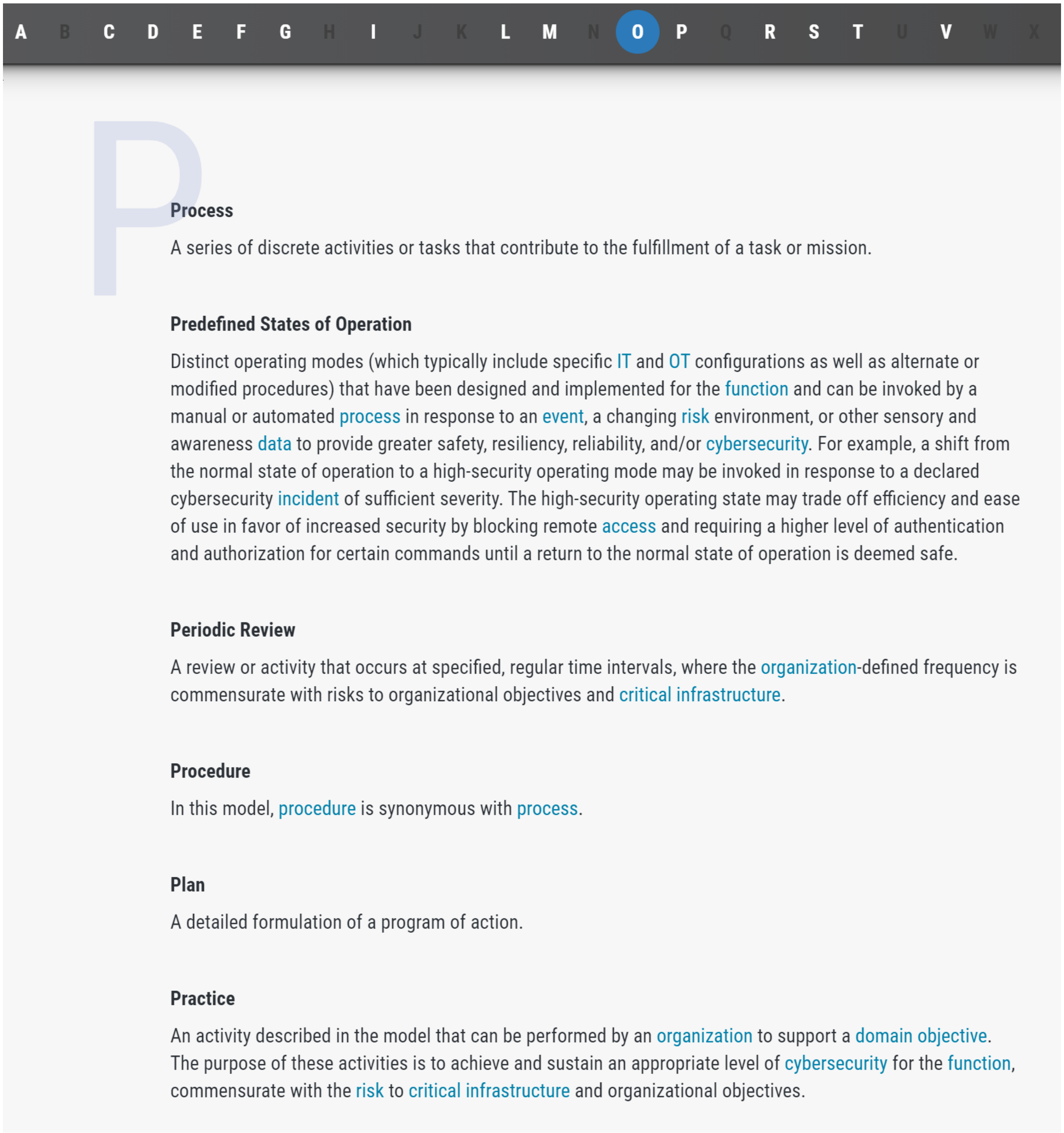
An inventory of assets that are imp ource in managing cybersecurity risk. Recording important information, such as software versi many other cybersecurity management activities. For example, a robust asset inventory can identify ing.

Managing asset configuration involves defining a configuration baseline for information assets, IT assets, and OT assets and ensuring that these assets are configured according to the baseline. Most commonly, this practice applies to ensuring that similar assets are configured in the same way. However, in cases where assets are either unique or must have individual configurations, managing asset configuration involves controlling the configuration baseline of the asset when it is deployed for operation and ensuring that the asset remains configured according to the baseline.

Managing changes to assets includes analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes. Change control applies to the entire asset lifecycle, including requirements definition, testing, deployment and maintenance, and retirement from operation.

Figure 2.10. Pop-up Definition of Glossary Terms from within the Tool

Clicking on a word in blue font opens a new tab in the browser that displays the C2M2 glossary. The glossary will be opened to the page where the clicked term is defined (as done for the word "practice" in Figure 2.11).



Process

A series of discrete activities or tasks that contribute to the fulfillment of a task or mission.

Predefined States of Operation

Distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resiliency, reliability, and/or cybersecurity. For example, a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity. The high-security operating state may trade off efficiency and ease of use in favor of increased security by blocking remote access and requiring a higher level of authentication and authorization for certain commands until a return to the normal state of operation is deemed safe.

Periodic Review

A review or activity that occurs at specified, regular time intervals, where the organization-defined frequency is commensurate with risks to organizational objectives and critical infrastructure.

Procedure

In this model, procedure is synonymous with process.

Plan

A detailed formulation of a program of action.

Practice

An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organizational objectives.

Figure 2.11. The C2M2 Glossary

After clicking "Begin" from Figure 2.9 or Figure 2.10, Figure 2.12 is displayed. It opens the first objective (i.e., "*Manage IT and OT Asset Inventory*") in the current domain ("*Asset, Change, and Configuration Management*" or "ASSET" for short). Nine practices are in this domain and as indicated by the blank white circles, none has an assigned implementation score. Clicking "Begin Section" or clicking any of the blank circles in Figure 2.12 starts the assessment and opens Figure 2.13. If "Begin Section" is clicked the first practice in the indicated objective will be displayed.

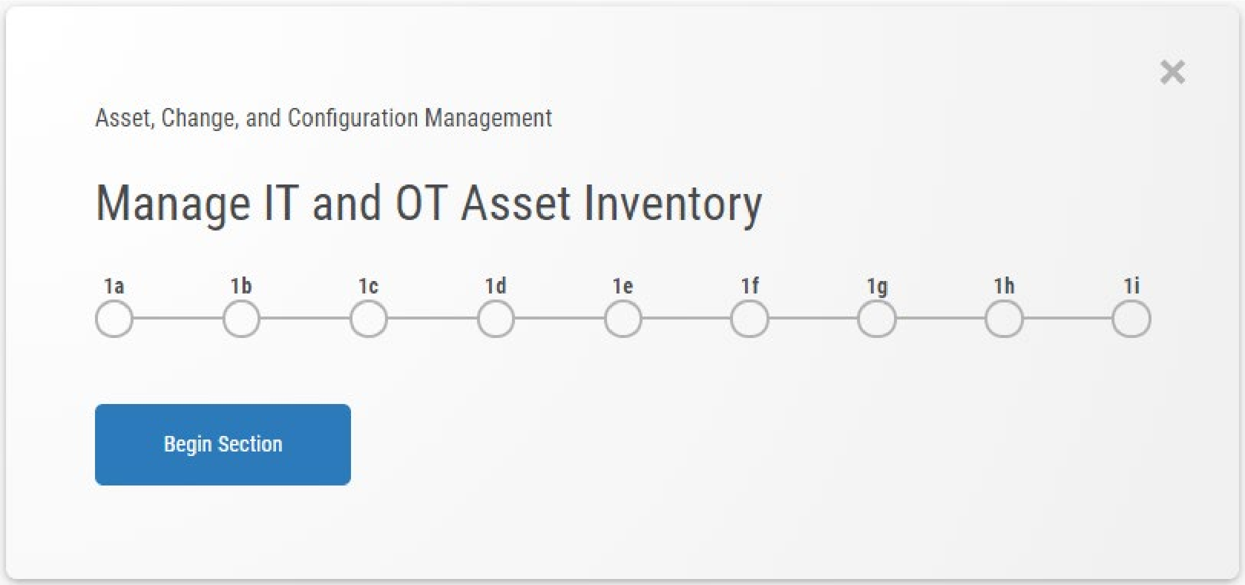
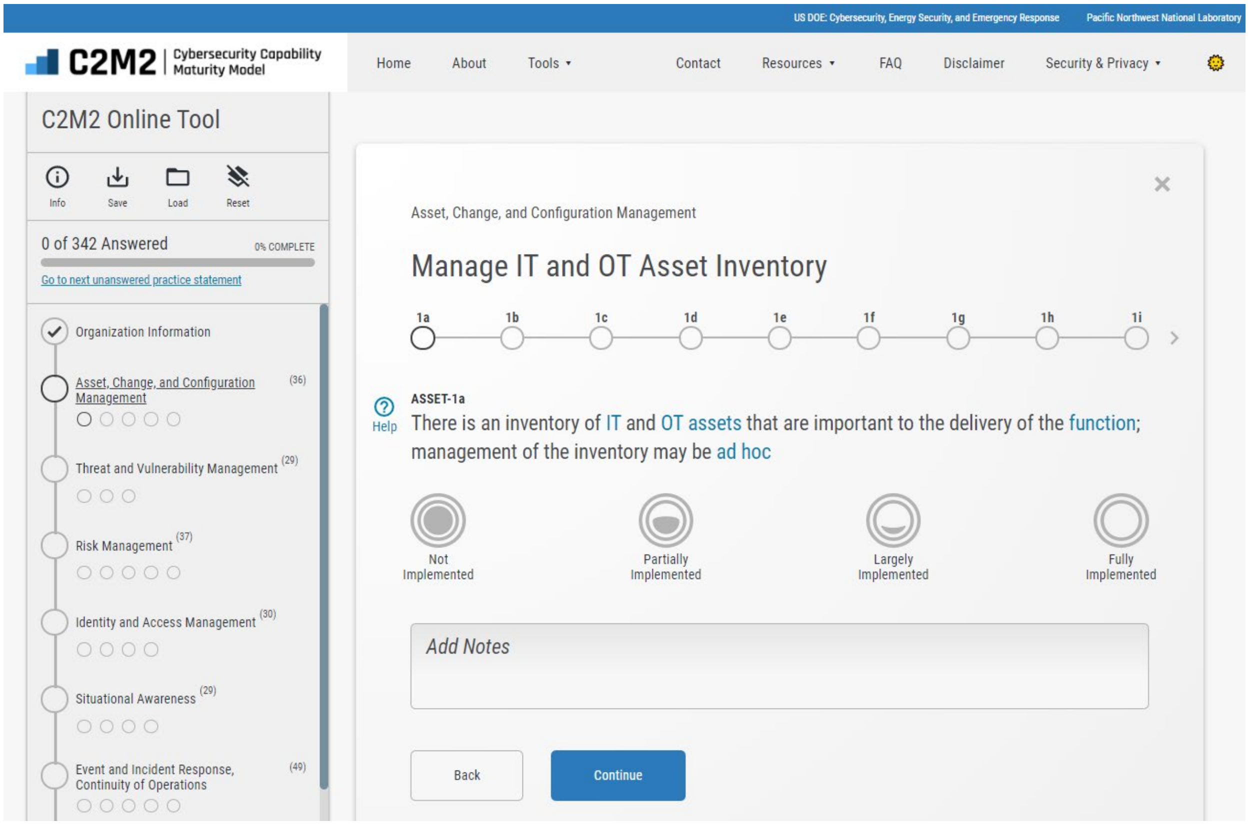

