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

TABLE OF CONTENTS

LIST OF FIGURES

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 HTML-Based 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 Grace McNally, Robert Harrington, Cliff Glantz, Joseph Loftus, Kade Cornelison, Zachary Newsom, and Caleb Ng.

The team at PNNL supporting the production of the C2M2 HTML-Based tool included:

- Clifford Glantz (project manager)
- Paul Skare (principal investigator and energy sector coordinator)
- Joseph Loftus (Programming team lead)
- Grace McNally
- Kade Cornelison
- Christiana Tebbs
- Robert Harrington
- Jasmine McKenzie
- Sraddhanjoli Bhadra
- Claudia Hildebrand
- Carla Raymond
- Devan Farrell
- Aarne Nixon
- Scott Mix
- Zachary Newsom
- Caleb Ng
- Brian Dean
- Aiden Arends

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 and Brian Benestelli (Carnegie Mellon University Software Engineering Institute), John Fry (Axio), Lindsay Kishter (Nexight), Lynna Estep (North American Transmission Forum), Ed Ernst (North American Transmission Forum), Sri Nikhil Gourisetti (formerly of PNNL), and Easton Gervais (formerly of PNNL).

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

1. Introduction

Cyber threats continue to grow, and they represent one of the most serious operational risks facing modern organizations. National security and economic vitality depend on the reliable functioning of critical infrastructure and the sustained operation of organizations of all types in the face of such threats. The Cybersecurity Capability Maturity Model (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 technology (IT), operational technology (OT), and information assets and the environments in which they operate. The model can be used to:

- strengthen organizations' cybersecurity capabilities
- enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- share knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities
- enable organizations to prioritize actions and investments to improve cybersecurity capabilities

The C2M2 is designed to guide the development of a new cybersecurity program or for use with a self-evaluation methodology to enable an organization to measure and improve an existing cybersecurity program. Two C2M2 self-evaluation tools are available for free to any organization. These include a PDF-Based tool and an HTML-Based tool. Both tools may be obtained by visiting the C2M2 tool webpage (https://c2m2.doe.gov). Both tools maintain all data on users' local machines. A self-evaluation using one of the tools can be completed in one day, but the model could also be adapted for a more rigorous self-evaluation effort. This document provides detailed user instructions for the HTML-Based C2M2 tool.

The C2M2 provides descriptive rather than prescriptive guidance. The model content is presented at a high level of abstraction so that it can be applied by organizations of various types, structures, sizes, and industries. Broad use of the model by a sector can support benchmarking of the sector's cybersecurity capabilities (DOE, 2022).

Background Information on the C2M2

Since the initial release of Version 1.0 of the Cybersecurity Capability Maturity Model (C2M2) in 2012, 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. Several subsequent versions of the model have been developed and released since 2012. The C2M2, Version 2.1 incorporates guidance from energy sector cybersecurity practitioners to continue to address these challenges and improve alignment with internationally recognized cyber standards and best practices, including the NIST Special Publication 800-53 and the NIST Cybersecurity Framework (CSF) Version 1.1, released in April 2018. Additional information in C2M2 Version 2.1

enhancements is provided in the Cybersecurity Capability Maturity Model Version 2.1 "model document" (DOE, 2022).

The C2M2 Version 2.1 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***.

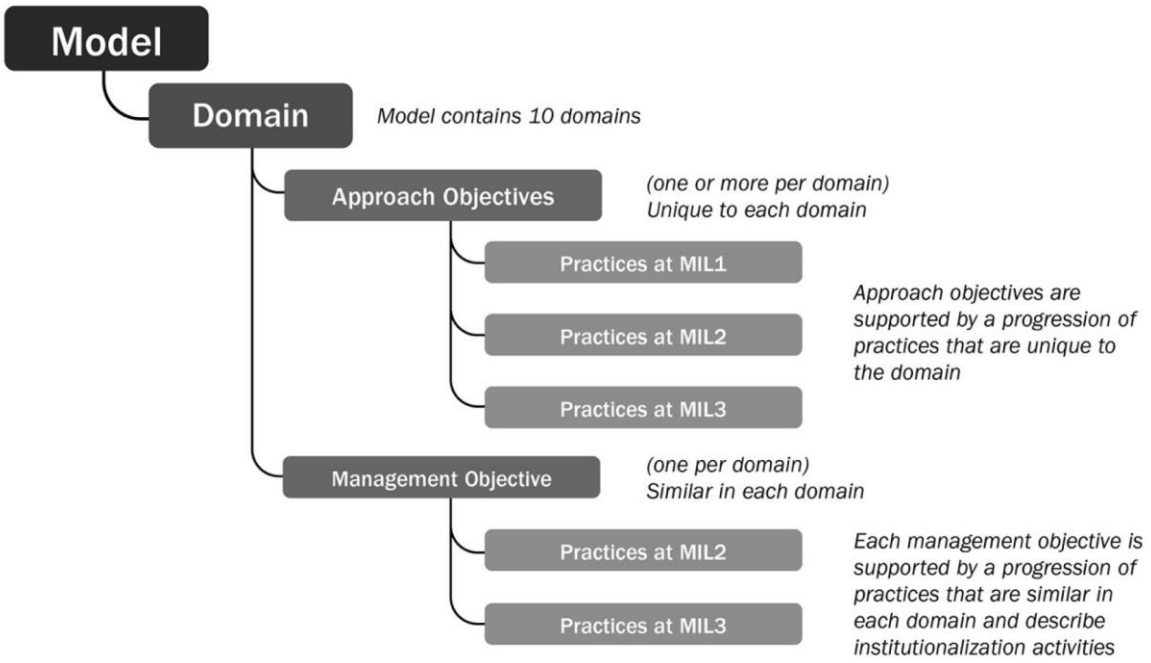

Figure 1.1. Model and Domain Elements

The model defines four maturity indicator levels (MILs) that indicate a progression of maturity and are applied independently to each domain in the model. Practices are assigned a MIL (either MIL0, MIL1,

MIL2, or MIL3) that corresponds to the level of programmatic maturity associated with that practice or not practiced at all:

- **MIL0** indicates that a practice is not implemented or has not been considered.
- **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. MIL achievements need to be aligned with business objectives and the organization's cybersecurity program strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL versus its potential benefits. However, the model was designed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

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.

Descriptions for self-evaluation response options are shown in the following table.

Response	Implementation Description
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed by the organization

Table 1: Description of Self-Evaluation Response Options

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 2.1 HTML-Based 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 HTML-Based 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 a self-evaluation. 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 self-evaluation results – including providing results for each objective in a domain.
- A detailed table containing all self-evaluation 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 Cybersecurity Capability Maturity Model document (DOE, 2022). 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 HTML-Based Tool and Entering Data

Accessing the C2M2 HTML-Based Tool

The C2M2 HTML-Based 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. The new version 2.1 splash screen alerts users of the switch from the version 2.0 to 2.1 as the default method for self-evaluations. The alert can be cleared by selecting the "x" and the end of the splash alert, as shown in the red rectangle below.

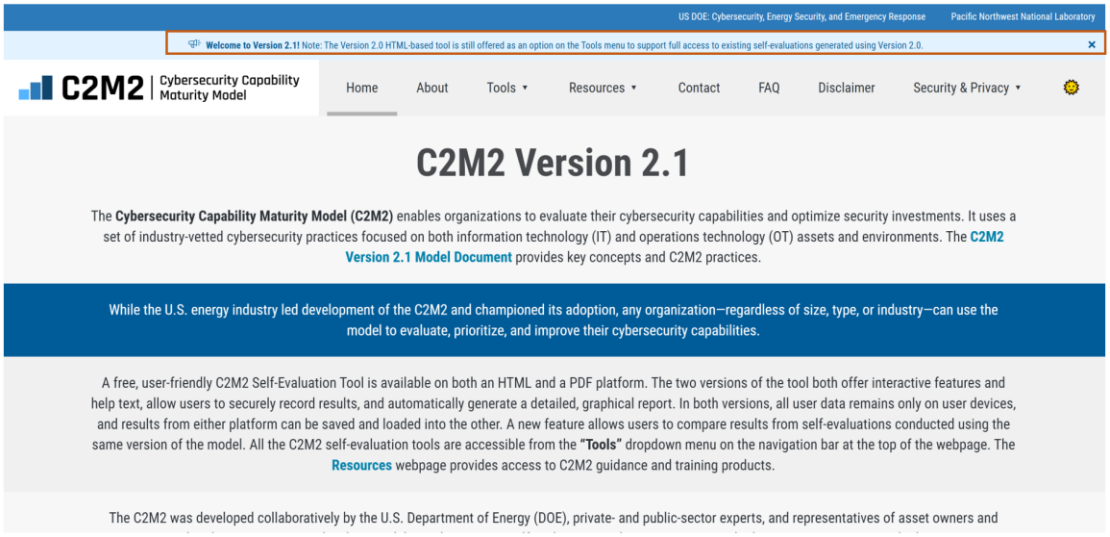

Figure 2.1. The C2M2.doe.gov Homepage

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

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

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

("A") learn more about the C2M2

("B") access Version 2.0 and 2.1 of the C2M2 HTML-Based tool, request the C2M2 PDF-Based tool, and access the HTML-Based Self-Evaluation Results Comparison tool.

("C") access additional C2M2 information resources. The resources site has been expanded to provide access to the PDF-Based tool user guide, Excel, and PowerPoint files with a broader scope than just the HTML-Based tool.

("D") view contact information for support on the C2M2 and its associated tools

("E") examine frequently asked questions

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

("G") read about how the C2M2 HTML-Based tool 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 as seen in **Figure *2.3***.