×
Asset, Change, and Configuration Management
Manage IT and OT Asset Inventory
1a
1b
1c
1d
1e
1f
1g
1h
1i
Begin Section

Figure 2.12. Preparing to Begin the Assessment of the Displayed Objective


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
0 of 342 Answered
0% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Situational Awareness (29)
Event and Incident Response, Continuity of Operations (49)
×
Asset, Change, and Configuration Management
Manage IT and OT Asset Inventory
1a
1b
1c
1d
1e
1f
1g
1h
1i
Help

ASSET-1a

There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc

Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
Add Notes
Back
Continue

Figure 2.13. The First Practice in the First Objective of the First Domain

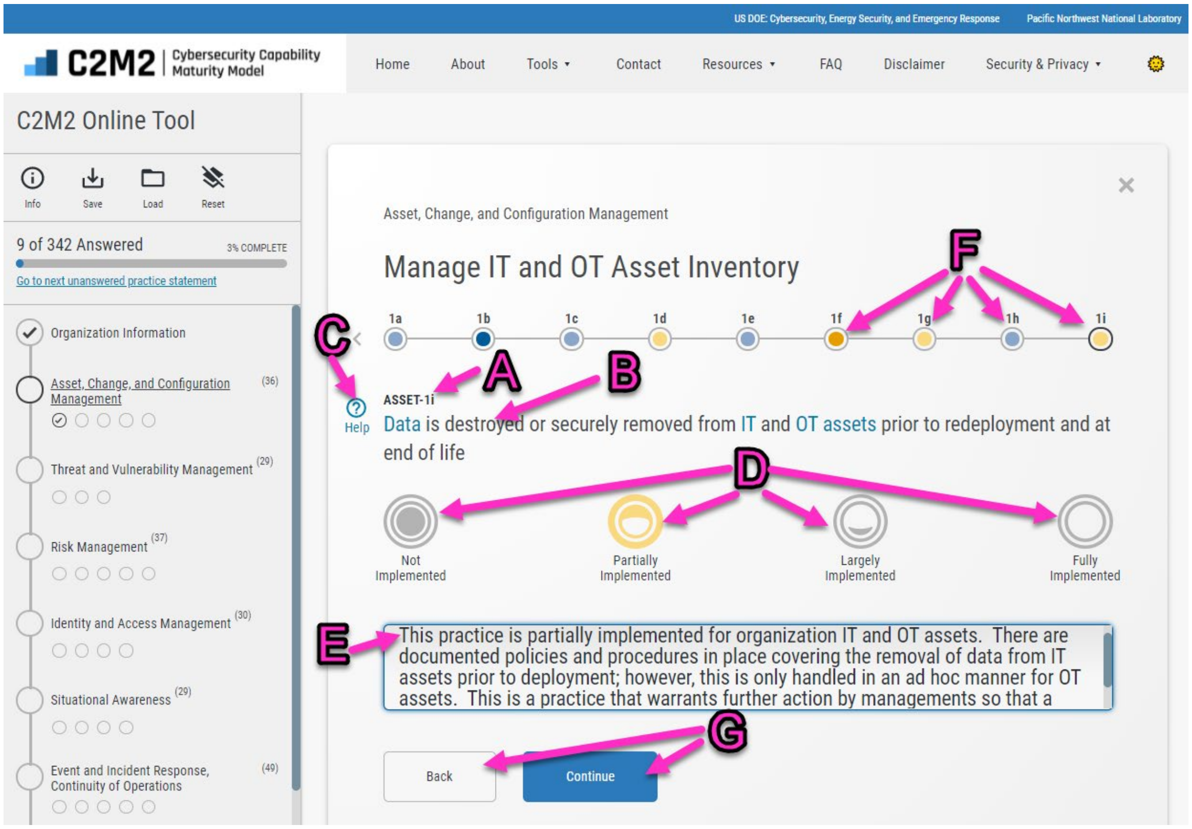
There is a lot going on in Figure 2.13. Figure 2.14 presents an example of a completed version of this practice evaluation page. In Figure 2.14, we see the results for the last practice in this objective, "ASSET-

1i" (labeled "A"). Beneath the practice identifier is the text of the practice (labeled "B"). If additional information is needed to understand the practice, click the Help icon (labeled "C"), and Help Text will be displayed on the screen (see Figure 2.15).

After reading and gaining an understanding of the practice, click one of the four implementation level choices available (labeled "D") -- Not, Partially, Largely, and Fully implemented are the four options. The options are color-coded and have different shapes. Notes can be entered in the note field (labeled "E") to document the rationale for the implementation score, identify activities that could be implemented in the future to increase the implementation score, record differences in opinion among the subject matter experts evaluating this practice, or add other information that may be helpful in the future. Notes can be typed directly into the tool in the note field or text can be copied and pasted into the note field from other files (e.g., a Word file).

A quick summary of the scores assigned to other practices in this Objective is provided using the horizontal string of color-coded circles (labeled "F") located below the Objective name.

To move to the next practice in the objective, click the "Continue" button (labeled "G"). At any time, other practices in the objective can be visited (or re-visited) by using the "Back" and "Continue" buttons or by directly clicking one of the color-coded circles (labeled "F") below the Objective name.

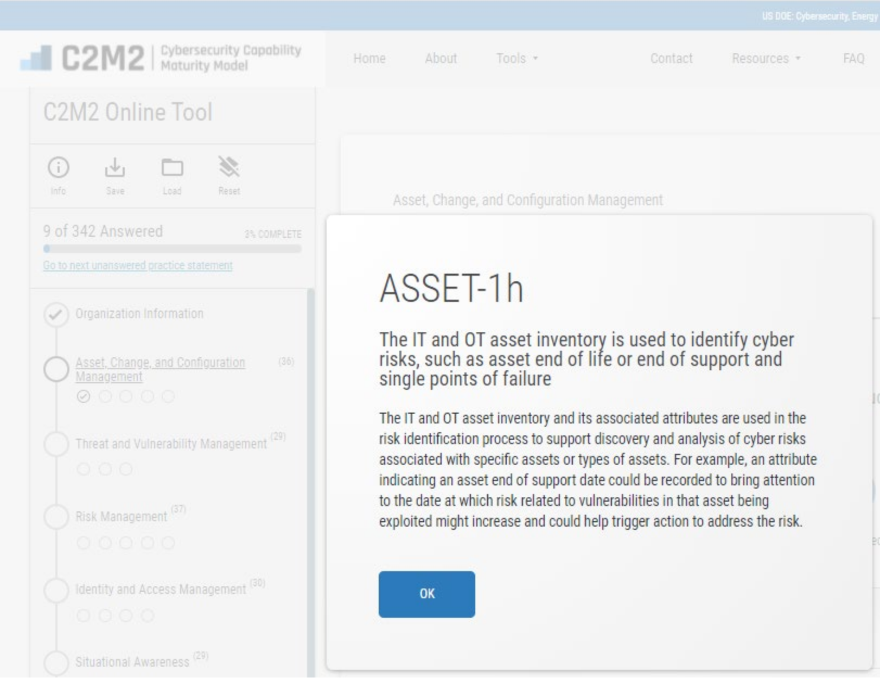

US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
9 of 342 Answered
3% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Situational Awareness (29)
Event and Incident Response, Continuity of Operations (49)
Asset, Change, and Configuration Management
Manage IT and OT Asset Inventory
F
1a
1b
1c
1d
1e
1f
1g
1h
1i
C
A
B
Help
ASSET-1i
D
Not Implemented
Partially Implemented
Largely Implemented
Fully Implemented
E
G
Back
Continue

Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life

This practice is partially implemented for organization IT and OT assets. There are documented policies and procedures in place covering the removal of data from IT assets prior to deployment; however, this is only handled in an ad hoc manner for OT assets. This is a practice that warrants further action by managements so that a

Figure 2.14. Scoring and Documenting a Practice Statement

After completing an evaluation of each of the practices for the current Objective, a summary of the completed practices and their scores is displayed in Figure 2.16. Scroll to the bottom of the page and click "Continue to the Next Section" to continue.