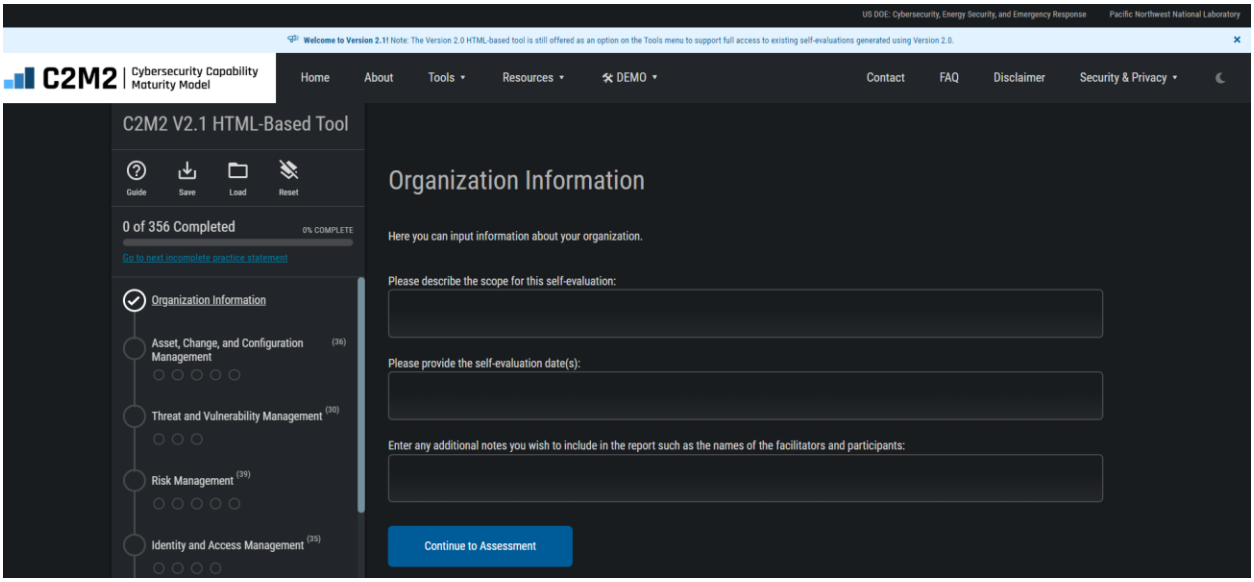

Figure 2.3. Dark Mode

To access the C2M2 model, click the "Tools" button in the menu bar (labeled "B" in **Figure *2.2***). This will open a drop-down menu as shown in **Figure *2.4***. Click the "C2M2 V2.1 HTML-Based Tool" to begin using the HTML-Based tool. Select the "Management Priorities" to view and define goals for each domain. Clicking the "Request C2M2 V2.1 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. Click the "Self-Evaluation Results Comparison" to open a new HTML-Based tool to compare the results from multiple C2M2 self-evaluations. Click the "C2M2 V2.0 HTML-Based Tool (Previous Version)" to open the HTM-based C2M2 V2.0 tool that was released in June 2021. Maintaining the ability of users to access the V2.0 tool will allow them to view, share, and modify their existing V2.0 assessments. However, new assessments should be conducted using V2.1. V2.1 will accept data for the 293 practices largely unchanged from V2.0, leaving only 63 new or extensively modified practices will need to be assessed to update a V2.0 assessment to V2.1.

Accessing the C2M2 HTML-Based Tool

Now the user is 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 pane area on the left ("A") and the data entry area ("B").

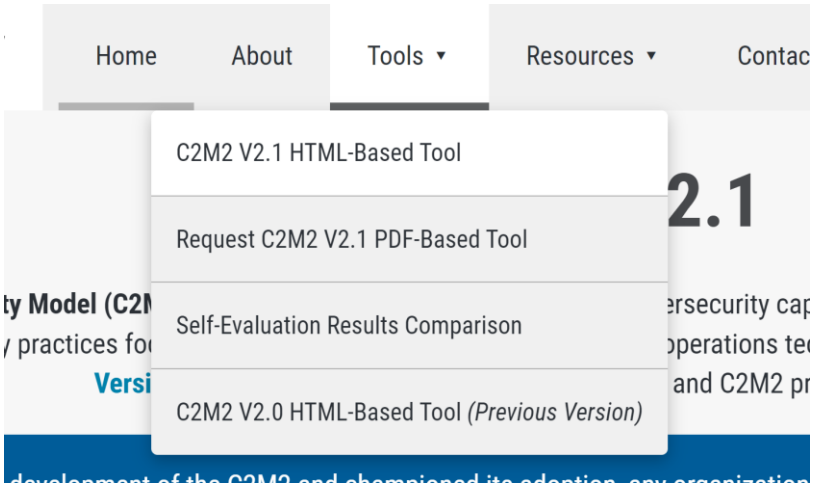

Figure 2.4. Tool Drop-Down Menu

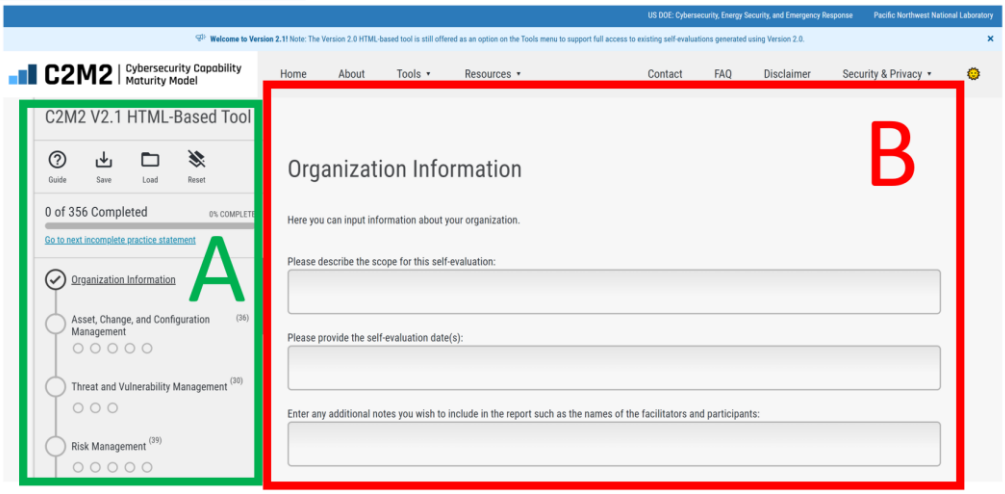

Figure 2.5. The Work Areas Within the Tool

The left area ("A" In **Figure *2.5***, also called the "navigation pane") starts with the name and version of the model currently accessed. Below the name and version number contains buttons to view the "Guide", "Save", "Load", or "Reset" the self-evaluation data. Beneath these buttons is a progress bar that displays the number of answered practice statements for the self-evaluation 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 self-evaluation, the icons for domains and objectives in the navigation pane are displayed as "checked" to acknowledge their completion. This navigation pane 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 is used here to enter "organization information" (i.e., information on the scope of the self-evaluation and the people performing the self-evaluation). On other tool pages, it is used to display descriptions of each domain, enter practice implementation scores, enter practice notes, or display messages to the user.

The Navigation Pane

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

The "Guide" button is labeled as "A." **Figure 2.7** shows the pop-up that will appear when selected. It allows the user to choose to navigate away from the self-evaluation and open the instruction guide.

The "Save" button is labeled as "B." It allows the user to download their current self-evaluation data to their computer. The data is 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 data can also be copied from the clipboard into a text file.

The "Load" button is labeled as "C." It allows the user to load a saved self-evaluation by dragging a saved JSON format data file and dropping it in the load window.

The "Reset" button is labeled as "D." Clicking it gives the user the option to clear the answered practice statements and start with a clean (i.e., blank) self-evaluation.

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

Clicking the "Go to next incomplete practice statement" button (labeled as "E") will navigate the self-evaluation to the next unanswered practice. This is quite useful when working with a partially completed self-evaluation 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 "F", "G", "H", and "I"), takes the user to the corresponding domain. Domains for which all the practices are assessed are denoted with a checkmark (as shown by "F"). A bolded circle indicates the current domain (as shown by "I"). If a circle is unchecked (as shown by "G" and "H"), practices in the domain are not yet fully assessed.

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

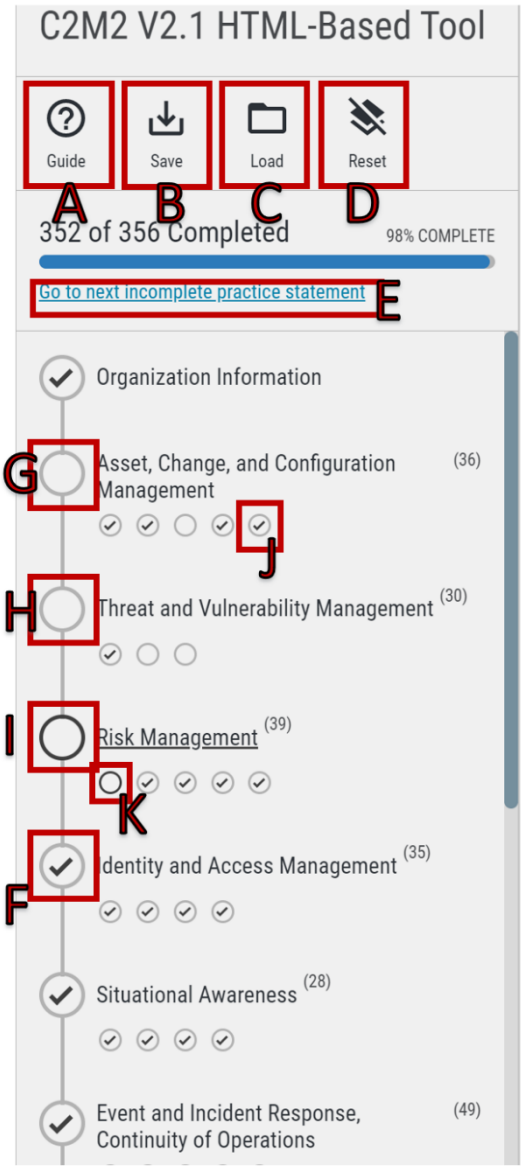

Figure 2.6. Navigation Pane

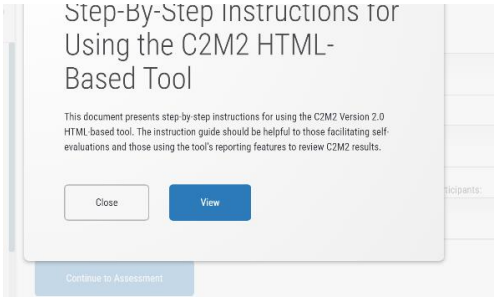

Figure 2.7. Guide Pop-Up

an objective circle icon indicates all the practices in the objective are scored (as shown by "J"). A slightly bolded circle indicates the current objective being assessed (as shown by "K").

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 a self-evaluation report. In this version of the tool, results cannot be displayed until all the C2M2 practices are scored.

Entering Data

Figure *2.8* presents the introductory screen for the self-evaluation. 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).

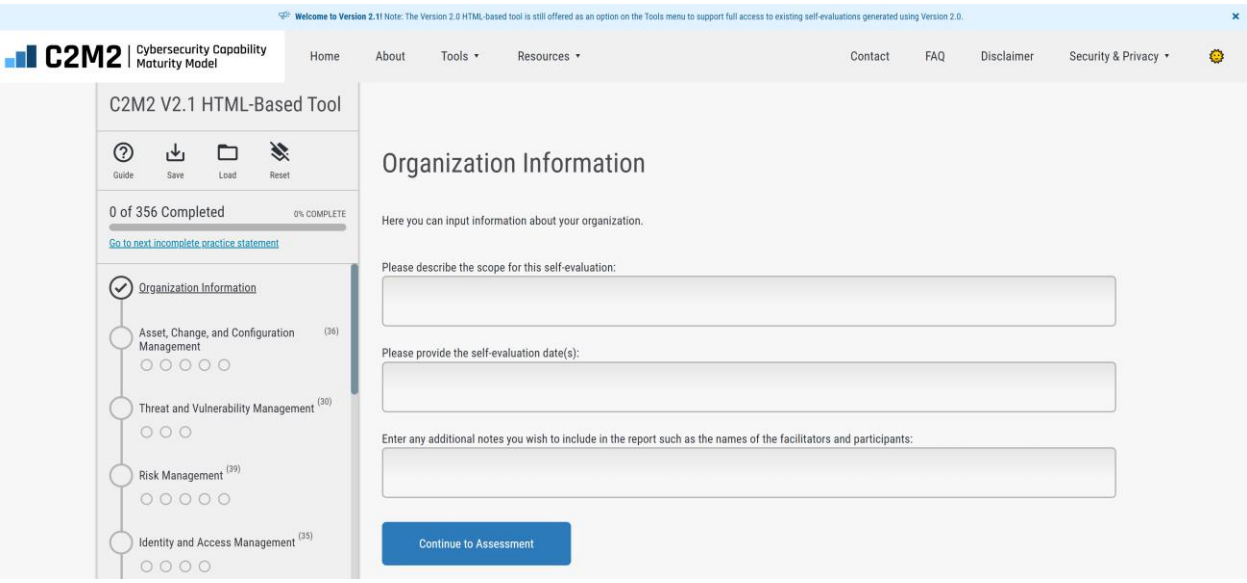

Figure 2.8. The "Organization Information" Screen

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-evaluation's 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 *2.9***) displays the title of the first domain, its purpose, its objectives, and a description of the domain. Click the "Begin" button (as shown by "A") to start the self-evaluation of this domain. The "Begin" button is offered above the purpose statement (near the top of the screen) and is repeated below the domain description (at the very bottom of the page).

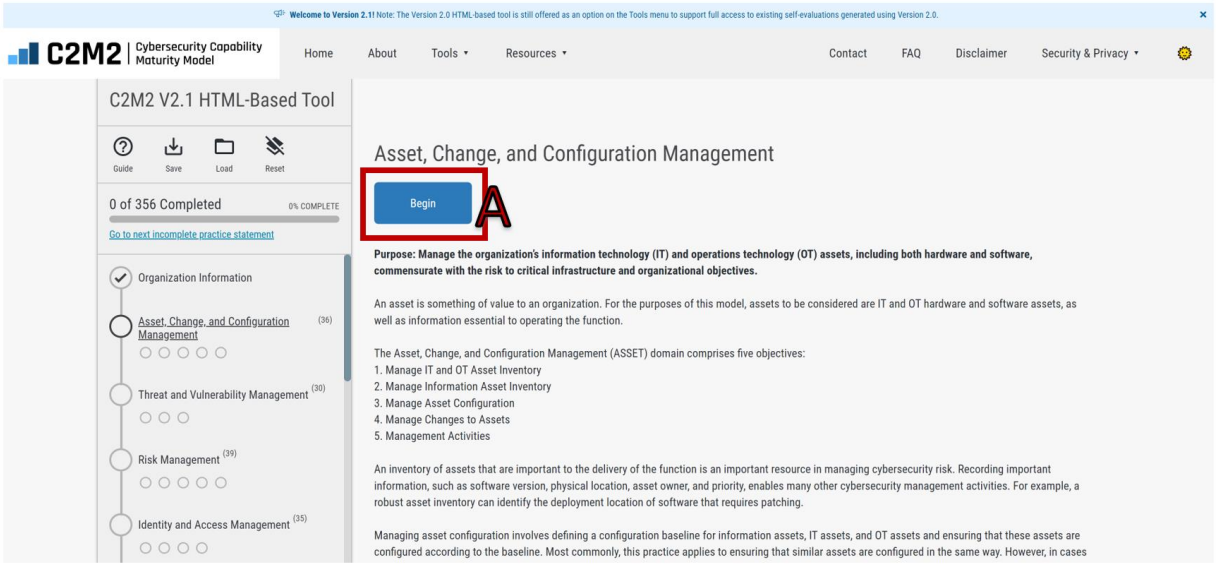

Figure 2.9. The Initial Display of the First Domain

After clicking "Begin" from **Figure *2.9***, **Figure *2.10*** is displayed. **Figure *2.10*** opens to the first objective (i.e., "Objective 1: *Manage IT and OT Asset Inventory*") in the current domain ("*Asset, Change, and Configuration Management*" or "ASSET" for short). Eight practices are in this objective and as indicated by the blank white circles, none have an assigned implementation practice. Clicking any of the blank circles in **Figure *2.10*** starts the self-evaluation. If "Begin" in **Figure *2.9*** is clicked, the first practice in the indicated objective will be displayed as shown below in **Figure *2.10***.

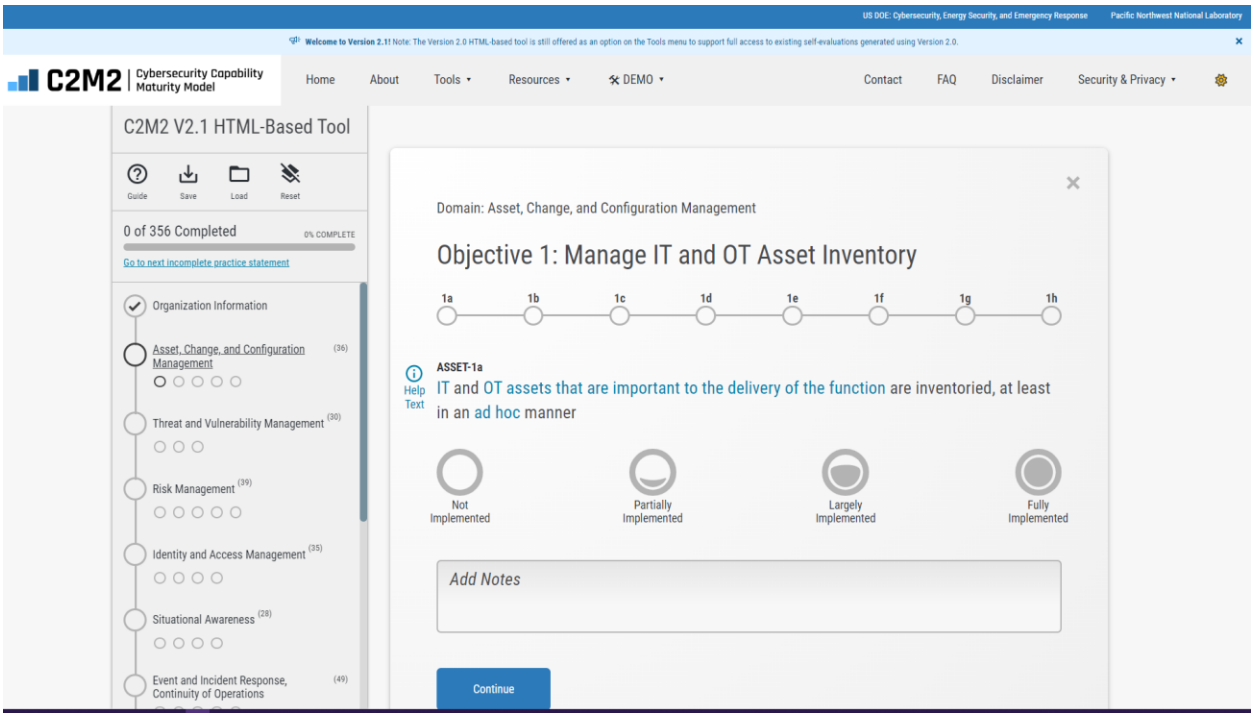

Figure 2.10. The First Practice in the First Objective of the First Domain

Note the text shown in **Figure *2.10***, and throughout the tool, displays some words or phrases in a light blue font. Clicking on a word in blue font opens a pop-up as shown in **Figure *2.11*** that displays the C2M2 glossary defintion of this term. The pop-up remains opened until it is cancled by selecting the "x" in the upper right corner of the pop-up, by clicking anywhere outside the pop-up, or by clicking on another glossary term. Selecting another glossary term will automatically close a currently opened glossary definition and open the new definition.