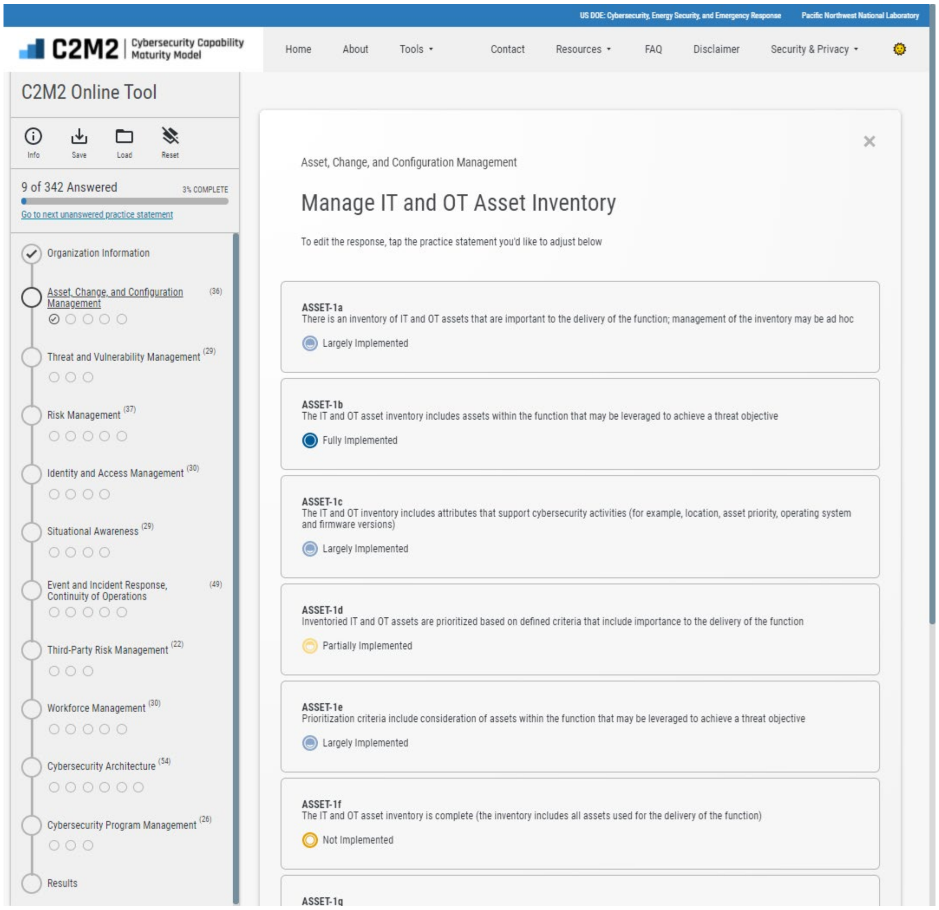

US DOE: Cybersecurity, Energy
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools
Contact
Resources
FAQ
C2M2 Online Tool
Info
Save
Load
Reset
9 of 342 Answered
3% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Situational Awareness (29)
Asset, Change, and Configuration Management
OK

ASSET-1h

The IT and OT asset inventory is used to identify cyber risks, such as asset end of life or end of support and single points of failure

The IT and OT asset inventory and its associated attributes are used in the risk identification process to support discovery and analysis of cyber risks associated with specific assets or types of assets. For example, an attribute indicating an asset end of support date could be recorded to bring attention to the date at which risk related to vulnerabilities in that asset being exploited might increase and could help trigger action to address the risk.

Figure 2.15. An Example Help Text Display


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools
Contact
Resources
FAQ
Disclaimer
Security & Privacy
C2M2 Online Tool
Info
Save
Load
Reset
9 of 342 Answered
3% COMPLETE
Go to next unanswered practice statement
Organization Information
Asset, Change, and Configuration Management (36)
Threat and Vulnerability Management (29)
Risk Management (37)
Identity and Access Management (30)
Situational Awareness (29)
Event and Incident Response, Continuity of Operations (49)
Third-Party Risk Management (22)
Workforce Management (30)
Cybersecurity Architecture (54)
Cybersecurity Program Management (26)
Results

Asset, Change, and Configuration Management

Manage IT and OT Asset Inventory

To edit the response, tap the practice statement you'd like to adjust below

ASSET-1a
There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc

Largely Implemented

ASSET-1b
The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective

Fully Implemented

ASSET-1c
The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, operating system and firmware versions)

Largely Implemented

ASSET-1d
Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function

Partially Implemented

ASSET-1e
Prioritization criteria include consideration of assets within the function that may be leveraged to achieve a threat objective

Largely Implemented

ASSET-1f
The IT and OT asset inventory is complete (the inventory includes all assets used for the delivery of the function)

Not Implemented

ASSET-1g

Figure 2.16. Summary Scores for the Current Objective

When each objective is completed (i.e., all the practices in the objective have been assigned implementation scores), a checkmark appears in the corresponding objective circle icon in the left navigation pane (as shown by label "A" in Figure 2.17). When all the objectives in a domain are completed (and all have checkmarks), a checkmark appears in the domain circle in the left navigation pane (as shown by label "B").

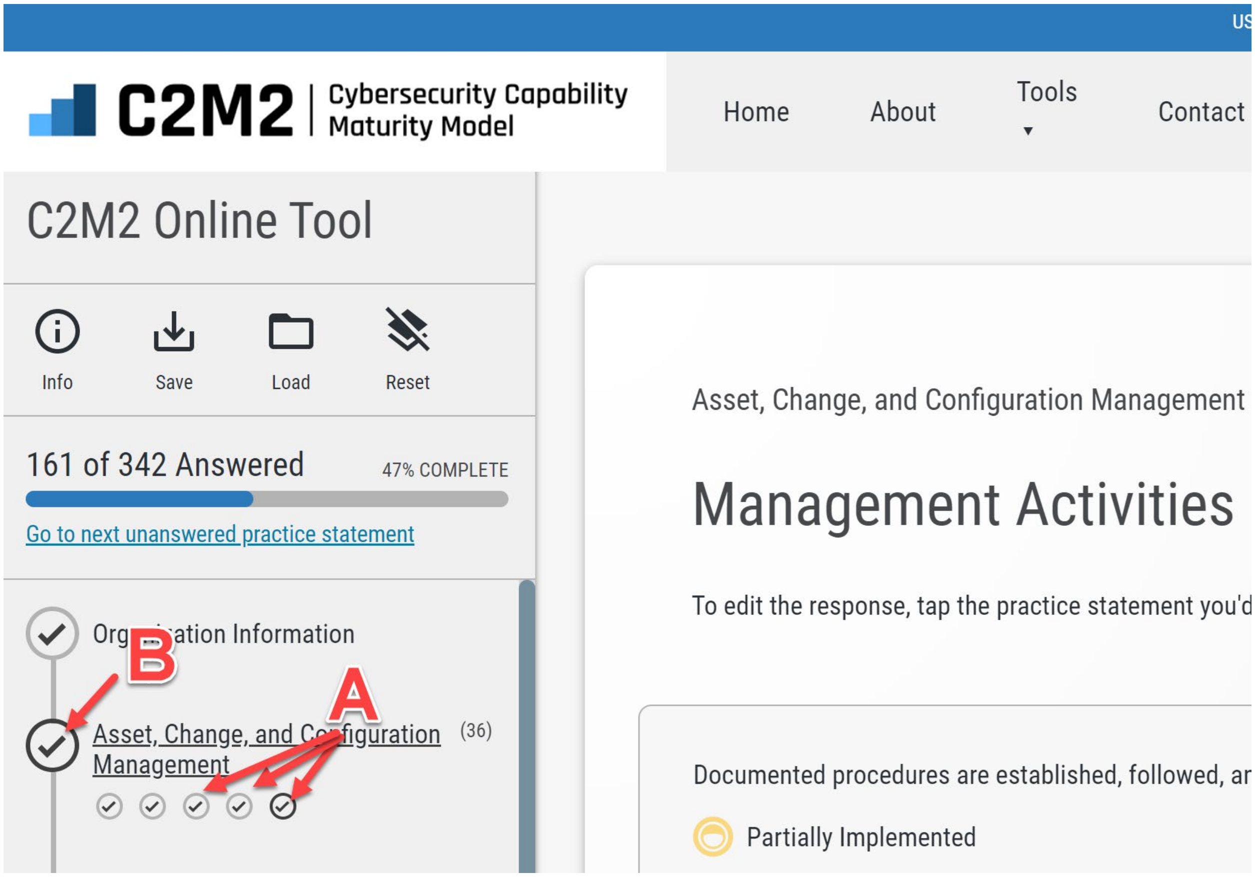
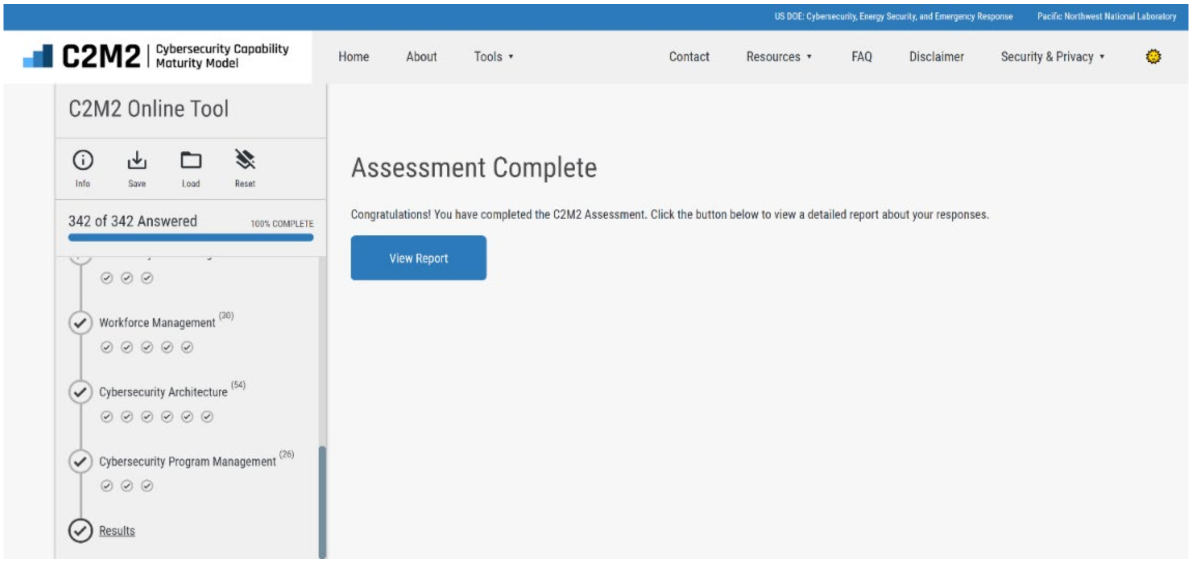

US
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
C2M2 Online Tool
Info
Save
Load
Reset
161 of 342 Answered
47% COMPLETE
Go to next unanswered practice statement
Organization Information
B
A
Asset, Change, and Configuration Management
(36)
Asset, Change, and Configuration Management
Management Activities
To edit the response, tap the practice statement you'd
Documented procedures are established, followed, ar
Partially Implemented

Figure 2.17. All Practices for Each Objective in the ASSET domain are Scored

When all the practices in all the domains have been scored, the evaluation is complete. The "Assessment Complete" screen will be displayed (Figure 2.18). The User can also click "Results" at the bottom of the left navigation window to display the "Assessment Complete" screen.