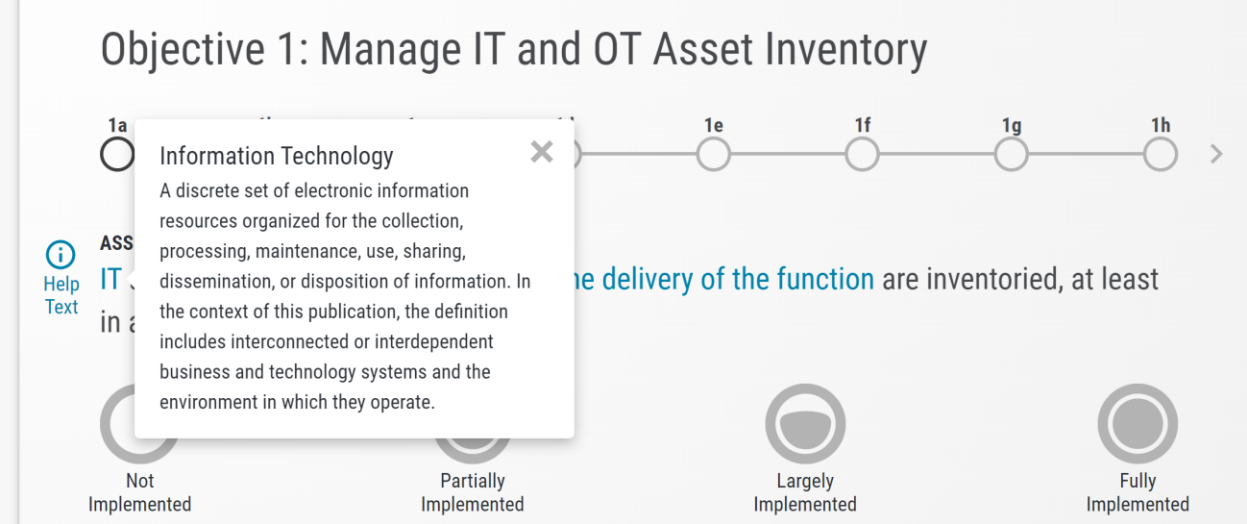

Figure 2.11. Pop-up Definition of Glossary Terms from within the Tool

The glossary of terms is also accessible from the resources dropdown in the menu bar).

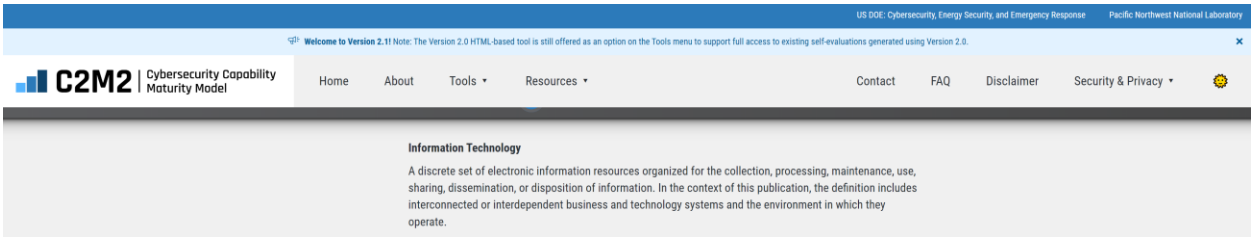

Figure 2.12. The C2M2 Glossary

Figure *2.10* displayed a lot of information for starting the self-evaluation. **Figure *2.13*** shows a completed version of the first set of practices in Objective 1. The following description will explain each of the key features in Figure 2.13.

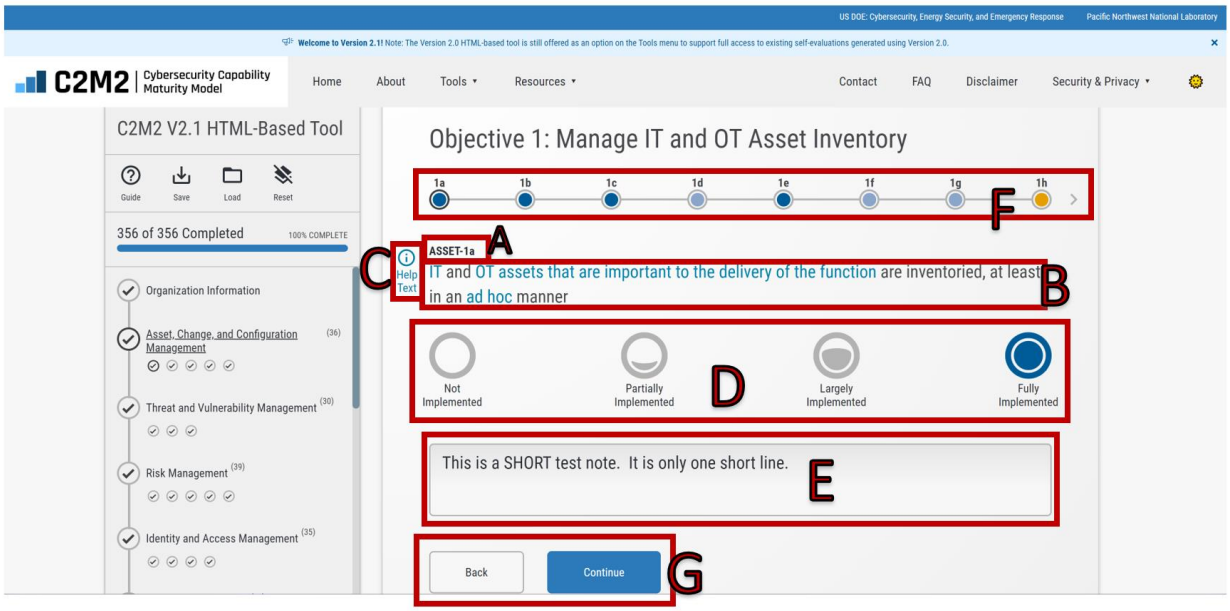

Figure 2.13. Scoring and Documenting a Practice Statement

In **Error! Reference source not found.**, we see the results for the first practice in this objective, "ASSET-1 a" (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 Text" icon (labeled "C"), and Help Text will be displayed on the screen as shown in **Figure *2.14***.

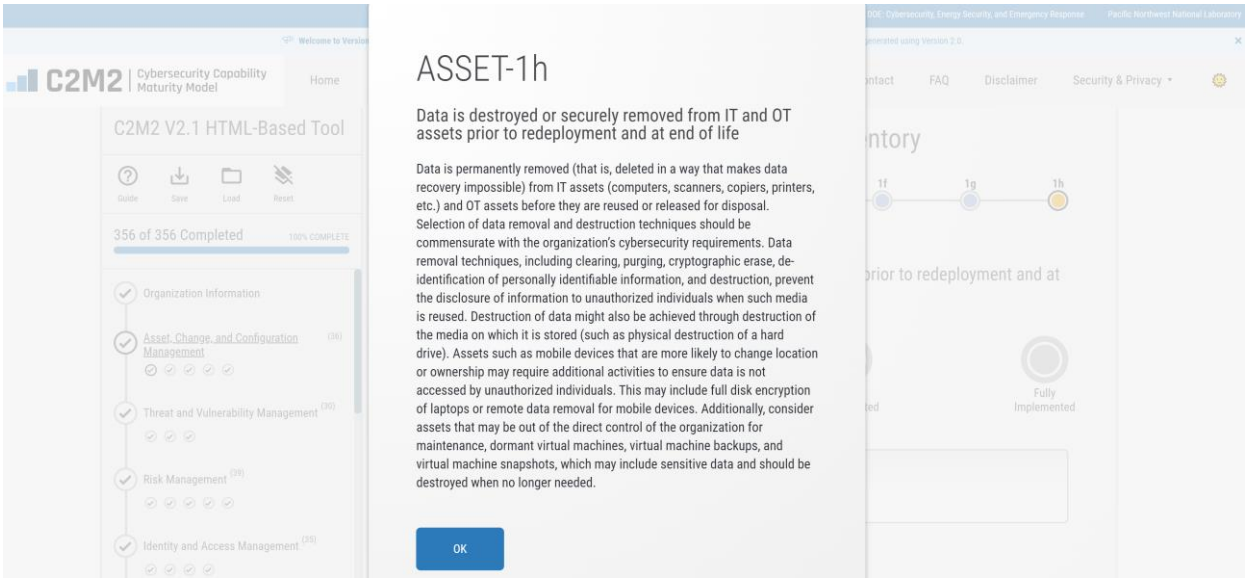

Figure 2.14. An Example of the Help Text Display

After reading and gaining an understanding of the practice, click one of the four implementation level choices available in **Figure *2.13*** (labeled "D"). Not, Partially, Largely, and Fully implemented are the four options. The options are color-coded and have different icons. 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 Microsoft 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.

After completing an evaluation of each of the practices for the current Objective, a summary of the completed practices and their scores are displayed in **Figure *2.15***. Scroll to the bottom of the page and click "Continue to the Next Section" to continue.

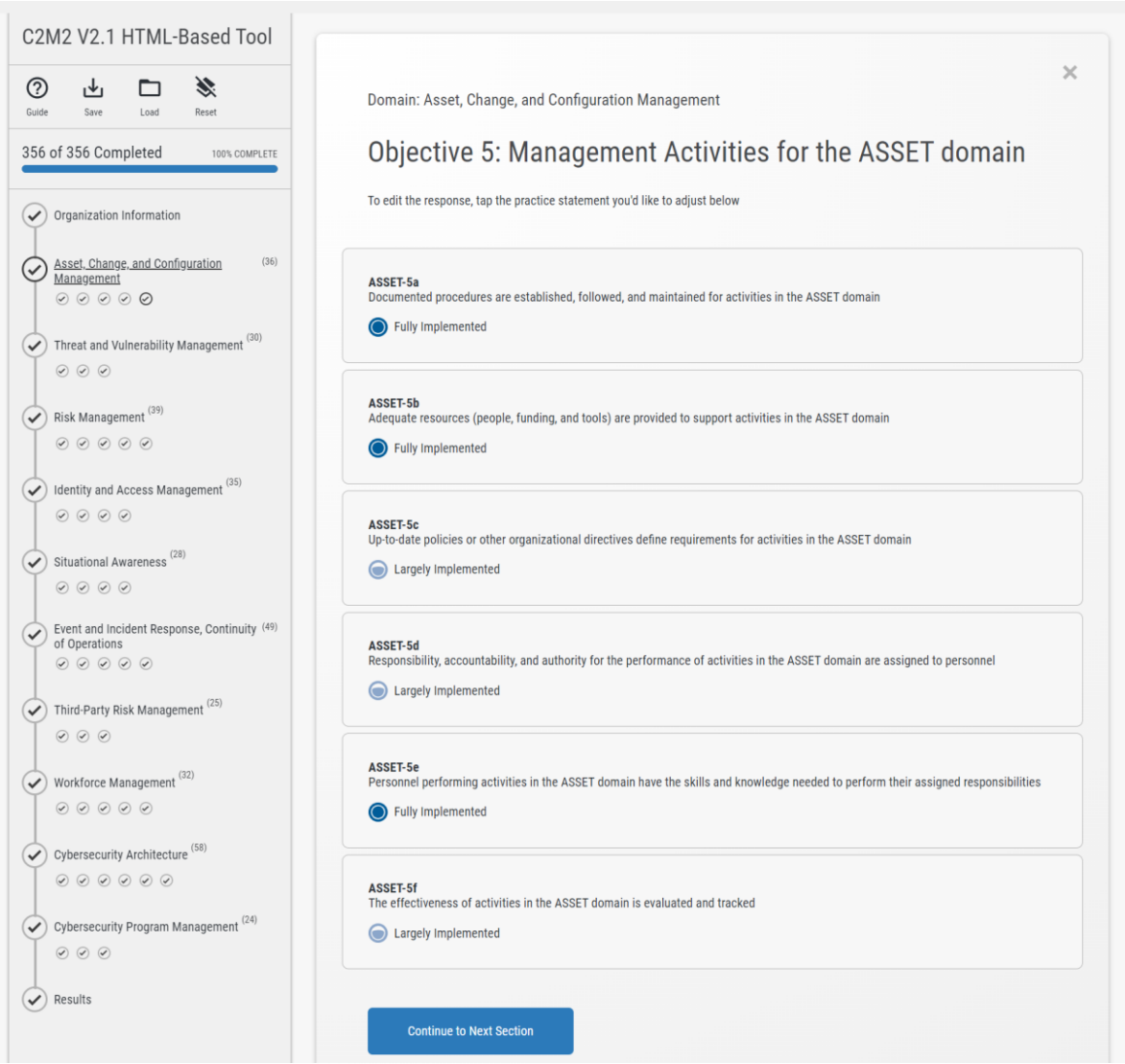

Figure 2.15. Summary Scores for the Current Objective

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 *2.16***). 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"). Clicking a checked objective in the navigation pane displays a concise summary of the scoring for all the objective's practices (as illustrated in Figure 2.15). Clicking any practice in that concise summary takes the user to that practice's scoring screen (e.g., Figure 2.13).

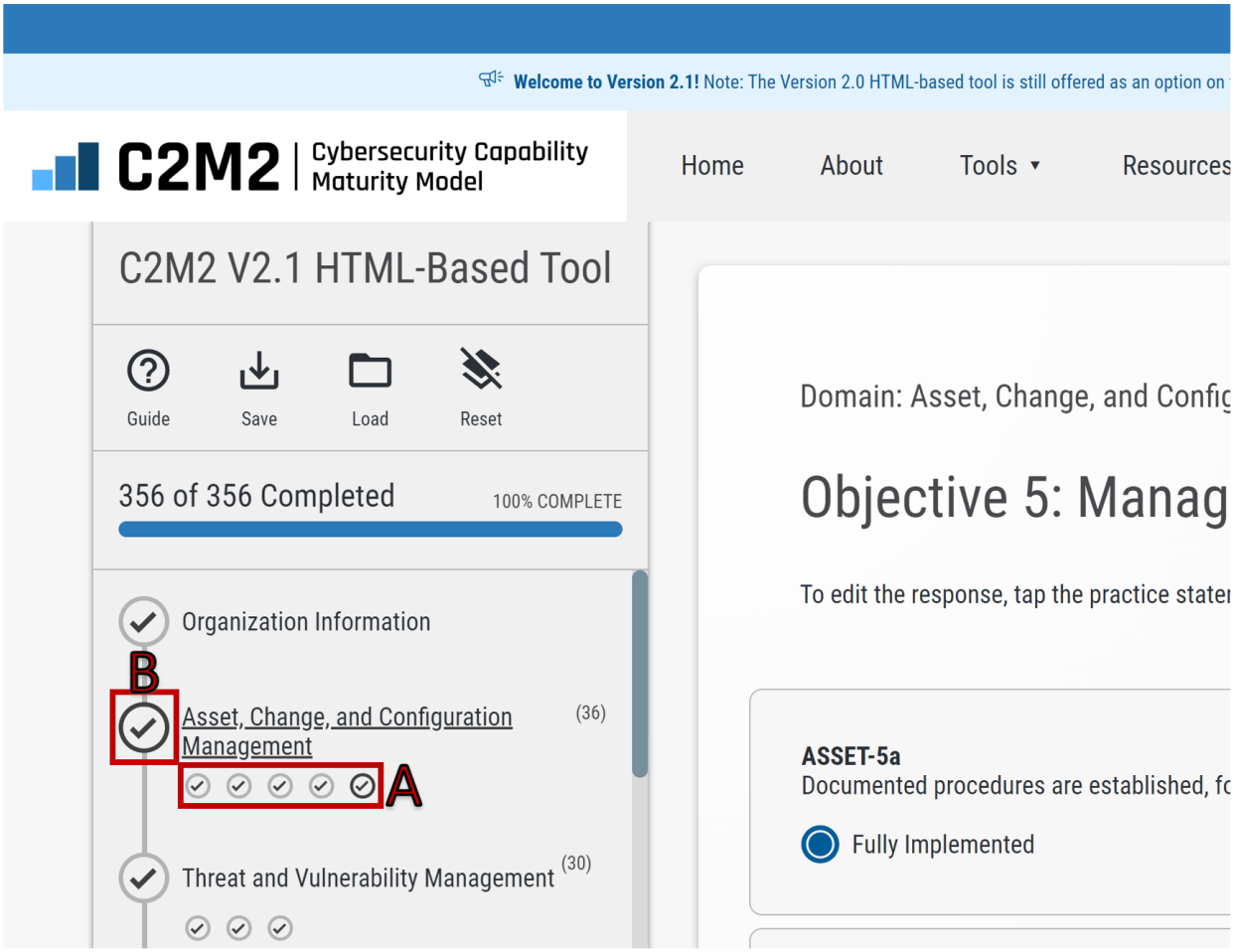

Figure 2.16. All Practices for Each Objective in the ASSET Domain are *Scored*

When all the practices in all the domains have been scored, the evaluation is complete, and the "Assessment Complete" screen will be displayed (**Figure *2.17***). The user can also click "Results" labeled as "A" in **Figure *2.17*** at the bottom of the left navigation window to display the "Assessment Complete" screen.

From the Assessment Complete screen, click "View Report" labeled "B" in **Figure *2.17*** to generate an automated evaluation report.