From the Assessment Complete screen, click "View Report" to generate an automated evaluation report. There may be a short delay (e.g., 30 seconds or less) while the report is being generated by the user's computer. A green spinning wheel (Figure 2.19) provides an indicator that the report is being generated. When completed, the report will be displayed on the right-side window of the tool.


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
C2M2 Online Tool
Info
Save
Load
Reset
342 of 342 Answered
100% COMPLETE
Workforce Management (30)
Cybersecurity Architecture (54)
Cybersecurity Program Management (26)
Results
View Report

Assessment Complete

Congratulations! You have completed the C2M2 Assessment. Click the button below to view a detailed report about your responses.

Figure 2.18. Completed Assessment

Figure 2.19. The Green Spinner Displayed While the Report is Being Generated

3. Saving, Loading, and Resetting Data

Before turning our attention to the output report, we will review the process for saving, loading, and resetting assessment data. As shown in Figure 3.1, near the top of the left navigation pane are icons for “Save” (labeled “A”), “Load” (labeled “B”), and “Reset” (labeled “C”). The save function saves user input locally on their computer in a JSON file (no user data are ever shared with or stored on the server). The load function reads and loads data from a previously saved model JSON file (either created by the online- or PDF-based C2M2 tools). The Reset function erases the current assessment data and allows the user to start over from scratch with a new evaluation (previously saved files are not affected by the Reset function).

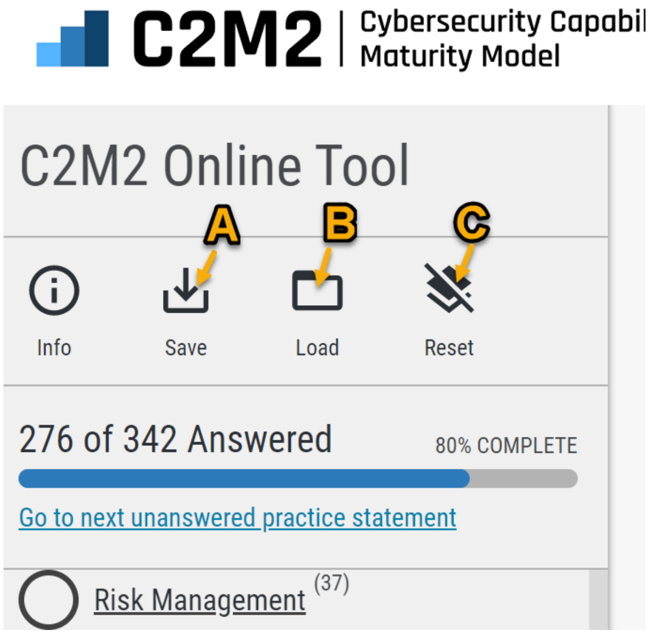
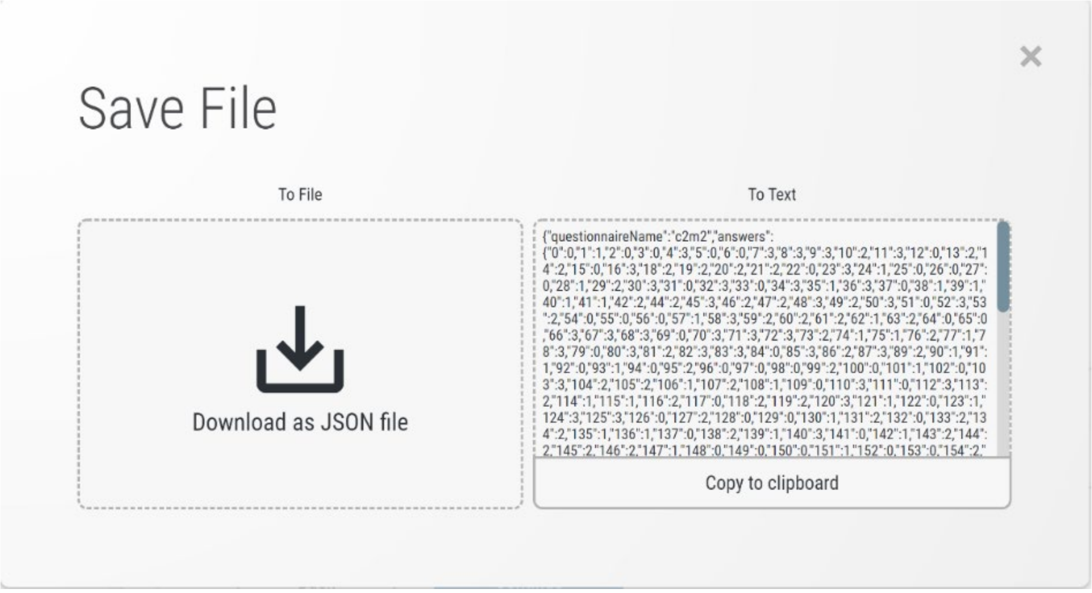


Figure 3.1. The Save, Load, and Reset Icons

Saving Data

When the “Save” icon is clicked, a pop-up window (Figure 3.2) directs the user to save their C2M2 input file to their computer. Options are provided to save the file either by downloading it as JSON file format or copying the data to a text file. Saving to a JSON is the preferred and standard approach for saving data files. Once downloaded, the date and time labeled JSON file can be renamed to aid in future identification.



{"questionnaireName":"c2m2","answers":
{"0":0,"1":1,"2":0,"3":0,"4":3,"5":0,"6":0,"7":3,"8":3,"9":3,"10":2,"11":3,"12":0,"13":2,"1
4":2,"15":0,"16":3,"18":2,"19":2,"20":2,"21":2,"22":0,"23":3,"24":1,"25":0,"26":0,"27":
0,"28":1,"29":2,"30":3,"31":0,"32":3,"33":0,"34":3,"35":1,"36":3,"37":0,"38":1,"39":1,"
40":1,"41":1,"42":2,"44":2,"45":3,"46":2,"47":2,"48":3,"49":2,"50":3,"51":0,"52":3,"53
":2,"54":0,"55":0,"56":0,"57":1,"58":3,"59":2,"60":2,"61":2,"62":1,"63":2,"64":0,"65":0
,"66":3,"67":3,"68":3,"69":0,"70":3,"71":3,"72":3,"73":2,"74":1,"75":1,"76":2,"77":1,"7
8":3,"79":0,"80":3,"81":2,"82":3,"83":3,"84":0,"85":3,"86":2,"87":3,"89":2,"90":1,"91":
1,"92":0,"93":1,"94":0,"95":2,"96":0,"97":0,"98":0,"99":2,"100":0,"101":1,"102":0,"10
3":3,"104":2,"105":2,"106":1,"107":2,"108":1,"109":0,"110":3,"111":0,"112":3,"113":
2,"114":1,"115":1,"116":2,"117":0,"118":2,"119":2,"120":3,"121":1,"122":0,"123":1,"
124":3,"125":3,"126":0,"127":2,"128":0,"129":0,"130":1,"131":2,"132":0,"133":2,"13
4":2,"135":1,"136":1,"137":0,"138":2,"139":1,"140":3,"141":0,"142":1,"143":2,"144":
2,"145":2,"146":2,"147":1,"148":0,"149":0,"150":0,"151":1,"152":0,"153":0,"154":2,"

Figure 3.2. The “Save File” Pop-up Window

Loading Data

Figure 3.3 illustrates the pop-up window for the C2M2 “load” function. After clicking “Load”, a pop-up window will appear with two options for loading data into the tool. A C2M2 JSON file containing previously saved data can be loaded into the tool. Alternatively, data saved to text using the Save feature can be pasted into the From Text field. Loading data using these options allows the modification or addition of information for a previously started evaluation. Loading a JSON is the preferred and standard approach for loading data into the tool.