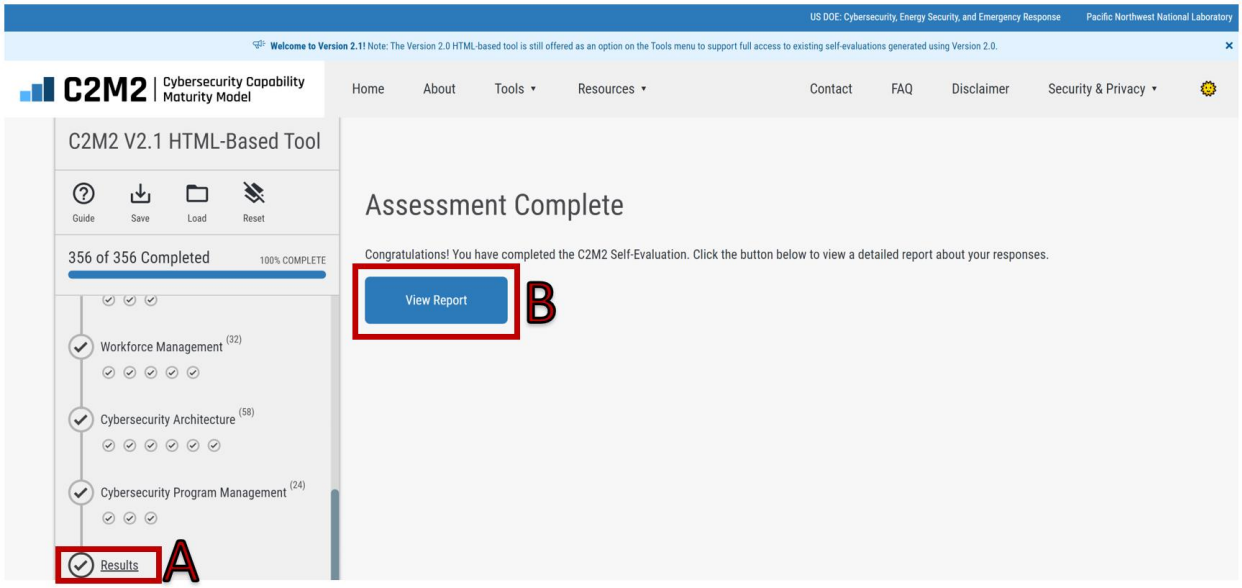

Figure 2.17. Completed Self-Evaluation

Note that 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 (shown in **Figure *2.18***) provides an indicator that the report is being generated. When completed, the report will be displayed on the right-side window of the tool.

Figure 2.18. 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 self-evaluation 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 is 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 C2M2 HTML-Based or PDF-Based tools). The Reset function erases the current self-evaluation data and allows the user to start over from scratch with a new evaluation (previously saved files are not affected by the Reset function).

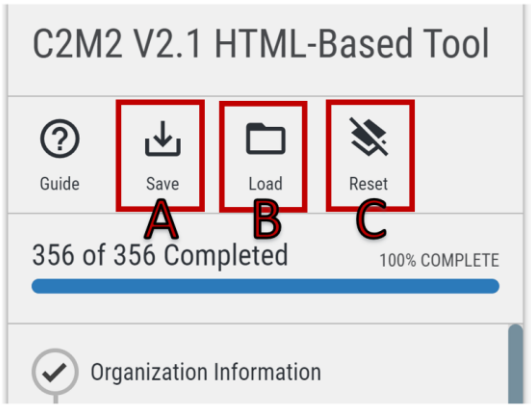

Figure 3.1. The Save, Load, and Reset Icons

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.

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 C2M2 JSON file is the preferred and standard approach for loading data into the tool.

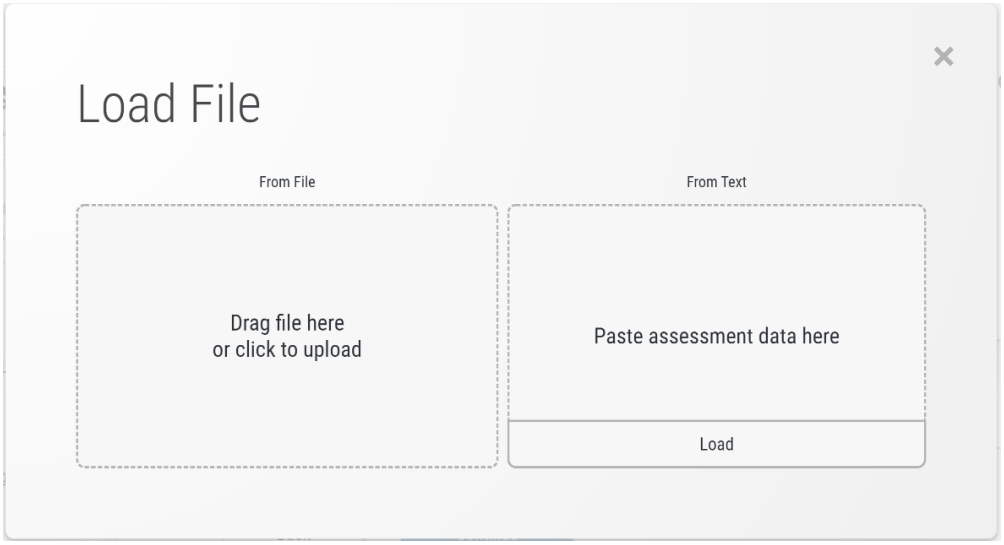

Figure 3.3. The Load File Pop-up Window

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.

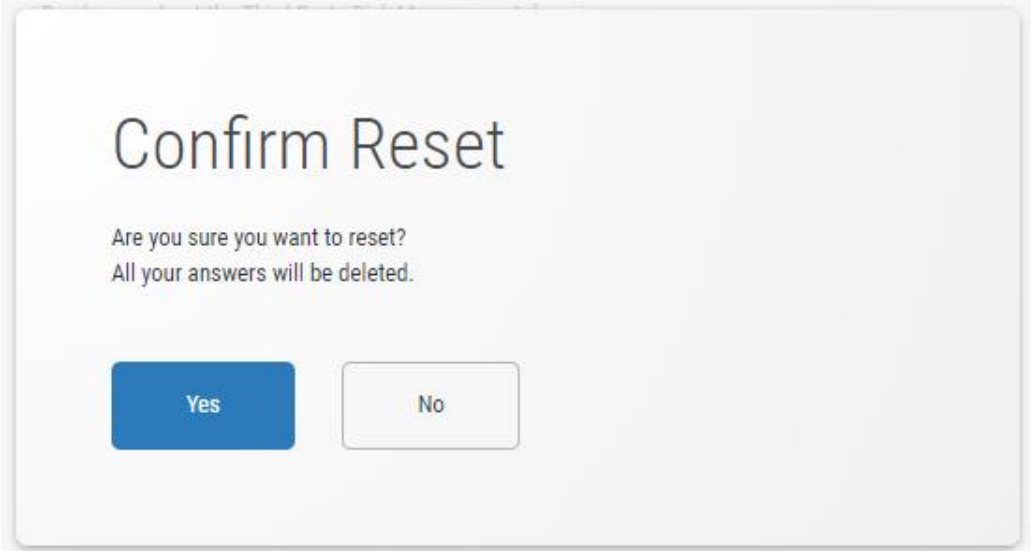

Figure 3.4. The Confirm Reset Pop-Up Window

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 self-evaluation (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).

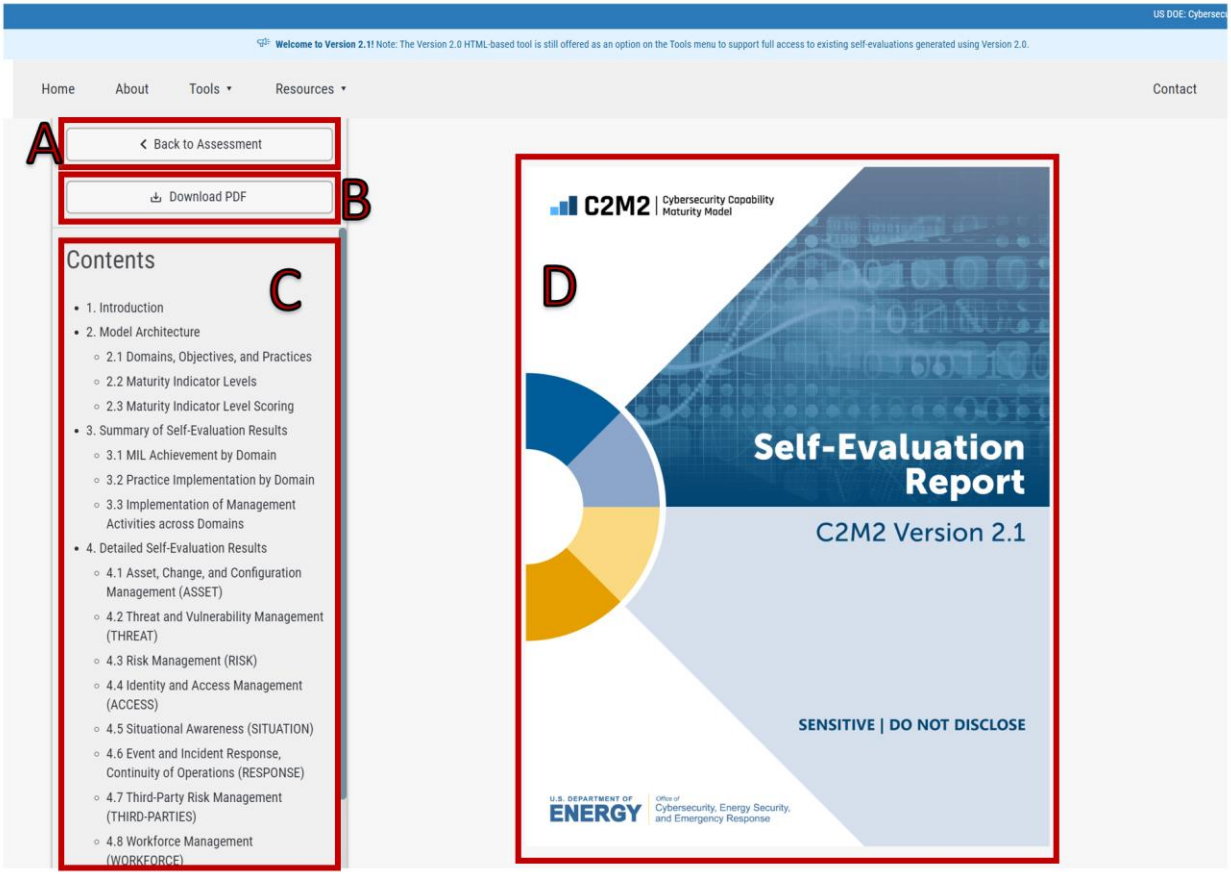

Figure 4.1. The Top of C2M2 Self-Evaluation Report

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

1. Introduction
2. Model Architecture
    - 2.1 Domains, Objectives, and Practices
    - 2.2 Maturity Indicator Levels

Figure *4.2* displays the four levels of practice implementation scores used throughout the HTML-Based 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.

Response	Implementation Description
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	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 self-evaluation, the self-evaluation dates, and additional notes – all information entered by the C2M2 facilitator in the "Organization Information" section of the tool. It also includes the date and time the self-evaluation report was created and the version of the C2M2 used to generate the report. Section 2: "Model Architecture" describes the Domain – Objective – Practice structure of the model. It provides the purpose description of 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 Self-Evaluation Results – 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 achieved by domain in a user friendly, comparable bar chart. Each of the 10 domains is represented by a row that indicates the MIL score achieved for the domain. The longer the horizontal bar, the greater the MIL achieved.

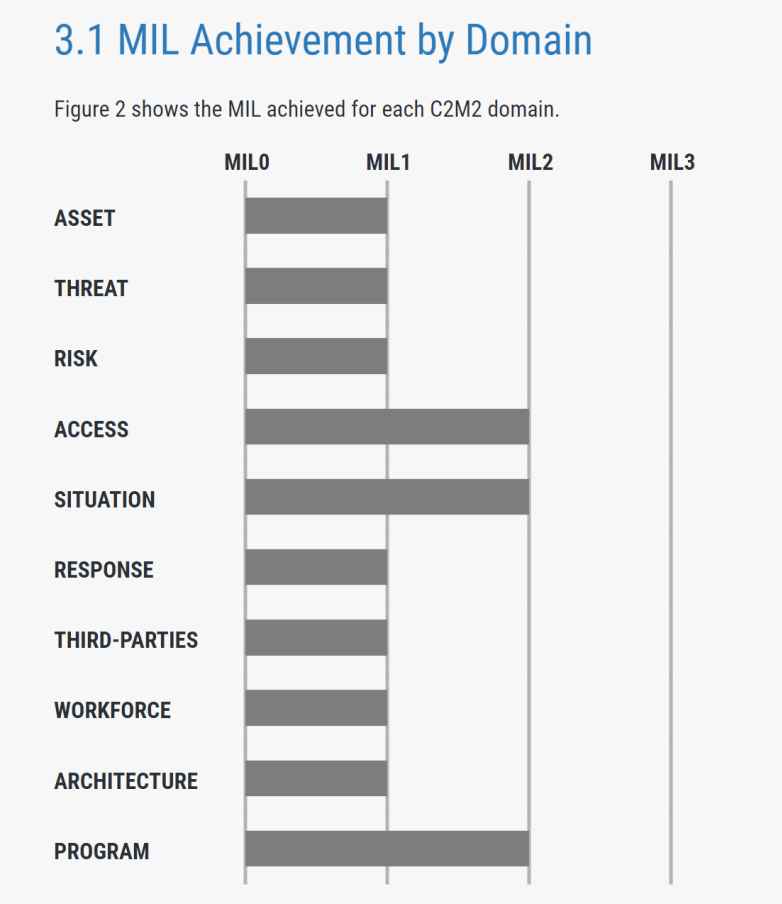

Figure 4.3. MIL Achieved by Domain

Figure *4.4* demonstrates the summary of MIL achieved using the traditional donut diagrams. The columns represent each domain, and the rows present for each domain, the implementation scores for the practices needed to achieve the indicated MIL (i.e., MIL1, 2, or 3). Below the donut diagrams is the overall MIL score achieved for each domain. In the example presented in **Figure *4.4***, the ACCESS, SITUATION, and PROGRAM domains achieve MIL2 because all the practices at MIL1 and MIL2 are largely or fully implemented. On the other end of the spectrum, the other seven domains achieve only MIL1 because it they each have some partially or not implemented MIL2 practices.

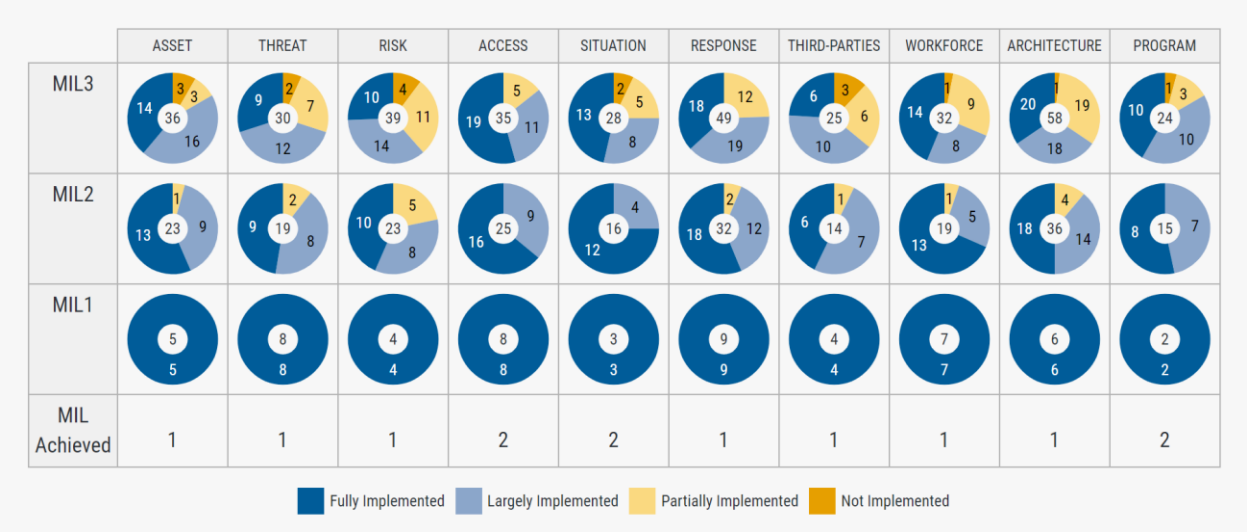

Figure 4.4. Sample Summary Donut Diagram Presenting MIL Score by Domain

Figure 4.5 provides a close-up view of the three donut diagrams and the MIL score for 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). All five practices are indicated at the "fully implemented" level (the dark-blue segment of the donut). There are no "largely implemented", "partially implemented", nor "not implemented" MIL1 practices for this domain.

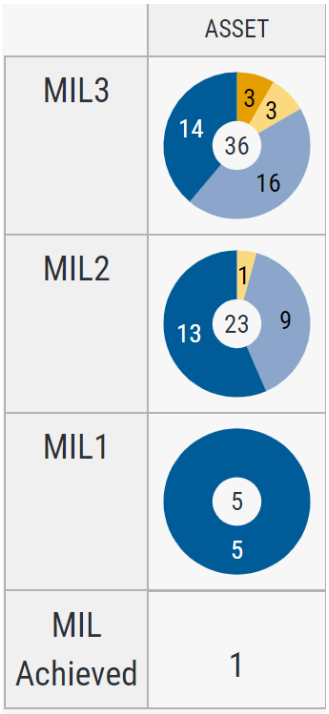

Figure 4.5. Close-up for a Domain

At the next level up, for MIL2, the number "23" in the middle of the donut indicates there are 23 practices at MIL1 and MIL2 that must be scored as fully or largely implemented for MIL2 to be achieved. This consists of the five practices from MIL1 and 18 additional practices for MIL2. Considered together, there are 13 practices that are fully implemented and nine that are largely implemented (the light-blue segment). There is one "partially implemented" and no "not implemented" MIL1 or MIL2 practices for this domain.

To achieve MIL3, there are 36 practices at MIL1, 2, and 3 that must be scored as fully or largely implemented. In total, there are 14 practices that are fully implemented, 16 practices are largely implemented, 3 practices that are partially implemented (indicated by the yellow segment in the donut diagram), and three practices that are not implemented (indicated by the orange segment in the donut diagram).

A net MIL score of one is achieved for the ASSET domain because it represents the highest MIL level achieved (all the associated MIL1 practices are fully or largely implemented, but the MIL2 practices still have partially or not implemented objectives).

The individual donut diagrams in **Figure *4.4*** 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 *4.6***.

In **Figure *4.6***, the data 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 filter 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.