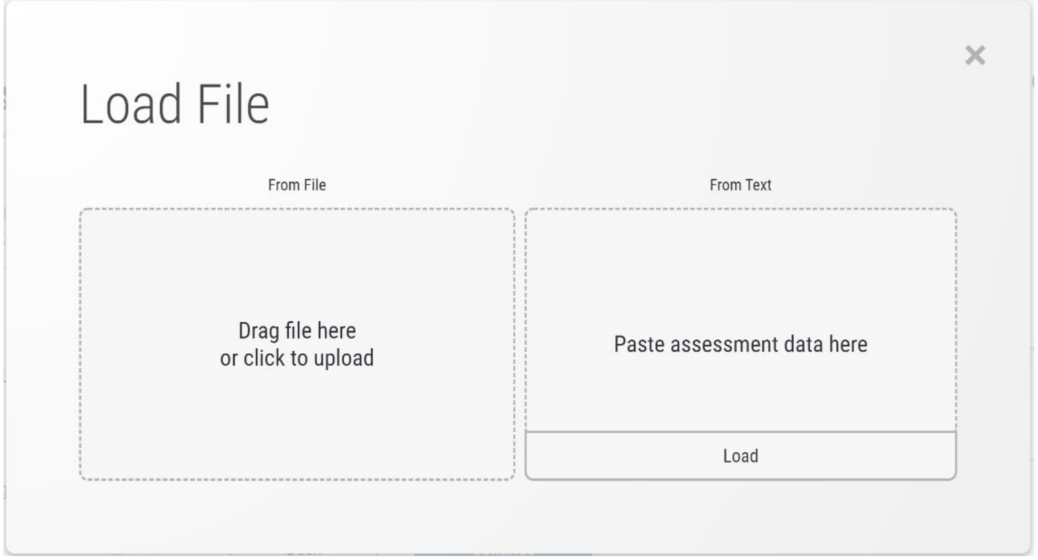
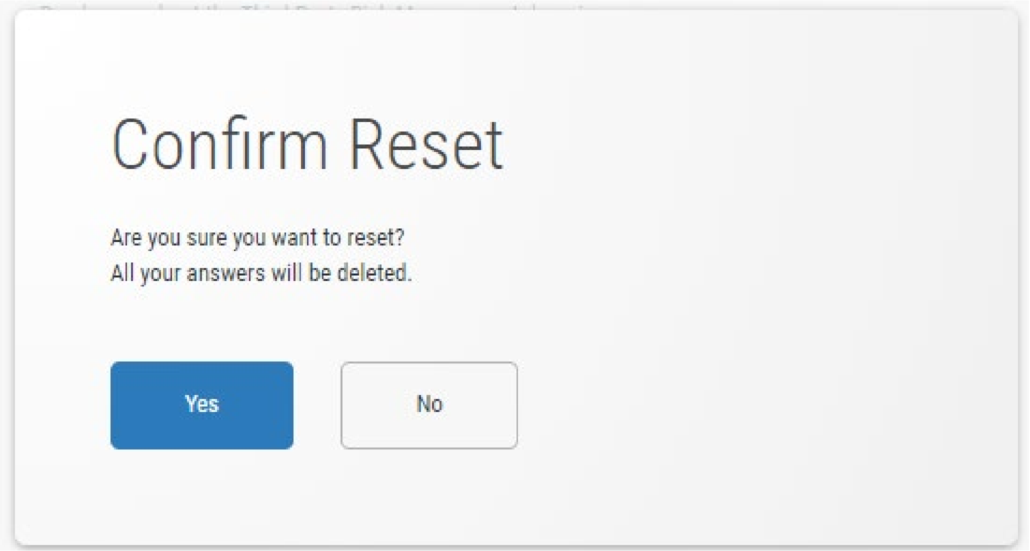


Figure 3.3. The “Load File” Pop-up Window

Resetting Data

Figure 3.4 illustrates the pop-up window for the C2M2 “reset” function. After clicking “Reset”, a pop-up window will appear that asks the user to confirm they want to reset their data and warns that the reset will delete all existing data currently active (i.e., displayed) in the tool. Click “yes” to confirm the decision to reset the data. Click “No” to return to the model with the current data retained.



Confirm Reset

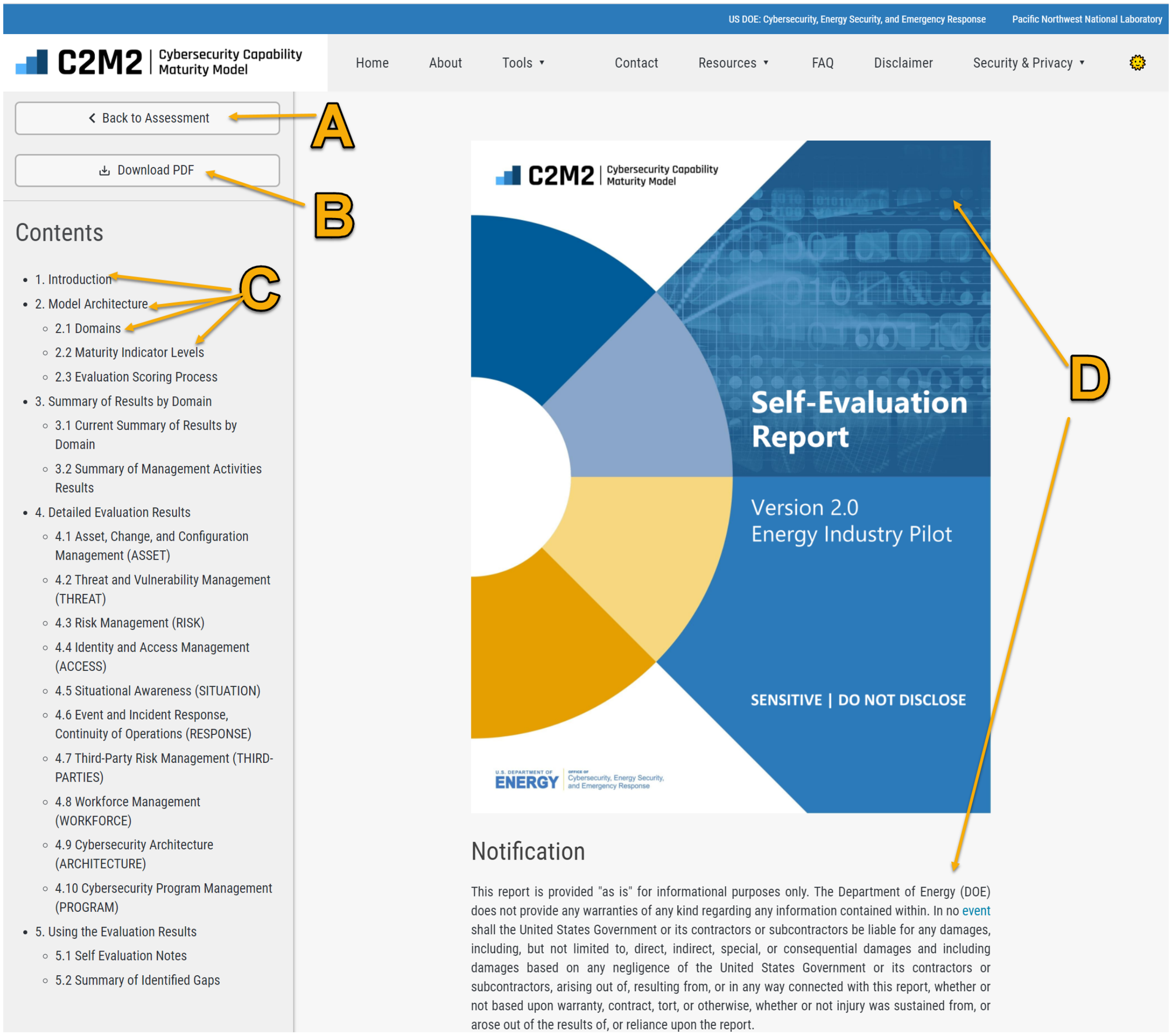
Are you sure you want to reset?
All your answers will be deleted.

Figure 3.4. The “Confirm Reset” Pop-Up Window

4. Interpreting the Report

The C2M2 Self-Evaluation Report – Introduction and Model Architecture

After the Self-Evaluation Report is generated, it is displayed on the screen. The initial display is similar to what is shown in Figure 4.1. In the left navigation pane, the option is provided to return to the assessment (labeled “A”) to view or modify the evaluation – including changing scoring or adding additional notes. The report, which is displayed on the screen can also be downloaded as a PDF file by clicking “Download PDF” (labeled “B”). In the Contents section of the navigation pane, the sections and subsections of the report are listed (labeled “C”) and each of these headings is clickable to facilitate the rapid navigation of the report. In the main section to the right of the navigation pane, the report is displayed. The initial display (labeled “D”) shows the report cover and the Notification section (which provides a standard disclaimer).


US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 | Cybersecurity Capability Maturity Model
Home
About
Tools ▾
Contact
Resources ▾
FAQ
Disclaimer
Security & Privacy ▾
‹ Back to Assessment
Download PDF
A
B
C
D
C2M2 | Cybersecurity Capability Maturity Model
U.S. DEPARTMENT OF ENERGY
OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Contents

Self-Evaluation Report

Version 2.0
Energy Industry Pilot

SENSITIVE | DO NOT DISCLOSE

Notification

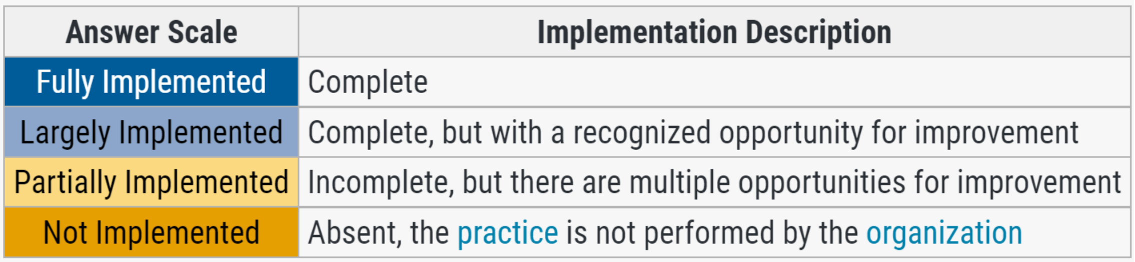
This report is provided "as is" for informational purposes only. The Department of Energy (DOE) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including, but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

Figure 4.1. The Top of C2M2 Self-Evaluation Report

The key sections of the C2M2 Self-Evaluation Report that follow the cover and notification are:

1. Introduction
2. Model Architecture
   2.1 Domains
   2.2 Maturity Indicator Levels
   2.3 Evaluation Scoring Process
3. Summary of Results by Domain
   3.1 Current Summary of Results by Domain
   3.2 Summary of Management Activities Results
4. Detailed Evaluation Results
   4.1 Asset, Change, and Configuration Management (ASSET)
   4.2 Threat and Vulnerability Management (THREAT)
   4.3 Risk Management (RISK)
   4.4 Identity and Access Management (ACCESS)
   4.5 Situational Awareness (SITUATION)
   4.6 Event and Incident Response, Continuity of Operations (RESPONSE)
   4.7 Third-Party Risk Management (THIRD-PARTIES)
   4.8 Workforce Management (WORKFORCE)
   4.9 Cybersecurity Architecture (ARCHITECTURE)
   4.10 Cybersecurity Program Management (PROGRAM)
5. Using the Evaluation Results
   5.1 Self Evaluation Notes
   5.2 Summary of Identified Gaps

Figure 4.2 displays the four levels of practice implementation scores used throughout the online tool and in all reporting products. “Fully implemented” is represented as a dark-blue color, “largely implemented” is light blue, “partially implemented” is yellow and “not implemented” is orange.



Answer Scale	Implementation Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete, but there are multiple opportunities for improvement
Not Implemented	Absent, the practice is not performed by the organization

Figure 4.2. Practice Implementation Scale (from Section 2.3 of the output report)

Introduction and Model Architecture– Report Sections 1 and 2

In the report, Section 1: “Introduction” presents the scope of the assessment, the self-evaluation dates, and additional notes – all information entered by the C2M2 facilitator in the “Organization Information” section of the tool. Section 2: “Model Architecture” describes the Domain – Objective – Practice structure of the model. It provides the purpose and description of each domain and lists the objectives within each domain. It also presents the rules for applying the maturity indicator levels (MILs). Finally, guidance is provided on how to interpret practice implementation scoring and how to achieve various maturity levels. These sections are particularly useful for decision-makers and subject matter experts who are reviewing the C2M2 Self-Evaluation Report and lack familiarity with the model and its structure.

Summary of Results by Domain – Report Section 3

Section 3 of the report displays the summary of MIL scores for each of the C2M2 domains. Figure 4.3 summarizes the MIL scores by domain using the traditional C2M2 "donut diagrams." Each of the 10 domains is represented by a column presenting three donut diagrams that represent the scores for the practices. Below the donut diagrams is the overall MIL score achieved for that domain. In the example presented in Figure 4.3, the ASSET, THREAT, and THIRD-PARTY domains achieve MIL3 because all the practices at MIL1, 2, and 3 are largely or fully implemented. On the other end of the spectrum, the ACCESS domain does not even achieve MIL1 because it has some partially and not implemented MIL1 practices.

Figure 4.4 provides a close-up view of the three donut diagrams and the MIL score of a sample domain. To interpret these results, start with the donut diagram for MIL1 (the bottom-most donut diagram). It shows that for this domain there are five practices that evaluate MIL1 performance, as indicated by the number "5" in the middle of the donut (i.e., within the donut hole). One of these practices is scored at the "fully implemented" level (the dark-blue segment of the donut) and four practices are "largely implemented" (the light-blue segment of the donut). There are no "partially implemented" nor "not implemented" MIL1 practices for this domain.

At the next level up, for MIL2, the number "17" in the middle of the donut indicates there are 17 practices at MIL1 and MIL2 that must be scored as fully or largely implemented for MIL 2 to be achieved. This consists of the five practices from MIL1 and 12 additional practices for MIL2. Considered together, there are four practices that are fully implemented and 13 that are largely implemented. There are no "partially implemented" nor "not implemented" MIL1 or MIL2 practices for this domain.

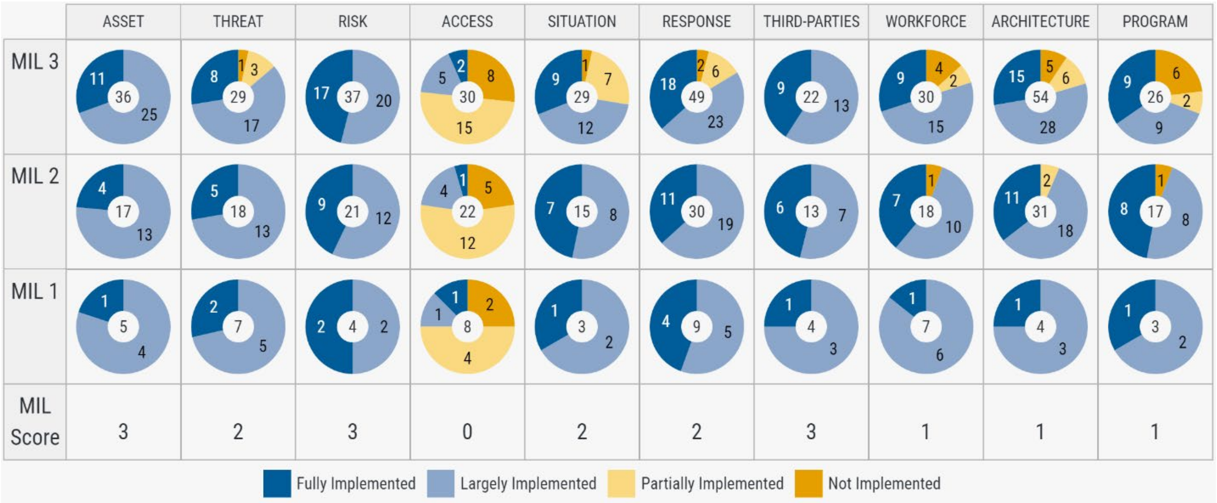


Figure 4.3. Sample Summary Donut Diagram Presenting MIL Score by Domain

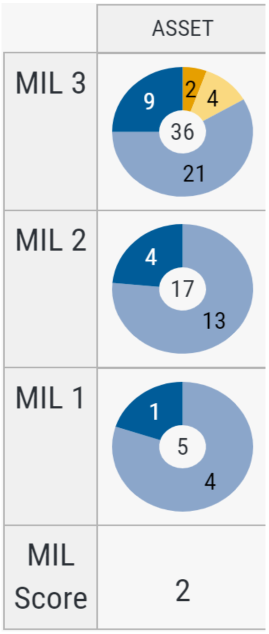


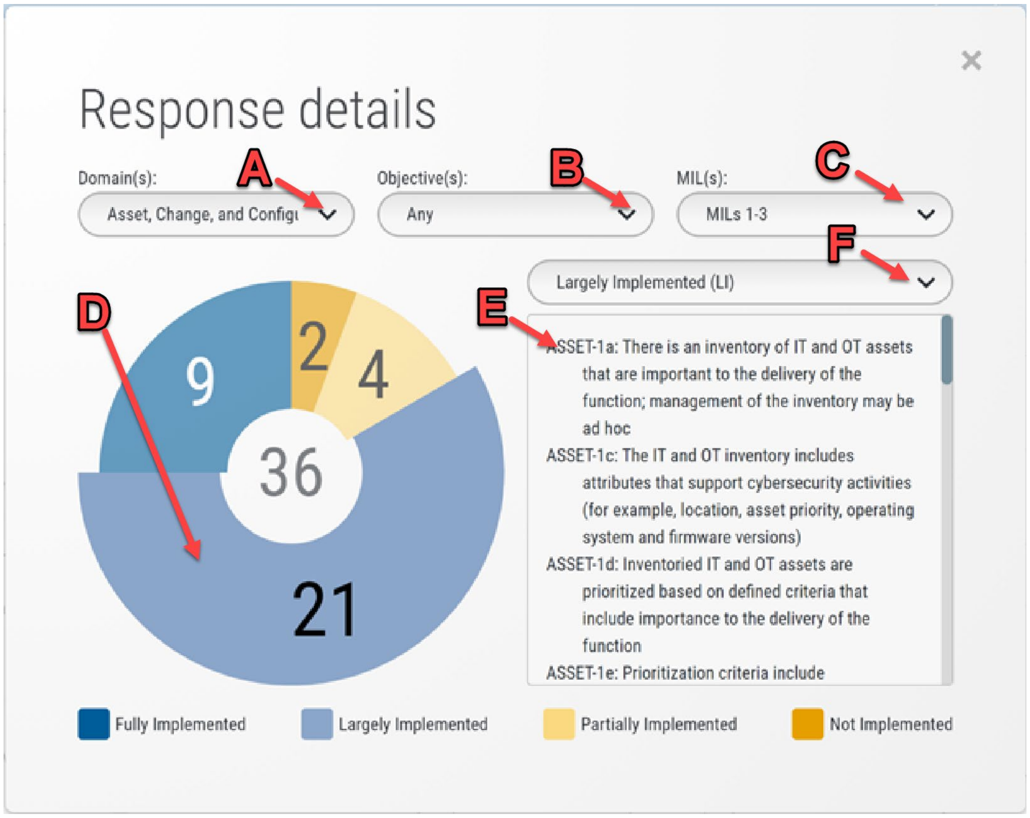
Figure 4.4. Close-up for a Domain

To achieve MIL 3, there are 36 practices at MIL1, 2, and 3 that must be scored as fully or largely implemented. In total, there are nine practices that are fully implemented, 21 practices are largely implemented, four practices that are partially implemented (indicated by the yellow segment in the donut diagram), and two practices that are not implemented (indicated by the orange segment in the donut diagram).

A net MIL score of "2" is achieved for the ASSET domain because it represents the highest MIL level achieved (because all the associated MIL1 and MIL2 practices are fully or largely implemented achieved).

The individual donut diagrams in Figure 4.3 can be interrogated to provide more detailed data analytics. Simply click any slice of any donut diagram and a data analytics product will appear in a pop-up window shown in Figure 4.5.

In Figure 4.5, the visualization details are presented for the entire *Asset, Change, and Configuration Management* (ASSET) domain. Label "A" points to the drop-down menu used to select this domain. Label "B" points to the drop-down menu used to select which of the Domain's Objectives are included in this data visualization (in this case, "any" refers to including all the objectives in this domain). Label "C" points to the drop-down menu used to select the inclusion of practices capturing all three MILs (i.e., MIL 1–3). The tool allows this product to display the results for practices at each MIL, for all MILs combined, or for both MIL1 and 2 practices combined.



Response details

Domain(s): Asset, Change, and Configu

Objective(s): Any

MIL(s): MILs 1-3

Largely Implemented (LI)

ASSET-1a: There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc

ASSET-1c: The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, operating system and firmware versions)

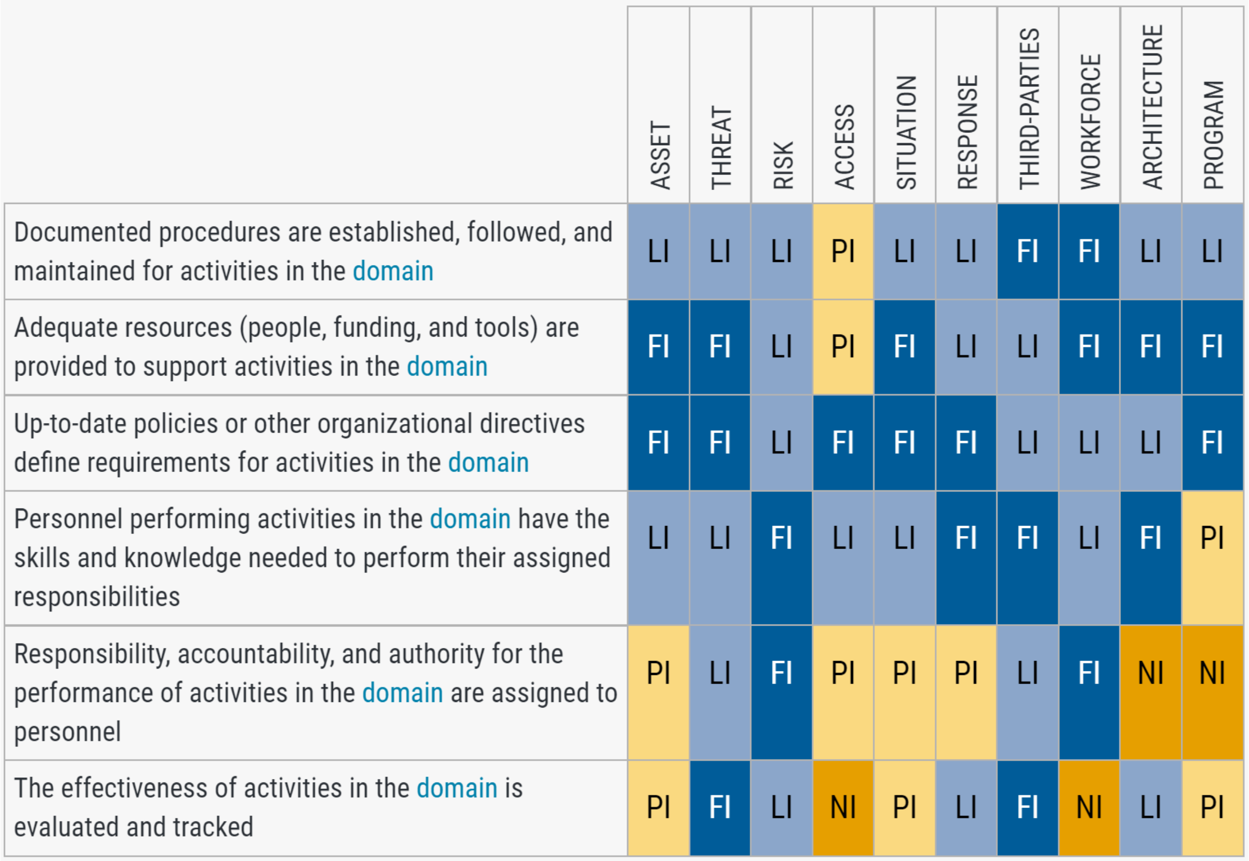
ASSET-1d: Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function

ASSET-1e: Prioritization criteria include

Figure 4.5. Response Details for MILs 1-3 of Asset, Change, and Configuration Domain

In Figure 4.5, the user has clicked on the largely implemented sector in the donut diagram. As a result, all the largely implemented practices for this domain are displayed in the text window (labeled "E"). The drop-down menu above this text window (labeled "F") can also be used to display the text of the practices for all implementation scores or any specific implementation score.

Figure 4.6 displays a summary of the implementation scores for the Management Activities Objective which is found in each domain (it is the only Objective that is common across all ten domains). It is provided because it may be instructive to see how the level of implementation of the six practices in this Objective varies across all the domains. The left column in Figure 4.6 presents the text for each of the six management practices, and the right side of the figure shows the implementation level for the practices in each of the 10 domains. In this example, all the management practices are fully or largely implemented in three domains: THREAT, RISK, and THIRD-PARTIES. In contrast, lower implementation scores are experienced in the ACCESS domain, where four of the six practices are either not or partially implemented.



	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	WORKFORCE	ARCHITECTURE	PROGRAM
Documented procedures are established, followed, and maintained for activities in the domain	LI	LI	LI	PI	LI	LI	FI	FI	LI	LI
Adequate resources (people, funding, and tools) are provided to support activities in the domain	FI	FI	LI	PI	FI	LI	LI	FI	FI	FI
Up-to-date policies or other organizational directives define requirements for activities in the domain	FI	FI	LI	FI	FI	FI	LI	LI	LI	FI
Personnel performing activities in the domain have the skills and knowledge needed to perform their assigned responsibilities	LI	LI	FI	LI	LI	FI	FI	LI	FI	PI
Responsibility, accountability, and authority for the performance of activities in the domain are assigned to personnel	PI	LI	FI	PI	PI	PI	LI	FI	NI	NI
The effectiveness of activities in the domain is evaluated and tracked	PI	FI	LI	NI	PI	LI	FI	NI	LI	PI

Figure 4.6. Summary of Management Activities Results Table

Detailed Evaluation Results – Report Section 4

The C2M2 Self-Evaluation Report continues by presenting "detailed evaluation results" for each of the 10 domains. The donut diagrams described in the previous section are presented again, but this time focusing on the individual Domains in the C2M2, with results presented for each Objective within the domain (Figure 4.7).

Also presented in this section of the report is a figure (a sample is provided in Figure 4.8) that displays the implementation scores for each of the practices in the domain.

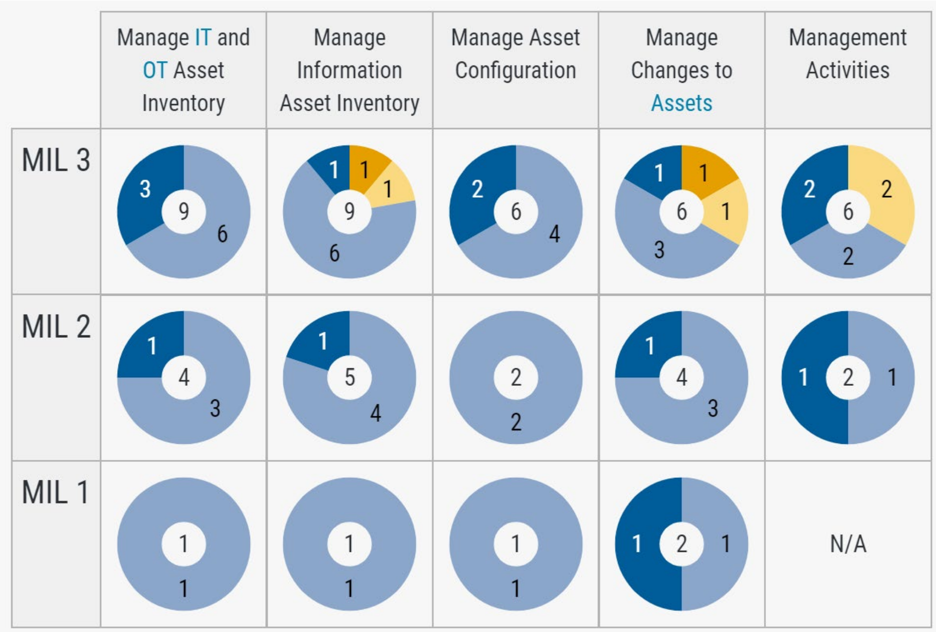
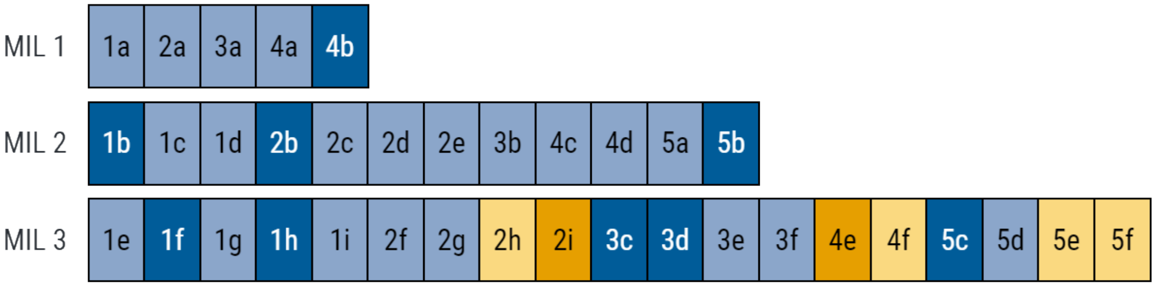


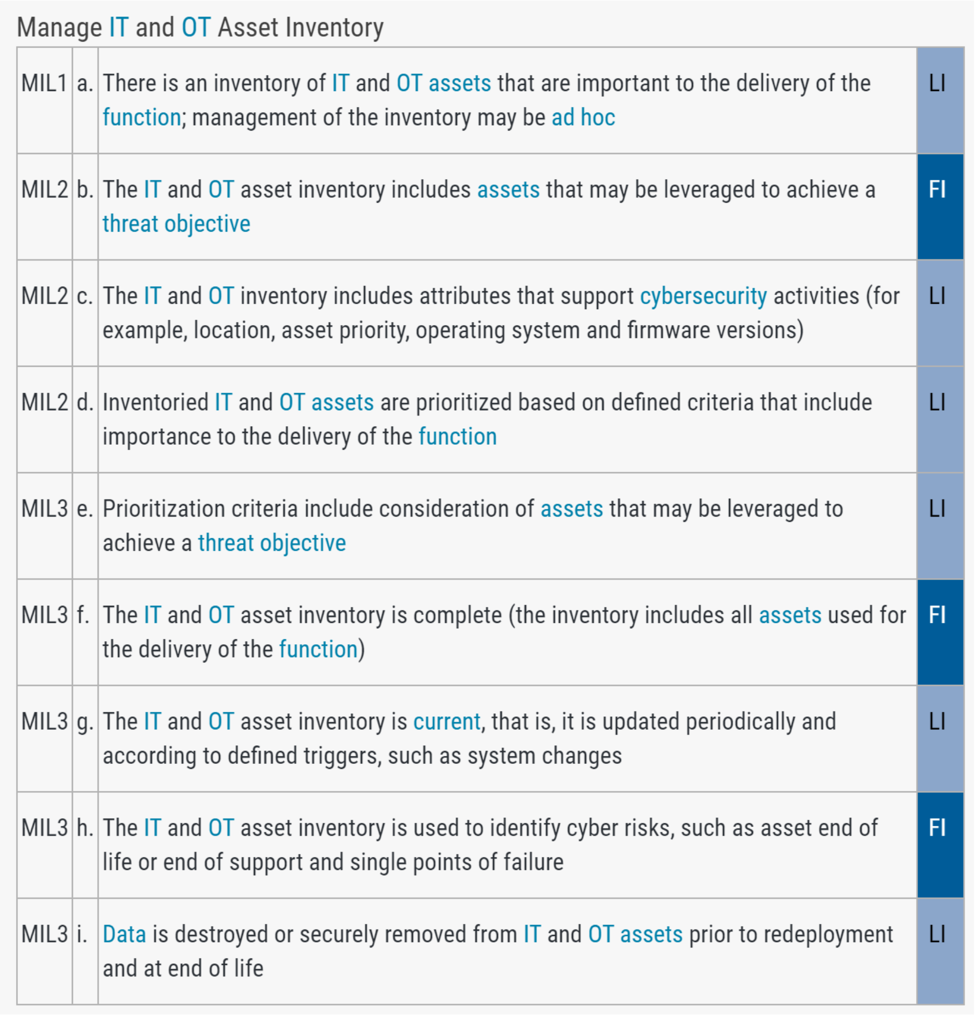
Figure 4.7. Detailed Evaluation Donut Diagrams for the ASSET Domain



MIL 1	1a	2a	3a	4a	4b													
MIL 2	1b	1c	1d	2b	2c	2d	2e	3b	4c	4d	5a	5b						
MIL 3	1e	1f	1g	1h	1i	2f	2g	2h	2i	3c	3d	3e	3f	4e	4f	5c	5d	5e	5f

Figure 4.8. Detailed Evaluation Practice Statement Summary for ASSET Domain

After presenting this information, a lengthy table is provided (Figure 4.9 is a partial sample) that presents more detailed information about the practices. Each practice is listed in order for each Objective in the Domain. Along with the text of the practice, this table indicates the maturity level that the practice is designed to evaluate. In the right-most column in the table, the assigned implementation score for each practice is indicated. This table presents a concise presentation of key data entered into the C2M2 assessment tool.



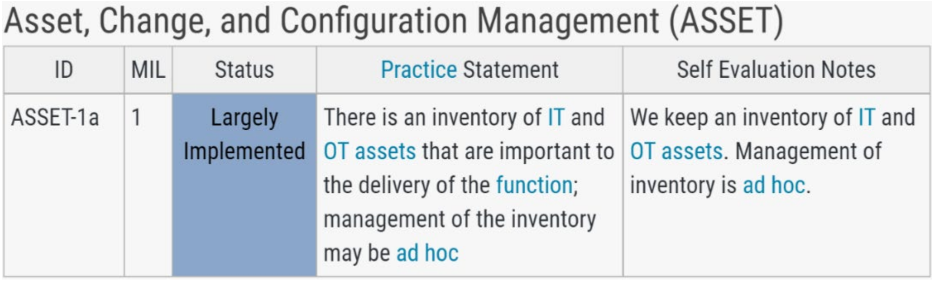
Manage IT and OT Asset Inventory

MIL1	a.	There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc	LI
MIL2	b.	The IT and OT asset inventory includes assets that may be leveraged to achieve a threat objective	FI
MIL2	c.	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, operating system and firmware versions)	LI
MIL2	d.	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	LI
MIL3	e.	Prioritization criteria include consideration of assets that may be leveraged to achieve a threat objective	LI
MIL3	f.	The IT and OT asset inventory is complete (the inventory includes all assets used for the delivery of the function)	FI
MIL3	g.	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	LI
MIL3	h.	The IT and OT asset inventory is used to identify cyber risks, such as asset end of life or end of support and single points of failure	FI
MIL3	i.	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	LI

Figure 4.9. Presentation of the MIL, Text, and Implementation Score Level, and MIL for Each Practice

Using the Evaluation Results – Report Section 5

Section 5.1 in the report begins by providing information on how to use the self-evaluation results (a four-step process is recommended). Section 5.2 presents a table with detailed information for each practice. Each row in the table presents the practice ID, the corresponding maturity level the practice evaluates, the implementation score, the practice statement, and the self-evaluation note for the practice. Figure 4.10 displays a sample row from this table.

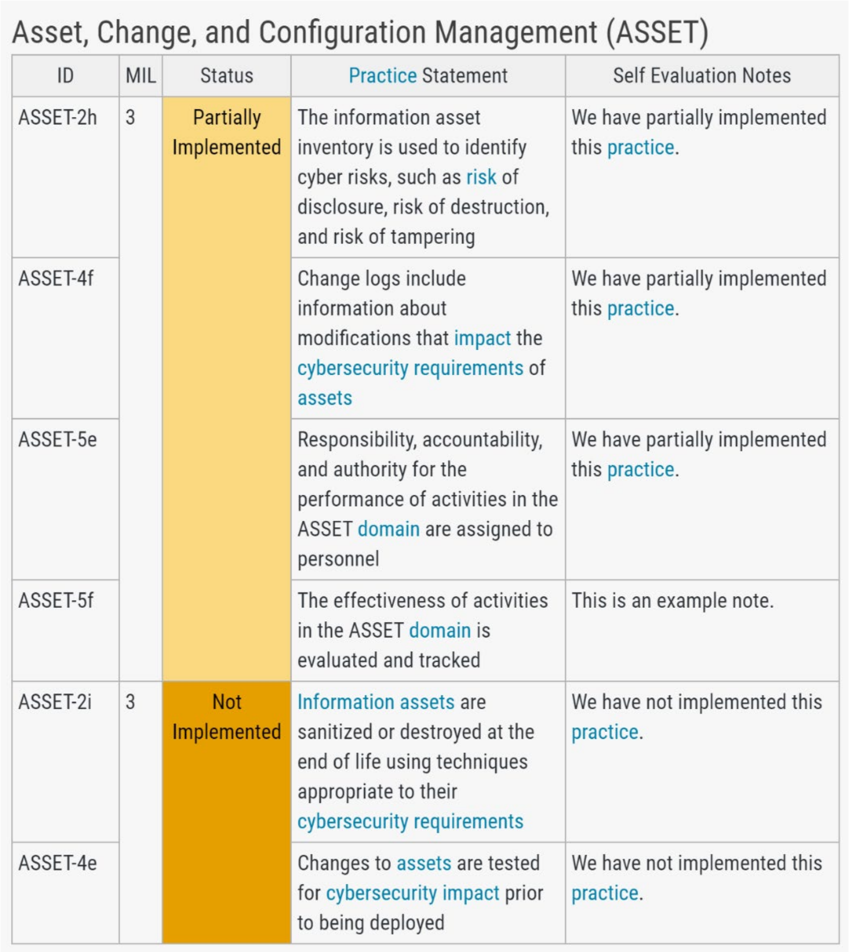


Asset, Change, and Configuration Management (ASSET)

ID	MIL	Status	Practice Statement	Self Evaluation Notes
ASSET-1a	1	Largely Implemented	There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc	We keep an inventory of IT and OT assets. Management of inventory is ad hoc.

Figure 4.10. Sample Row from the Table Presenting the Self-Evaluation Notes

Section 5.2 also presents a table with a focused summary of all the partially implemented and not implemented practices identified in the self-evaluation. This table provides a quick overview of the practices in each domain that need improvement to reach the next maturity level. The user notes regarding the practice statement are also displayed in the last column of the table. Figure 4.11 presents a sample excerpt from this table.



Asset, Change, and Configuration Management (ASSET)

ID	MIL	Status	Practice Statement	Self Evaluation Notes
ASSET-2h	3	Partially Implemented	The information asset inventory is used to identify cyber risks, such as risk of disclosure, risk of destruction, and risk of tampering	We have partially implemented this practice.
ASSET-4f			Change logs include information about modifications that impact the cybersecurity requirements of assets	We have partially implemented this practice.
ASSET-5e			Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel	We have partially implemented this practice.
ASSET-5f			The effectiveness of activities in the ASSET domain is evaluated and tracked	This is an example note.
ASSET-2i	3	Not Implemented	Information assets are sanitized or destroyed at the end of life using techniques appropriate to their cybersecurity requirements	We have not implemented this practice.
ASSET-4e			Changes to assets are tested for cybersecurity impact prior to being deployed	We have not implemented this practice.

Figure 4.11. Excerpt from a Sample Table Summarizing Identified Gaps Using Model Results

5. Conclusions

The guidance provided in this publication provides step-by-step instructions for using the C2M2 Version 2.0 online tool. This includes instructions for navigating to the C2M2 online tool from the tool's website, navigating through the tool's pages, entering and reviewing maturity modeling information, saving input data and loading previous data files, generating a C2M2 output report, and reviewing the report.

Additional information on C2M2 Version 2.0, including a comprehensive guidance document, is available at https://c2m2.doe.gov/resources. That guidance document describes the C2M2's main structure and content. It includes descriptions of core concepts pertaining to the content and structure of the C2M2; reviews the architecture of the C2M2; and provides a detailed presentation of the model domains, objectives, and practices.