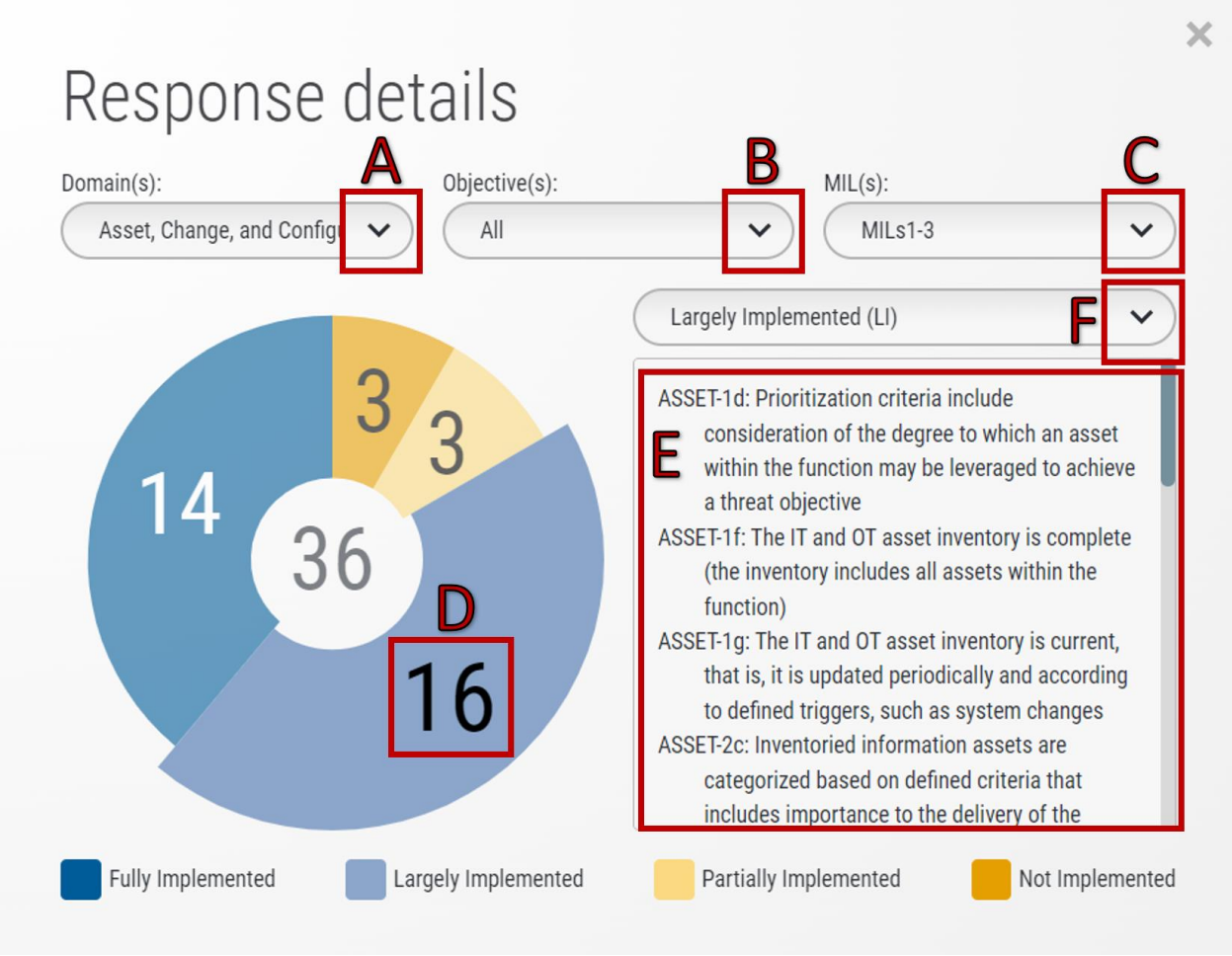

Figure 4.6. Response Details for MILs 1-3 of Asset, Change, and Configuration Domain

In **Figure *4.6***, 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 *4.7* displays a summary of the implementation scores for the Management Activities Objective that is found in each domain (it is the only Objective that is common across all ten domains). This figure

is provided in the report 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 *4.7*** 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 two domains: ASSET and ACCESS. In contrast, lower implementation scores are recorded for one or more practices in the other eight domains. For example, in the RISK domain, three of the six practices are 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	FI	FI	LI	FI	FI	FI	FI	FI	FI	FI
Adequate resources (people, funding, and tools) are provided to support activities in the domain	FI	LI	PI	FI	FI	FI	LI	FI	FI	FI
Up-to-date policies or other organizational directives define requirements for activities in the domain	LI	LI	PI	FI	FI	LI	LI	FI	FI	FI
Responsibility, accountability, and authority for the performance of activities in the domain are assigned to personnel	FI	LI	LI	FI	LI	LI	LI	LI	LI	LI
Personnel performing activities in the domain have the skills and knowledge needed to perform their assigned responsibilities	LI	PI	LI	FI	LI	LI	PI	PI	PI	LI
The effectiveness of activities in the domain is evaluated and tracked	LI	PI	PI	LI	PI	PI	NI	PI	PI	PI

Figure 4.7. 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 *4.8***). In this section, separate donut diagrams are not presented for the three MILs. Instead, results are consolidated so there is only one donut diagram for each objective. This single donut diagram is similar to the MIL3 donut diagram presented in Figure 4.5. It incorporates the implementation scores for all the practices across all the MILs.

4.1 Domain: Asset, Change, and Configuration Management (ASSET)

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

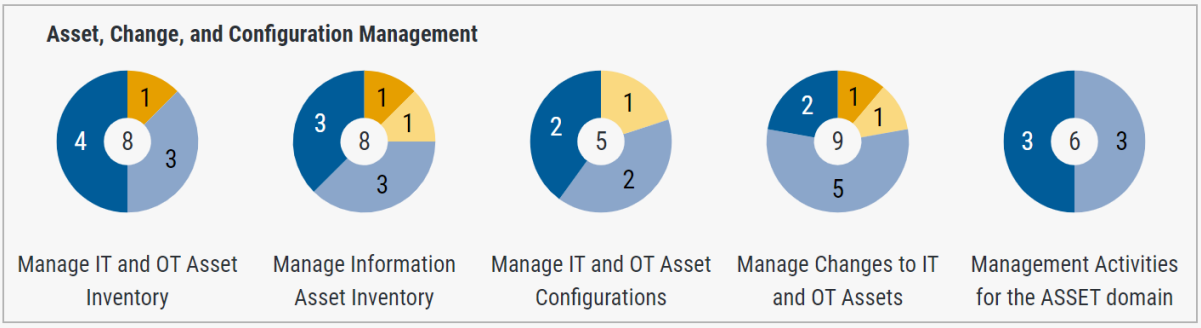

Figure 4.8. Detailed Evaluation Donut Diagrams for the ASSET Domain

Also presented in this section of the report is a figure (a sample is provided in **Figure *4.9***) that displays the implementation scores for each of the practices in the domain.

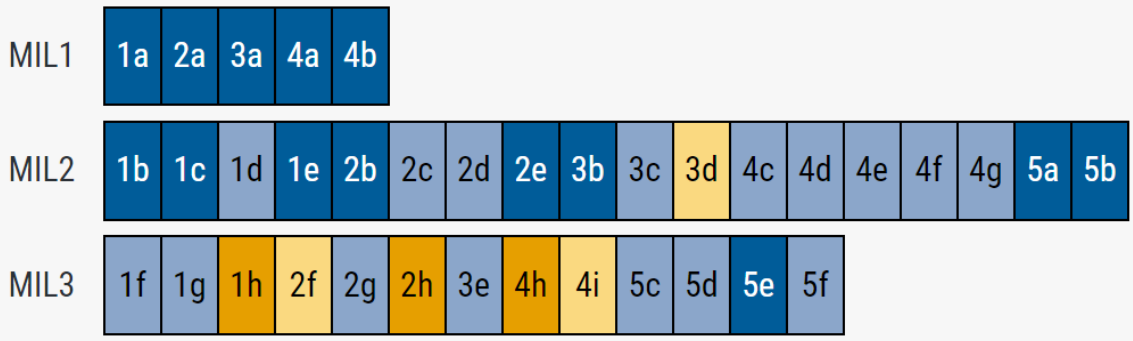

Figure 4.9. Detailed Evaluation Practice Statement Summary for ASSET Domain

After presenting this information, a lengthy table is provided (**Figure *4.10*** is a partial sample) that presents more detailed information about the practices. Each practice is listed in order first by domain, then objective, then by practice number. The MIL that each practice evaluates is given in the left most column. In the next column, the practice identifier is presented. The third column presents the text of the practice. The final column provides the assigned implementation score for the practice. This table presents a concise presentation of key data entered into the C2M2 self-evaluation tool.

Objective 1: Manage IT and OT Asset Inventory

MIL1	ASSET-1a	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	FI
MIL2	ASSET-1b	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	FI
MIL2	ASSET-1c	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	FI
MIL2	ASSET-1d	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	LI
MIL2	ASSET-1e	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions)	FI
MIL3	ASSET-1f	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	LI
MIL3	ASSET-1g	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	LI

Figure 4.10. Presentation of the MIL Level, Objective Identifier, Text, and Implementation Score for Each Practice

Using the Evaluation Results – Report Sections 5 - 7

Section 5 in the report begins by providing information on how to use the self-evaluation results (a four-step process is recommended). Section 6 presents a table with detailed information for each practice. Each row in the table presents the practice identifier, the corresponding maturity level the practice evaluates, the practice statement, the implementation score (i.e., user response), and the self-evaluation note for the practice. **Figure *4.11*** displays a sample row from this table.

Domain: Asset, Change, and Configuration Management (ASSET)

ID	MIL	Practice	Response	Self-Evaluation Notes
ASSET-1a	1	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	Fully Implemented	This is a SHORT test note. It is only one short line.

Figure 4.11. Sample Row from the Table Presenting the Self-Evaluation Notes

Section 7 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 *4.12*** presents a sample excerpt from this table.

Domain: Threat and Vulnerability Management (THREAT)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented	THREAT-1i	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	
		THREAT-2h	Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs])	This is a SHORT test note. It is only one short line.
3	Partially Implemented	THREAT-1j	Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored	
		THREAT-1l	Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective	
		THREAT-2k	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action	This is a SHORT test note. It is only one short line.

Figure 4.12. 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 2.1 HTML-Based tool. This includes instructions for navigating to the C2M2 HTML-Based 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 2.1 is available at https://c2m2.doe.gov/resources. The C2M2 model is particularly interesting because it 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.

6. References

DOE. 2022. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. June 2022. U.S Department of Energy. Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Washington DC. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf