PNNL-34954

User Guide to the Facility Cybersecurity Capability Maturity Model (F-C2M2) Assessment

September 2023

Arcadio Vielma
Roger Kwon
Paul Francik
Julia Rotondo
Chris Bonebrake

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

User Guide to the Facility Cybersecurity Capability Maturity Model (F-C2M2) Assessment

September 2023

Arcadio Vielma
Roger Kwon
Paul Francik
Julia Rotondo
Chris Bonebrake

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

List of Effective Pages

<table>
<tr><td colspan="4">Dates of issue for latest changes are:
Total number of pages in this publication is _________ consisting of the following:</td></tr>
<tr><th>Page Number</th><th>Change Number</th><th>Page Number</th><th>Change Number</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Table 1: Latest Changes

Revision History

Name	Date	Reason For Changes	Version
PNNL	09/29/2023		Version 1.0

Table 2: Revision History

Acronyms and Abbreviations

C2M2	Cybersecurity Capability Maturity Model
FCF	Facility Cybersecurity Framework
F-C2M2	Facility Cybersecurity Capability Maturity Model
FEMP	Federal Energy Management Program
IT	information technology
NIST	National Institute of Standards and Technology
OT	operational technology

Contents

Figures

Tables

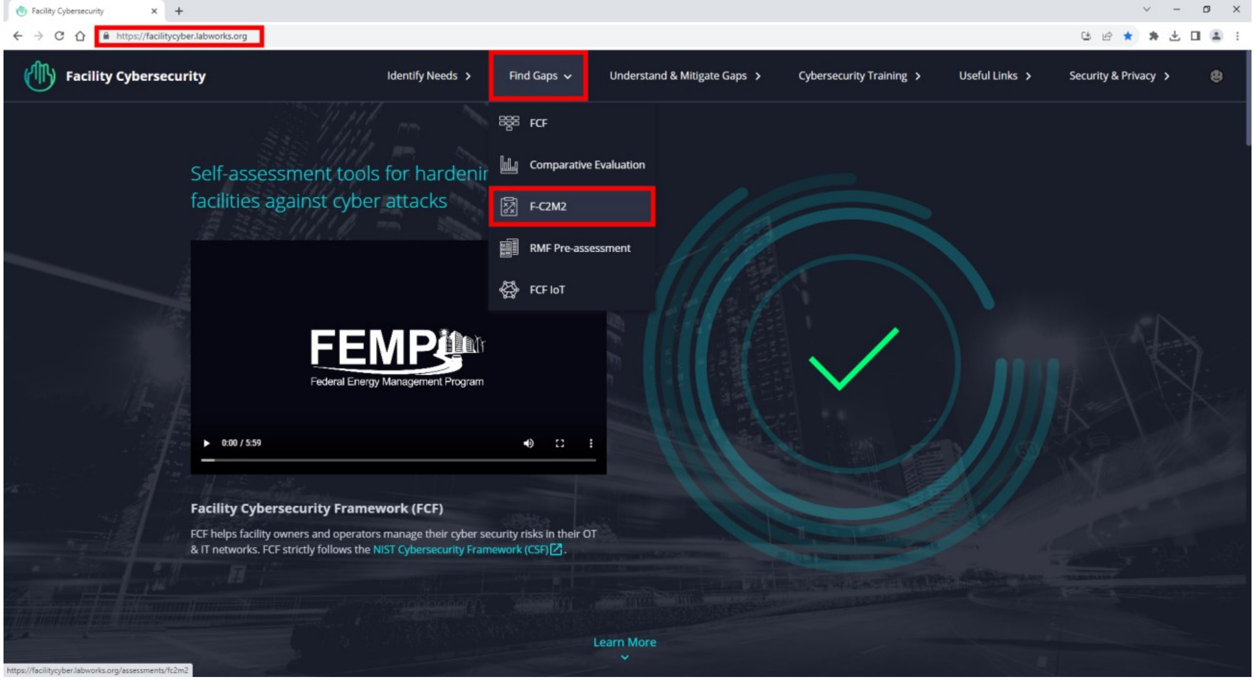
1.0 Introduction

The Facility Cybersecurity Capability Maturity Model (F-C2M2) assessment was designed to help facilities address their unique cybersecurity challenges. Building upon the foundational principles of the U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2), the F-C2M2 was explicitly tailored for federal facilities to help evaluate, benchmark, and enhance the cybersecurity capabilities of both their information technology (IT) and operational technology (OT) environments. This user guide was developed to facilitate a thorough understanding of the tool. Whether users are familiar with the original C2M2 or are new to the maturity model concept, this guide was designed to offer clarity, direction, and support.

2.0 Getting Started

To begin, open a web browser and enter the following URL: https://facilitycyber.labworks.org/. Upon arriving at the homepage, locate the “Find Gaps” tab. Click the tab, and a dropdown menu will appear. From this menu, select “F-C2M2” to access the tool as shown in **Figure 1**.

Tool Tip: *While using the F-C2M2 assessment tool, all user data entered will remain on the local cache of the workstation that the user is logged into. No information is transmitted to the server. Additionally, the information stored in the cache can be used across multiple tools hosted on the FCF website, and the data is not transmitted outside the user’s control. However, please exercise caution when clearing the cache, as this action will result in the deletion of any progress made within the tool. A local copy can be downloaded to save progress.*



Self-assessment tools for hardenir facilities against cyber attacks

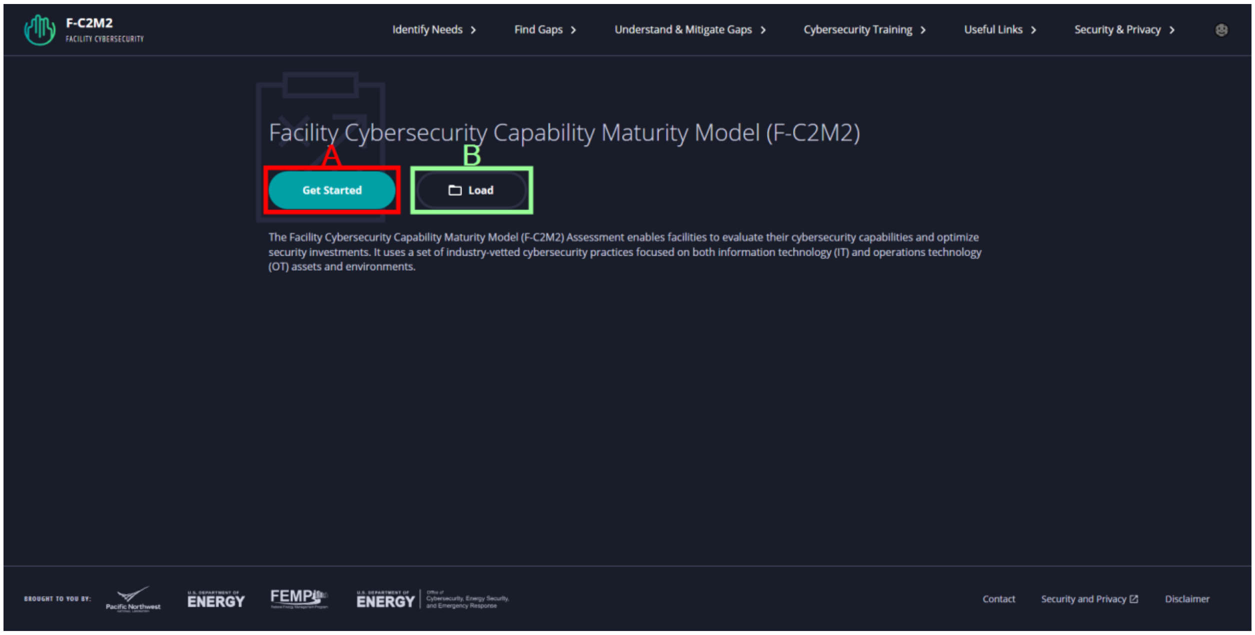
Facility Cybersecurity Framework (FCF)

FCF helps facility owners and operators manage their cyber security risks in their OT & IT networks. FCF strictly follows the NIST Cybersecurity Framework (CSF).

Figure 1: Navigating to the F-C2M2

2.1 New User

As a new user visiting the site for the first time and preparing to perform an assessment, the user will be presented with two distinct options for proceeding as shown in **Figure 2**.



Facility Cybersecurity Capability Maturity Model (F-C2M2)

The Facility Cybersecurity Capability Maturity Model (F-C2M2) Assessment enables facilities to evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

Figure 2: Getting Started – F-C2M2 Landing Page

A: Get Started – The user will begin a new assessment. Read the background text and when finished click “Get Started” to start the assessment.

B: Load – The user will have the option of loading a file from a previous assessment.

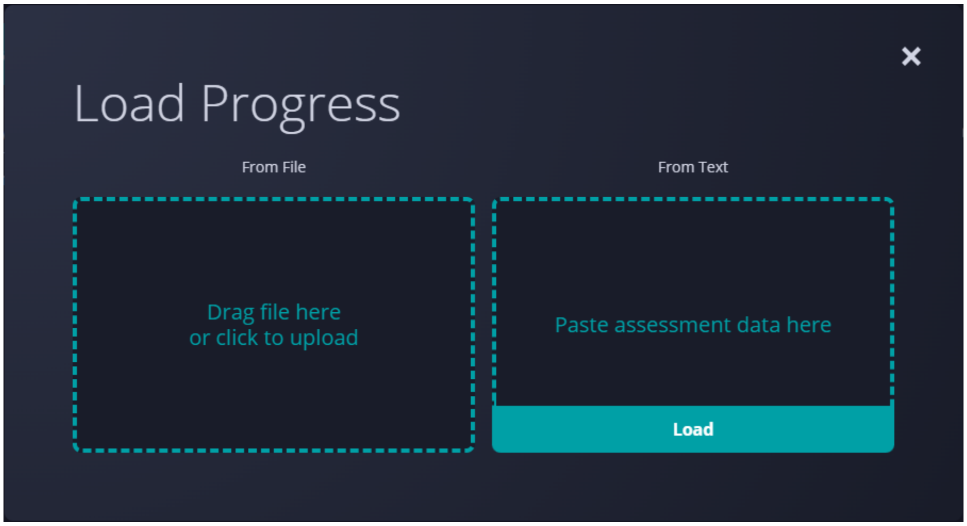


Figure 3: Load Options

If loading a prior session, click on the “Load” option. From here the user will have two methods to retrieve the session as shown in Error! Reference source not found.:

1. **From File:** Simply drag and drop the JSON file into the designated area or click on the section to browser and select the file to upload (**Figure 4**).

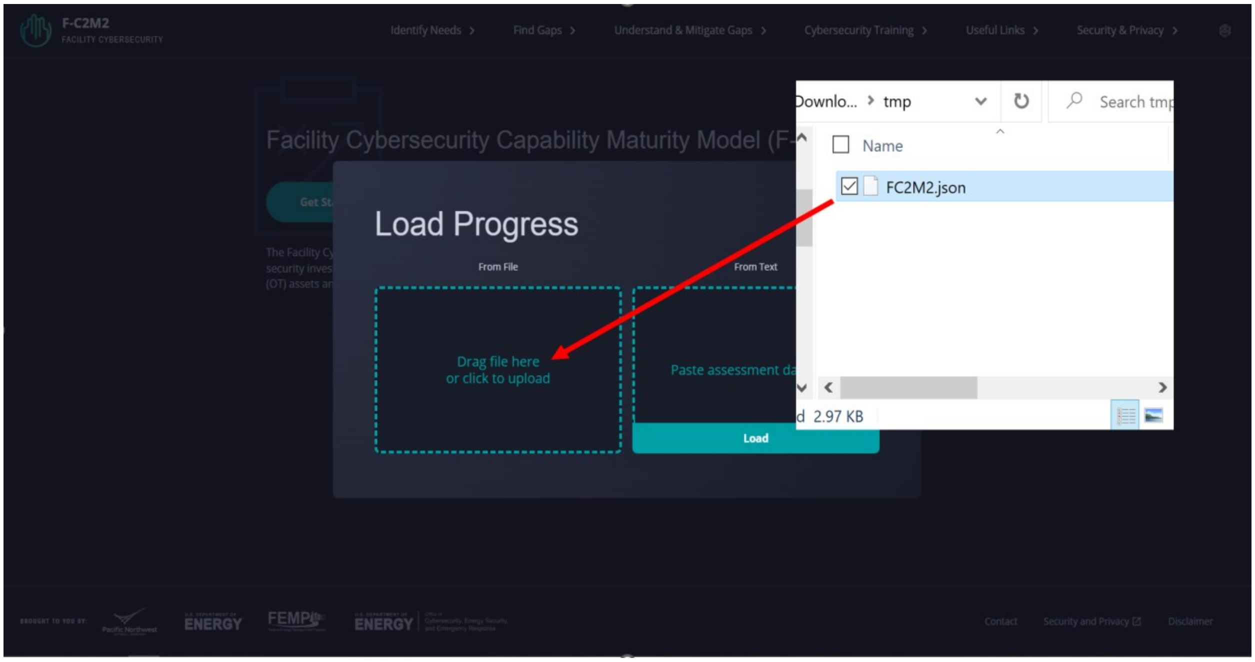
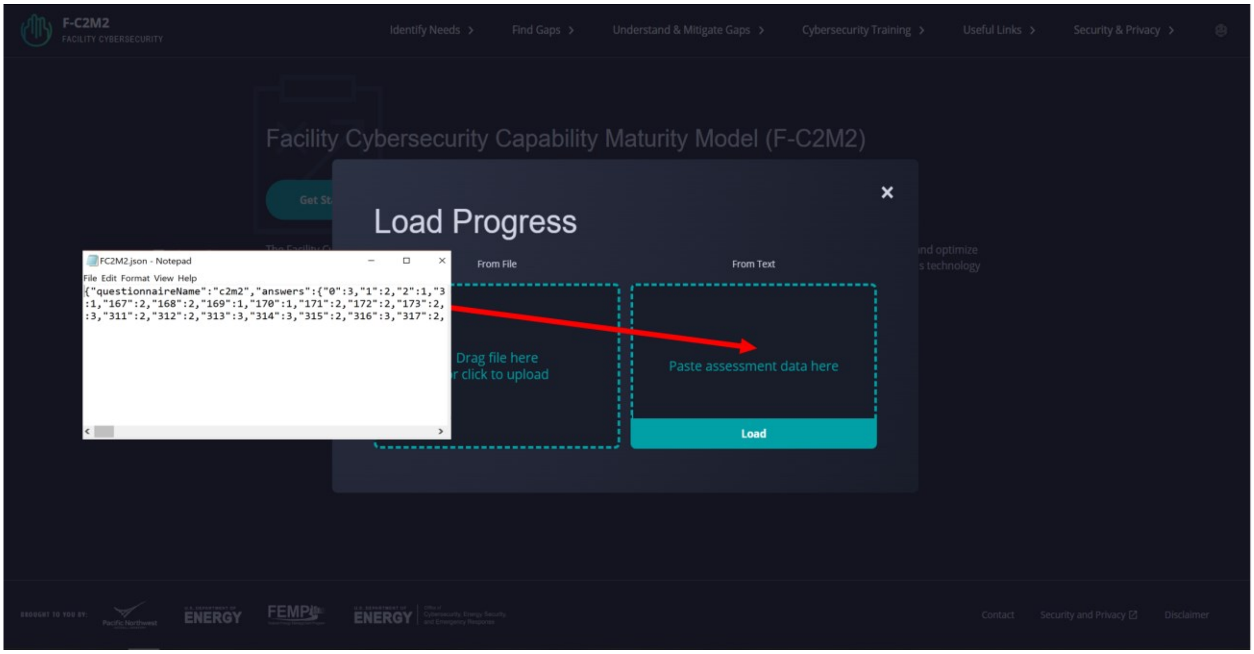


Figure 4: Load From File

2. **From Text:** The user can simply paste in the JSON format assessment data into the provided text box (**Figure 5**).

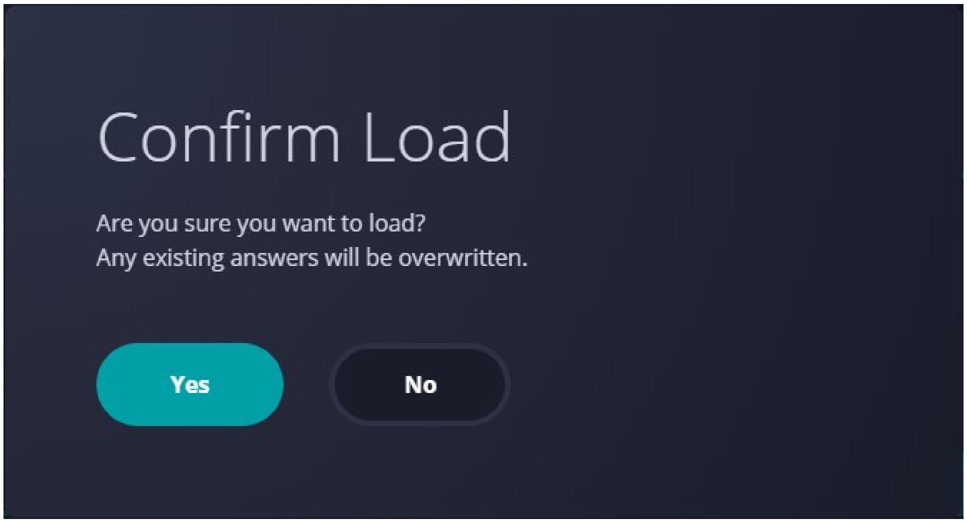
Tool Tip: *Please note that only JSON files are supported, and to ensure the correct display of past results, the user should use the “Save” button to produce a JSON file for loading. Otherwise, errors may occur.*



```
{"questionnaireName":"c2m2","answers":{"0":3,"1":2,"2":1,"3
:1,"167":2,"168":2,"169":1,"170":1,"171":2,"172":2,"173":2,
:3,"311":2,"312":2,"313":3,"314":3,"315":2,"316":3,"317":2,
```

Figure 5: Load From Text

A confirmation window will pop up, asking, “Are you sure you want to load? Any existing data will be overwritten.” If the user is certain about continuing, they would select “Yes.” A visual representation of this interaction can be found in **Figure 6**.

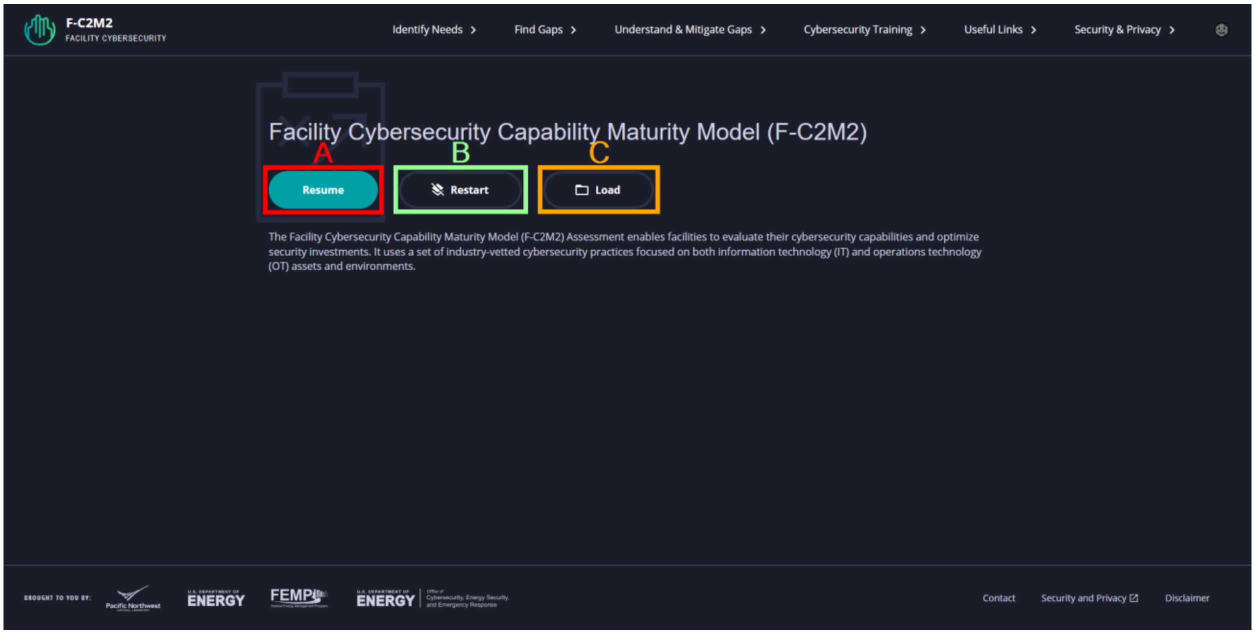

Confirm Load

Are you sure you want to load?
Any existing answers will be overwritten.

Figure 6: Confirmation Load Dialogue

2.2 Returning User

Returning to the site, the user will be presented with three options for proceeding as shown in **Figure 7**.



Facility Cybersecurity Capability Maturity Model (F-C2M2)

The Facility Cybersecurity Capability Maturity Model (F-C2M2) Assessment enables facilities to evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

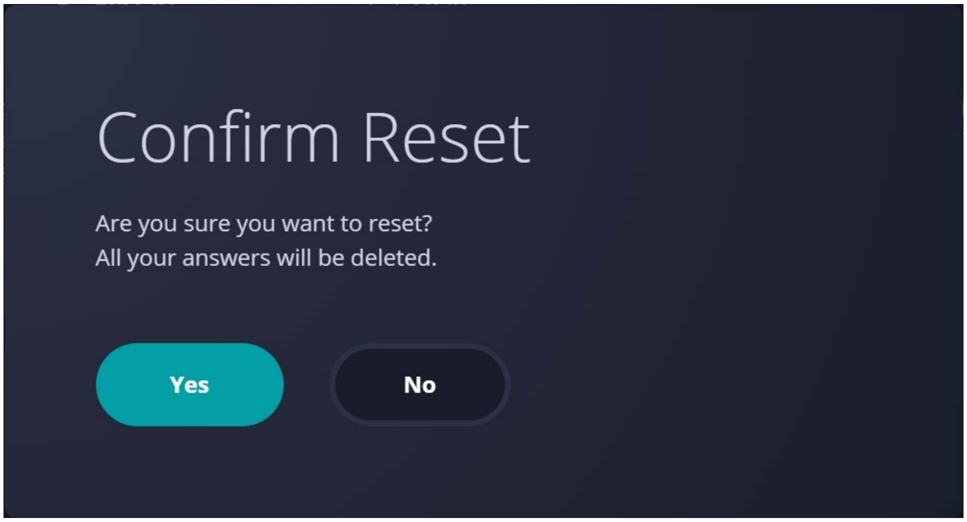
Figure 7: Returning User Options

A: Resume – Users are allowed to resume a session in progress that has been stored in their local cache.

B: Restart – Users will restart, and all prior data will be erased.

C: Load – Users will have the option of loading a file of a prior session in progress or completed report.

If restarting a session, click on the “Restart” option. The user will be prompted to confirm the reset and is notified of the loss of existing data as shown in **Figure 8**. After confirmation, the user will be redirected to the Getting Started – F-C2M2 Landing Page where they may start over.



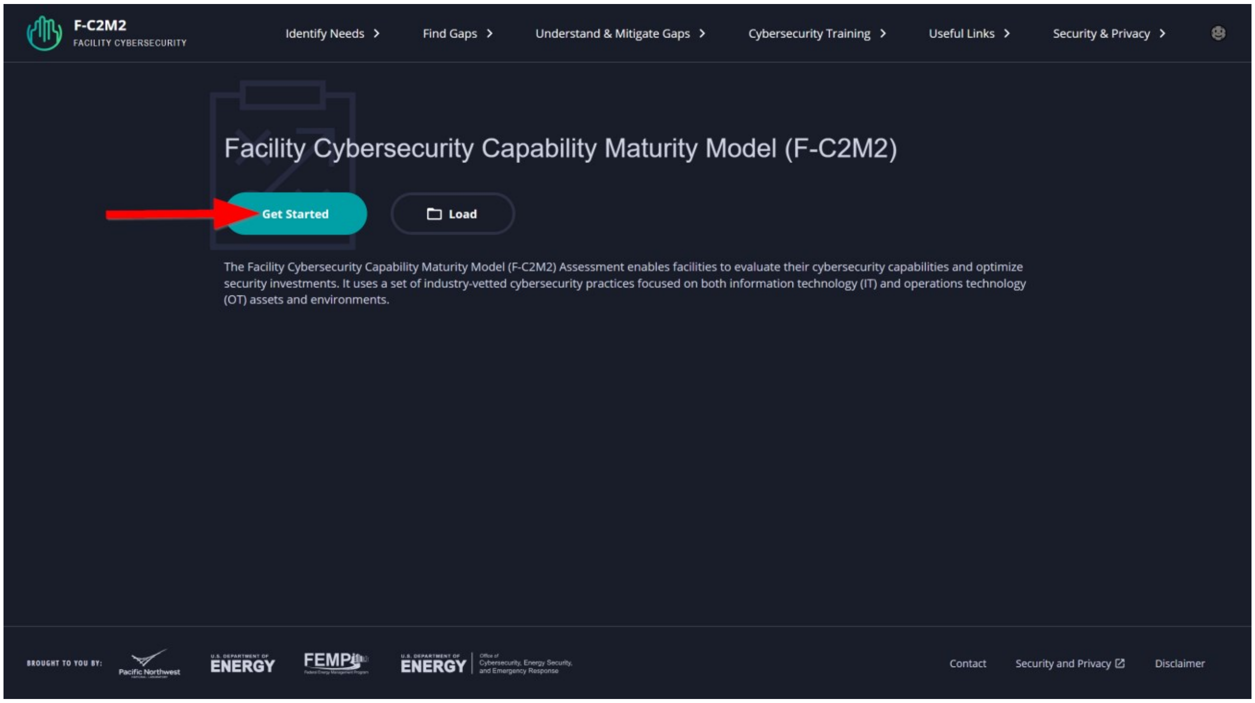
Confirm Reset

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

Figure 8: Confirmation Reset Option

2.3 Navigating the Assessment

When beginning, read the background text on the landing page to get familiarized with the F-C2M2 assessment tool. When finished, click “Get Started” (**Figure 9**).

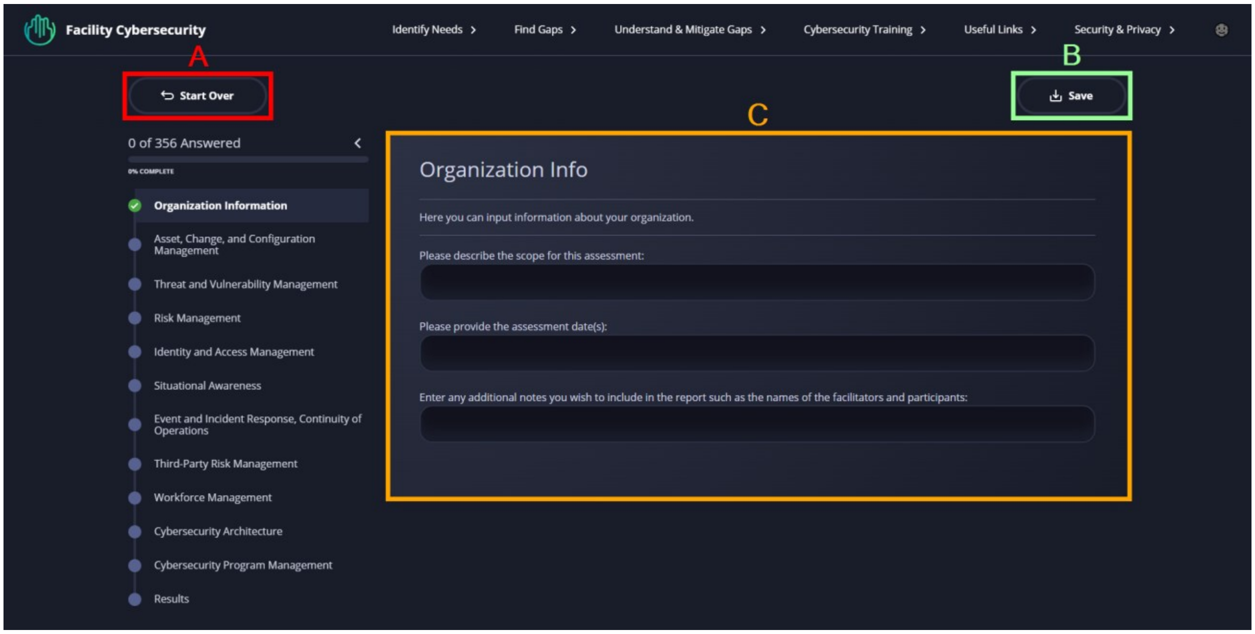


Facility Cybersecurity Capability Maturity Model (F-C2M2)

The Facility Cybersecurity Capability Maturity Model (F-C2M2) Assessment enables facilities to evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

Figure 9: Starting the Assessment

The user will have several options available and displayed on the page while performing the assessment (**Figure 10**).


Facility Cybersecurity
Identify Needs
Find Gaps
Understand & Mitigate Gaps
Cybersecurity Training
Useful Links
Security & Privacy
A
Start Over
B
Save
C
0 of 356 Answered
0% COMPLETE
Organization Information
Asset, Change, and Configuration Management
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
Results

Organization Info

Here you can input information about your organization.

Please describe the scope for this assessment:

Please provide the assessment date(s):

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

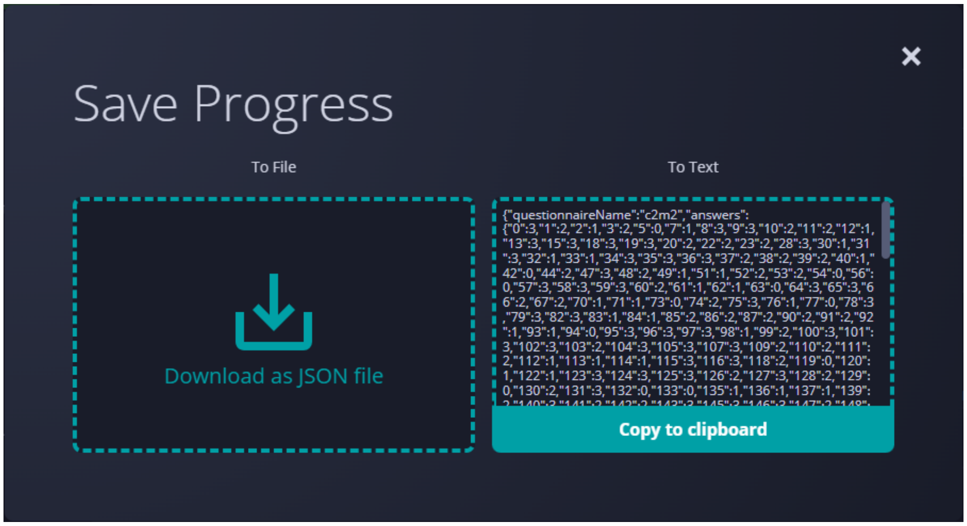
Figure 10: Navigation Options

A: Start Over – If users want to start over at any point, select this option. Please note if a user chooses to start over at any time during the assessment, all current data will be deleted.

B: Save – Choose this option to save a session in progress or a completed assessment. Clicking the Save button opens a save progress dialogue window (**Figure 11**) that gives the user the choice of downloading the current architecture as a JSON file extension or copying the raw JSON formatted text into the clipboard so the user can paste the JSON text into their choice of tools to read or save for future use.

C: Organization Info – The information entered here will be recorded in the report generated after the assessment is completed.

Tool Tip: *Since the organization information entered will be recorded in the report generated after completion, providing accurate and complete information on this page is recommended.*

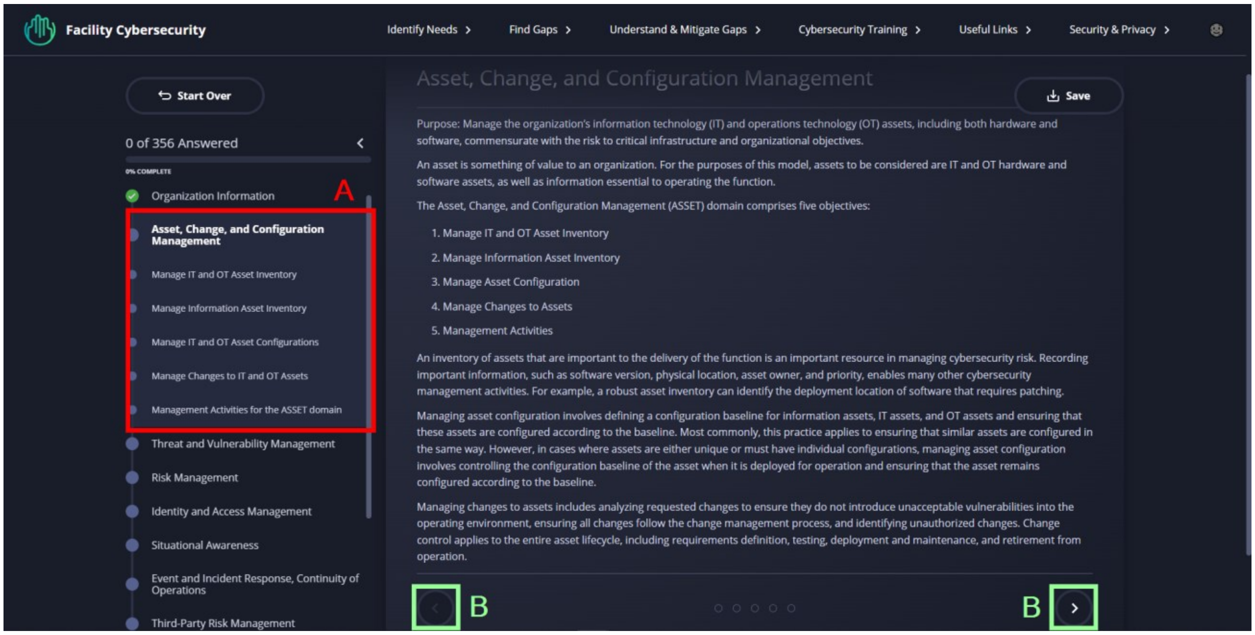


{"questionnaireName":"c2m2","answers":
{"0":3,"1":2,"2":1,"3":2,"5":0,"7":1,"8":3,"9":3,"10":2,"11":2,"12":1,
"13":3,"15":3,"18":3,"19":3,"20":2,"22":2,"23":2,"28":3,"30":1,"31
":3,"32":1,"33":1,"34":3,"35":3,"36":3,"37":2,"38":2,"39":2,"40":1,"
42":0,"44":2,"47":3,"48":2,"49":1,"51":1,"52":2,"53":2,"54":0,"56":
0,"57":3,"58":3,"59":3,"60":2,"61":1,"62":1,"63":0,"64":3,"65":3,"6
6":2,"67":2,"70":1,"71":1,"73":0,"74":2,"75":3,"76":1,"77":0,"78":3
,"79":3,"82":3,"83":1,"84":1,"85":2,"86":2,"87":2,"90":2,"91":2,"92
":1,"93":1,"94":0,"95":3,"96":3,"97":3,"98":1,"99":2,"100":3,"101":
3,"102":3,"103":2,"104":3,"105":3,"107":3,"109":2,"110":2,"111":
2,"112":1,"113":1,"114":1,"115":3,"116":3,"118":2,"119":0,"120":
1,"122":1,"123":3,"124":3,"125":3,"126":2,"127":3,"128":2,"129":
0,"130":2,"131":3,"132":0,"133":0,"135":1,"136":1,"137":1,"139":
2,"140":3,"141":2,"142":2,"143":3,"145":3,"146":3,"147":2,"148":

Figure 11: Save Options

2.4 Progressing Through the Assessment

Begin answering the assessment questions by clicking the first set of questions located in the left navigation menu or by using the Next button (**Figure 12**).


Facility Cybersecurity
Identify Needs
Find Gaps
Understand & Mitigate Gaps
Cybersecurity Training
Useful Links
Security & Privacy
Start Over
0 of 356 Answered
0% COMPLETE
Organization Information
A
Asset, Change, and Configuration Management
Manage IT and OT Asset Inventory
Manage Information Asset Inventory
Manage IT and OT Asset Configurations
Manage Changes to IT and OT Assets
Management Activities for the ASSET domain
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Save
B
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.

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.

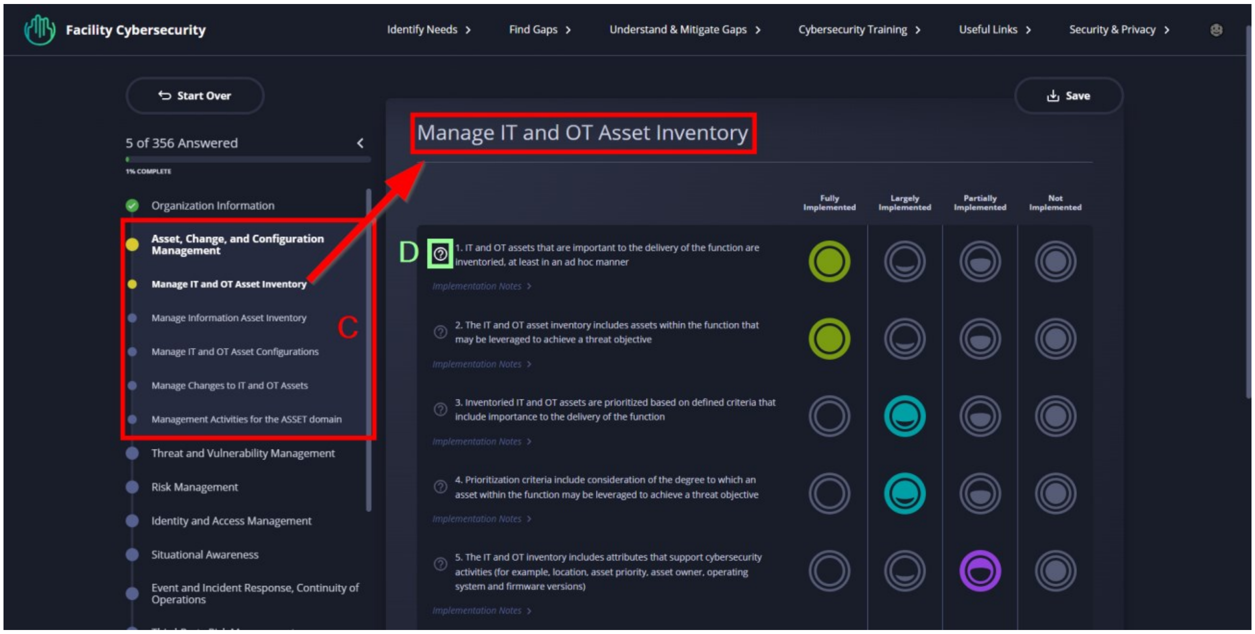
Managing changes to assets includes analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes. Change control applies to the entire asset lifecycle,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

Figure 12: Asset, Change, and Configuration Management Domain

A: Asset, Change, and Configuration Management Domain – When landing on each domain, users are presented with a comprehensive overview of that specific domain and its importance. Users will also find definitions and the objectives pertaining to that domain. Each objective is then elaborated upon, serving as a guide, and preparing users for the assessment questions that follow.

B: Back and Next Buttons – When all questions on the current page have been answered, clicking the next button will take users to the subsequent set of questions for either a given objective or domain. Users may also click the back button to visit previously answered questions as users progress through the assessment.

When beginning the first set of questions, users will see the following displayed in **Figure 13**.



- Organization Information
- Asset, Change, and Configuration Management
- Manage IT and OT Asset Inventory
- Manage Information Asset Inventory
- Manage IT and OT Asset Configurations
- Manage Changes to IT and OT Assets
- Management Activities for the ASSET domain
- Threat and Vulnerability Management
- Risk Management
- Identity and Access Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations

Manage IT and OT Asset Inventory

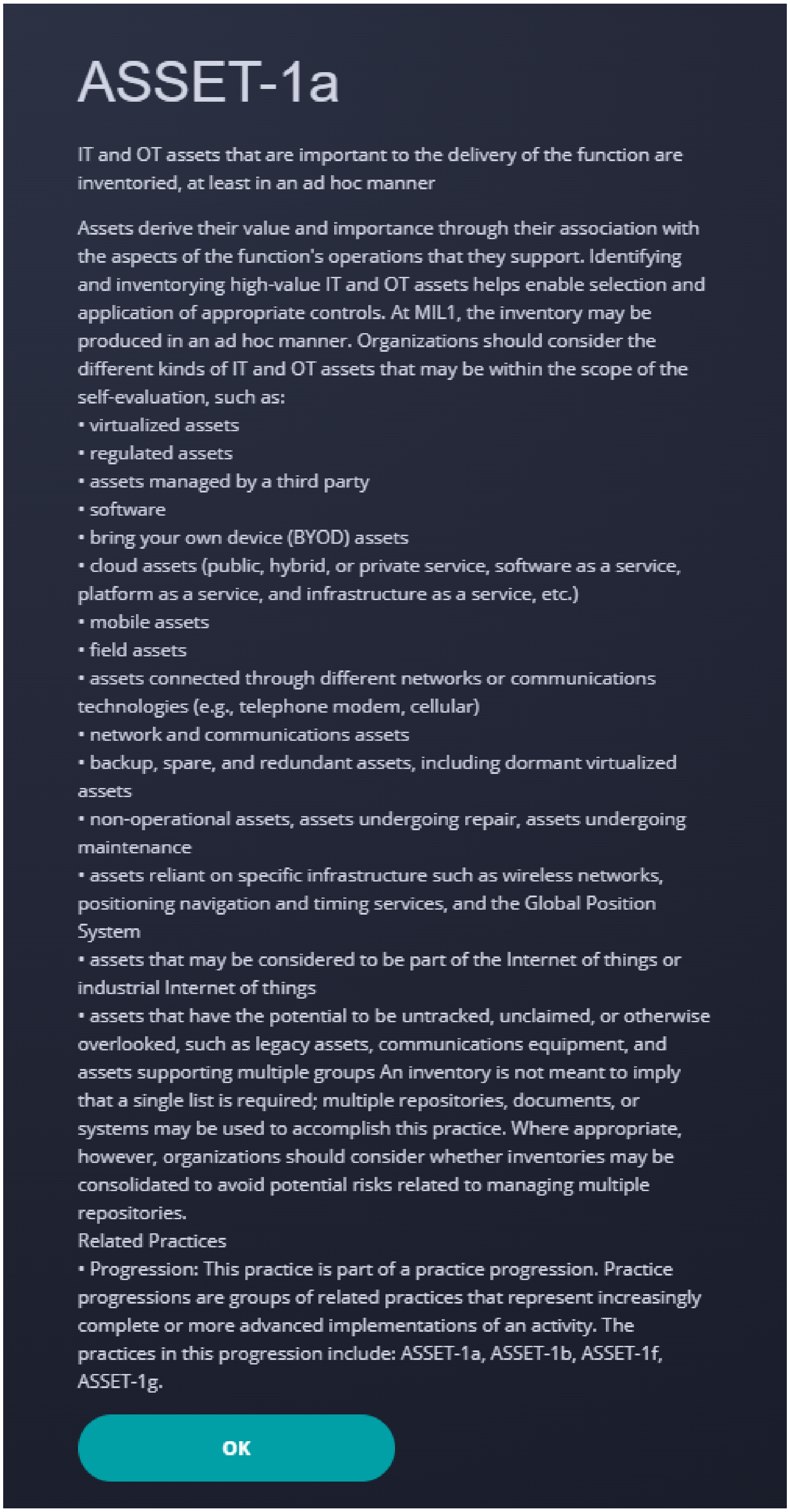
	Fully Implemented	Largely Implemented	Partially Implemented	Not Implemented
1. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner Implementation Notes >	●	○	○	○
2. The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective Implementation Notes >	●	○	○	○
3. Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function Implementation Notes >	○	●	○	○
4. Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective Implementation Notes >	○	●	○	○
5. The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions) Implementation Notes >	○	○	●	○

Figure 13: Objective 1 – Manage IT and OT Asset Inventory

C: Objective 1 Questions – This is the first set of questions users will begin to answer that pertain to Objective 1 (Manage IT and OT Asset Inventory) of the Asset, Change, and Configuration Management Domain.

D: Help Text (“?”) Button – If users need additional guidance, click this button located to the left of each question.

When clicking on the "?" button, a pop-up window will display text describing the given question in more depth and providing guidance related to the practice. The help text will also highlight related practices users will encounter as they progress through the assessment (**Figure 14**).



ASSET-1a

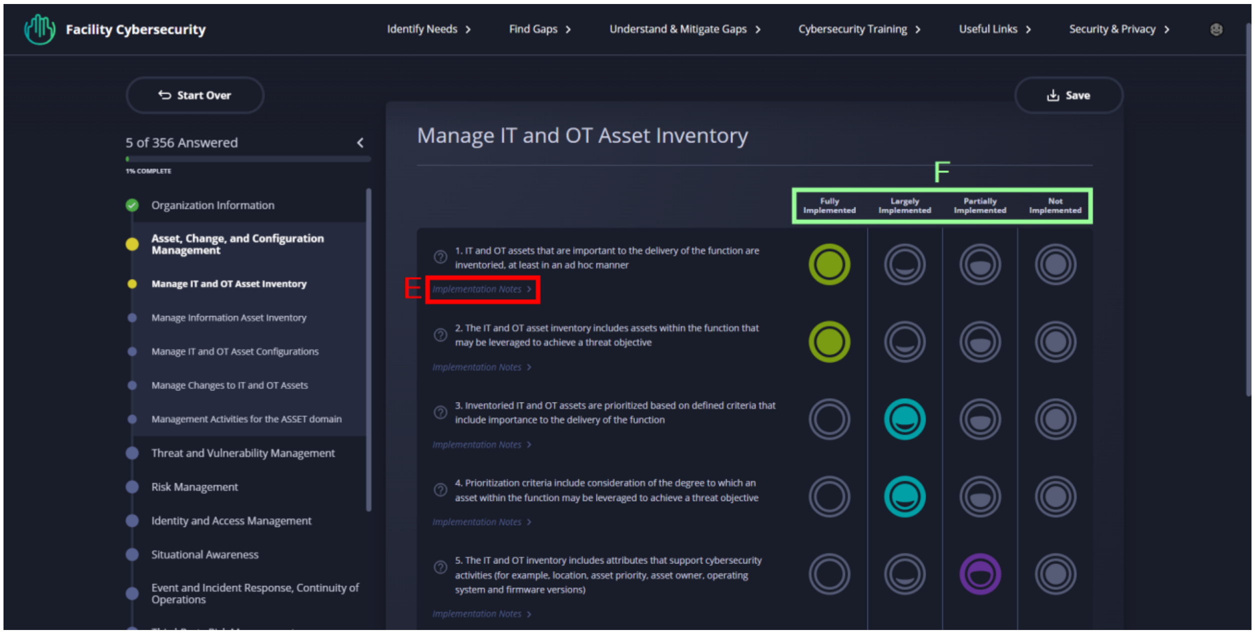
IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner

Assets derive their value and importance through their association with the aspects of the function's operations that they support. Identifying and inventorying high-value IT and OT assets helps enable selection and application of appropriate controls. At MIL1, the inventory may be produced in an ad hoc manner. Organizations should consider the different kinds of IT and OT assets that may be within the scope of the self-evaluation, such as:
- virtualized assets
- regulated assets
- assets managed by a third party
- software
- bring your own device (BYOD) assets
- cloud assets (public, hybrid, or private service, software as a service, platform as a service, and infrastructure as a service, etc.)
- mobile assets
- field assets
- assets connected through different networks or communications technologies (e.g., telephone modem, cellular)
- network and communications assets
- backup, spare, and redundant assets, including dormant virtualized assets
- non-operational assets, assets undergoing repair, assets undergoing maintenance
- assets reliant on specific infrastructure such as wireless networks, positioning navigation and timing services, and the Global Position System
- assets that may be considered to be part of the Internet of things or industrial Internet of things
- assets that have the potential to be untracked, unclaimed, or otherwise overlooked, such as legacy assets, communications equipment, and assets supporting multiple groups An inventory is not meant to imply that a single list is required; multiple repositories, documents, or systems may be used to accomplish this practice. Where appropriate, however, organizations should consider whether inventories may be consolidated to avoid potential risks related to managing multiple repositories.

Related Practices
- Progression: This practice is part of a practice progression. Practice progressions are groups of related practices that represent increasingly complete or more advanced implementations of an activity. The practices in this progression include: ASSET-1a, ASSET-1b, ASSET-1f, ASSET-1g.

Figure 14: Example of the Help Text Display

During the assessment, in relation to each question, users will be able to do the following (**Figure 15**):


Facility Cybersecurity
Identify Needs >
Find Gaps >
Understand & Mitigate Gaps >
Cybersecurity Training >
Useful Links >
Security & Privacy >
Start Over
Save
5 of 356 Answered
1% COMPLETE
Organization Information
Asset, Change, and Configuration Management
Manage IT and OT Asset Inventory
Manage Information Asset Inventory
Manage IT and OT Asset Configurations
Manage Changes to IT and OT Assets
Management Activities for the ASSET domain
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
F
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented
E
Implementation Notes >

Manage IT and OT Asset Inventory

1. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner

2. The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective

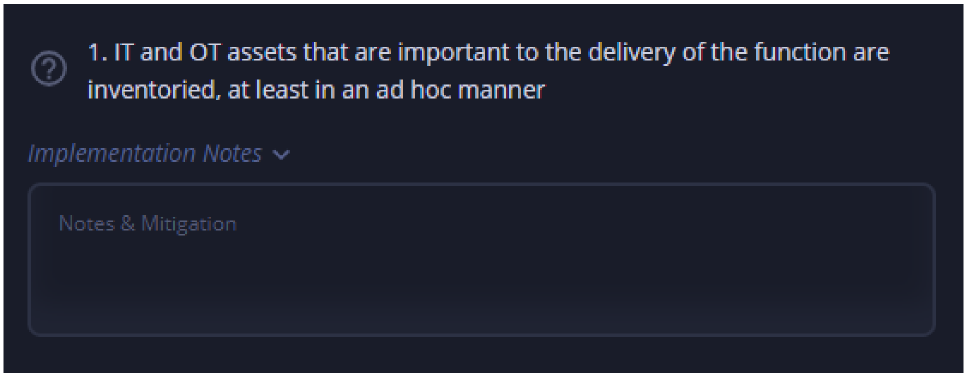
3. Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function

4. Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective

5. The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions)

Figure 15: Implementation Notes and Levels

E: Implementation Notes – When navigating the assessment section, users will encounter questions with an accompanying "Implementation Notes" text box beneath each. This allows users to type any thoughts or additional information about the question (**Figure 16**).



1. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner

Figure 16: Implementation Notes

F: Implementation Levels – While answering a given question, users will be presented with four options representing different levels of implementation, as shown in **Figure 17**.

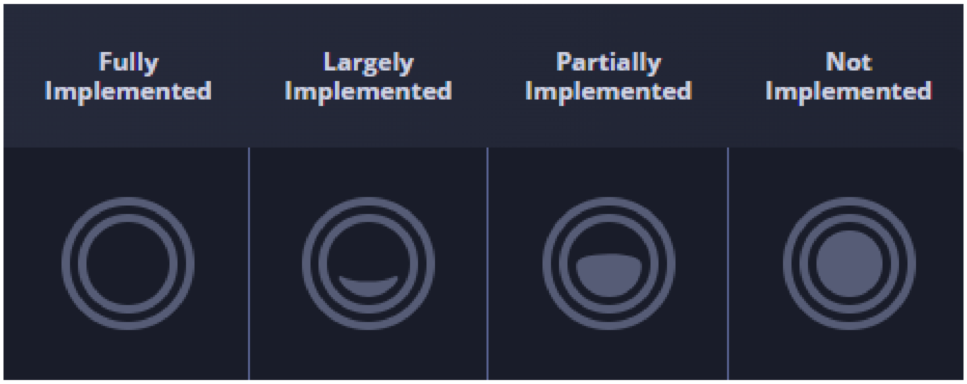
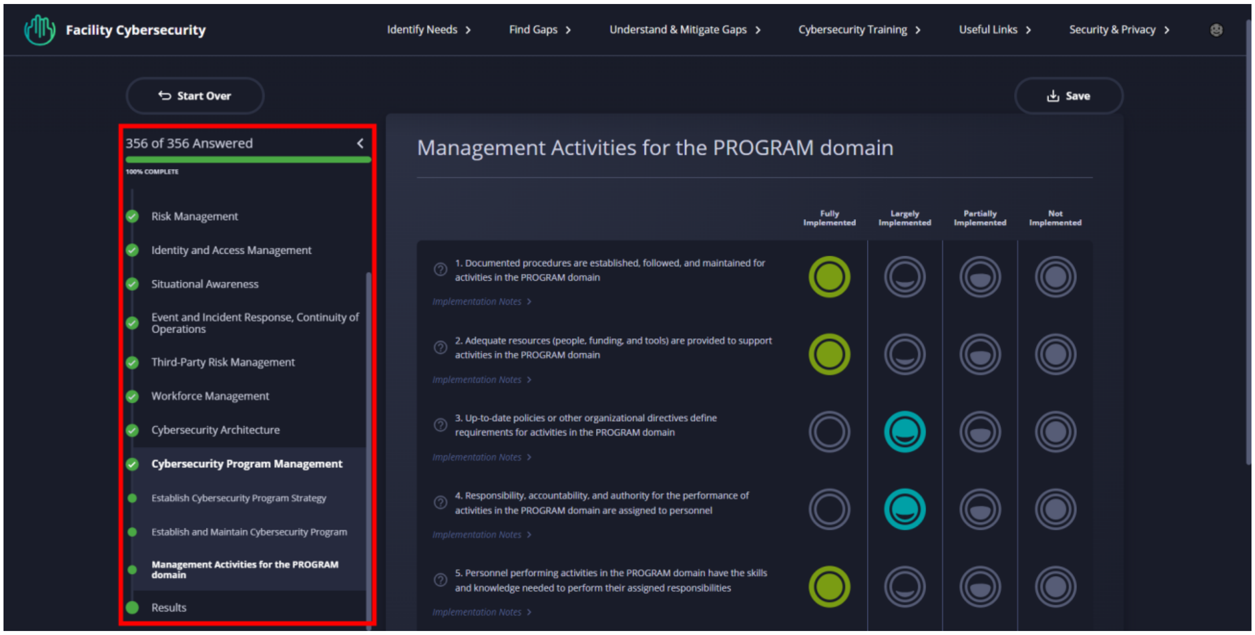


Figure 17: Implementation Levels

Tool Tip: *Notes allow users to jot down reflections, references, or insights related to each question. The implementation levels help categorize user responses based on the current state of the feature or process in a system. Choose the one that best fits.*

When finished reviewing, click the “OK” button to exit out of the pop-up window and resume the assessment.



356 of 356 Answered

100% COMPLETE

- ✓ Risk Management
- ✓ Identity and Access Management
- ✓ Situational Awareness
- ✓ Event and Incident Response, Continuity of Operations
- ✓ Third-Party Risk Management
- ✓ Workforce Management
- ✓ Cybersecurity Architecture
- ✓ **Cybersecurity Program Management**
- Establish Cybersecurity Program Strategy
- Establish and Maintain Cybersecurity Program
- **Management Activities for the PROGRAM domain**
- Results

Management Activities for the PROGRAM domain

	Fully Implemented	Largely Implemented	Partially Implemented	Not Implemented
1. Documented procedures are established, followed, and maintained for activities in the PROGRAM domain Implementation Notes >	●	○	○	○
2. Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain Implementation Notes >	●	○	○	○
3. Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain Implementation Notes >	○	●	○	○
4. Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel Implementation Notes >	○	●	○	○
5. Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities Implementation Notes >	●	○	○	○

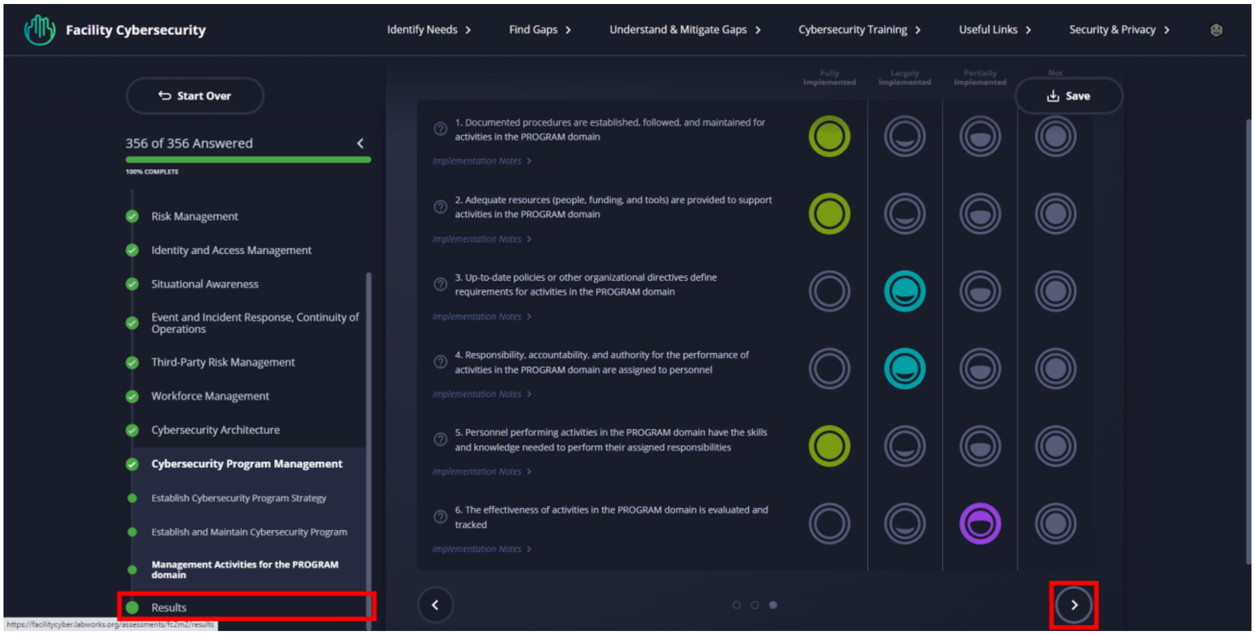
Figure 18: Completed Assessment

Upon completion of all domains, every segment of the navigation menu will be marked with green circles and a check mark, indicating that 356 of 356 questions have been answered – this represents 100% completion (**Figure 18**).

Tool Tip: *This would be a good time to save the progress in the top right-hand corner by clicking on the “Save” button.*

2.5 Report Generation

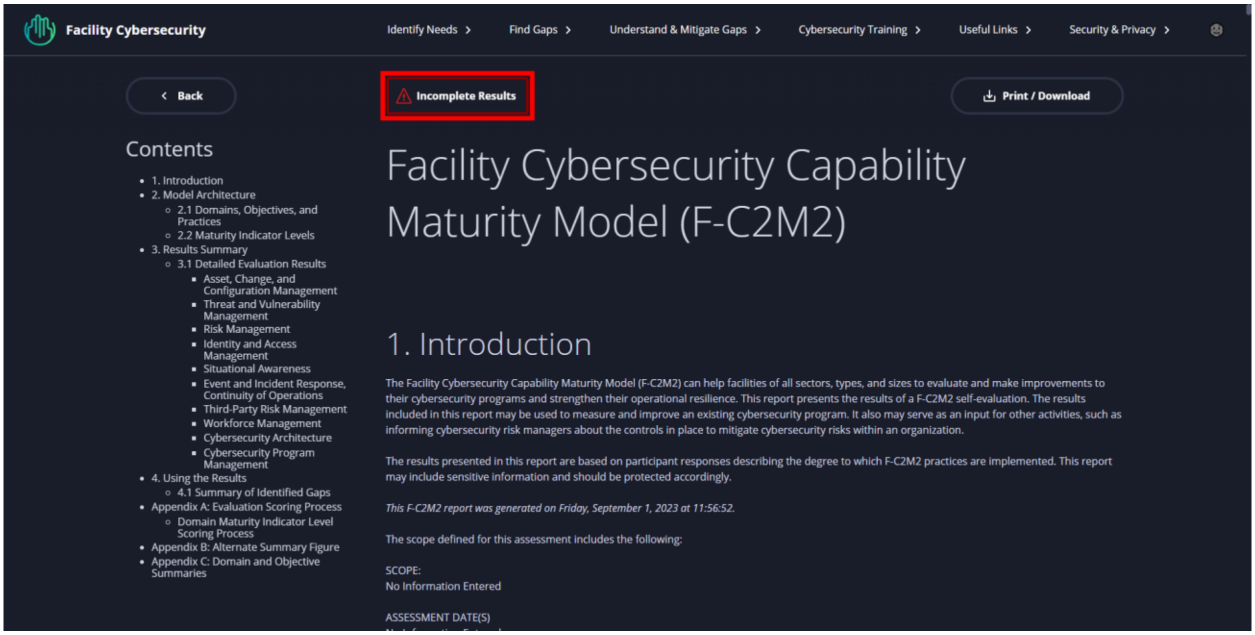
To view the report, simply click on the “Results” at the bottom left corner of the navigation menu or click the next button after completing the questions of the last objective, Management Activities, pertaining to the Cybersecurity Program Management domain (**Figure 19**).


Facility Cybersecurity
Identify Needs >
Find Gaps >
Understand & Mitigate Gaps >
Cybersecurity Training >
Useful Links >
Security & Privacy >
Start Over
356 of 356 Answered
100% COMPLETE
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
Establish Cybersecurity Program Strategy
Establish and Maintain Cybersecurity Program
Management Activities for the PROGRAM domain
Results
https://facilitycyber.labworks.org/assessments/fc2m2/results
Fully Implemented
Largely Implemented
Partially Implemented
Not
Save
Implementation Notes >

1. Documented procedures are established, followed, and maintained for activities in the PROGRAM domain
2. Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain
3. Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain
4. Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel
5. Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities
6. The effectiveness of activities in the PROGRAM domain is evaluated and tracked

Figure 19: Results

However, if the assessment isn’t complete, users will see a message indicating “Incomplete Results” as shown in **Figure 20**. The incomplete section of the report will also remain blank.



Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

Facility Cybersecurity Capability Maturity Model (F-C2M2)

1. Introduction

The Facility Cybersecurity Capability Maturity Model (F-C2M2) can help facilities of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. This report presents the results of a F-C2M2 self-evaluation. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization.

The results presented in this report are based on participant responses describing the degree to which F-C2M2 practices are implemented. This report may include sensitive information and should be protected accordingly.

This F-C2M2 report was generated on Friday, September 1, 2023 at 11:56:52.

The scope defined for this assessment includes the following:

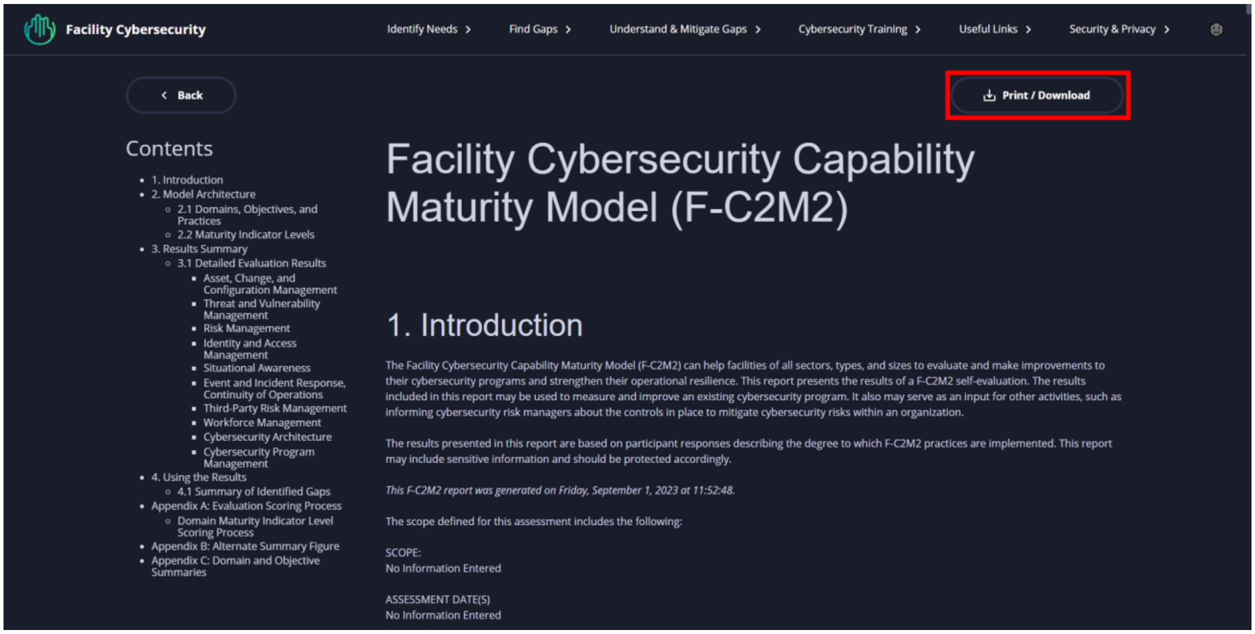
SCOPE:
No Information Entered

ASSESSMENT DATE(S)

Figure 20: Incomplete Results

Print/Download Report

The F-C2M2 offers the functionality to print or download reports. By clicking the “Print/Download” button located in the upper right corner of the report (**Figure 21**), a print option screen will appear.



Contents

Facility Cybersecurity Capability Maturity Model (F-C2M2)

1. Introduction

The Facility Cybersecurity Capability Maturity Model (F-C2M2) can help facilities of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. This report presents the results of a F-C2M2 self-evaluation. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization.

The results presented in this report are based on participant responses describing the degree to which F-C2M2 practices are implemented. This report may include sensitive information and should be protected accordingly.

This F-C2M2 report was generated on Friday, September 1, 2023 at 11:52:48.

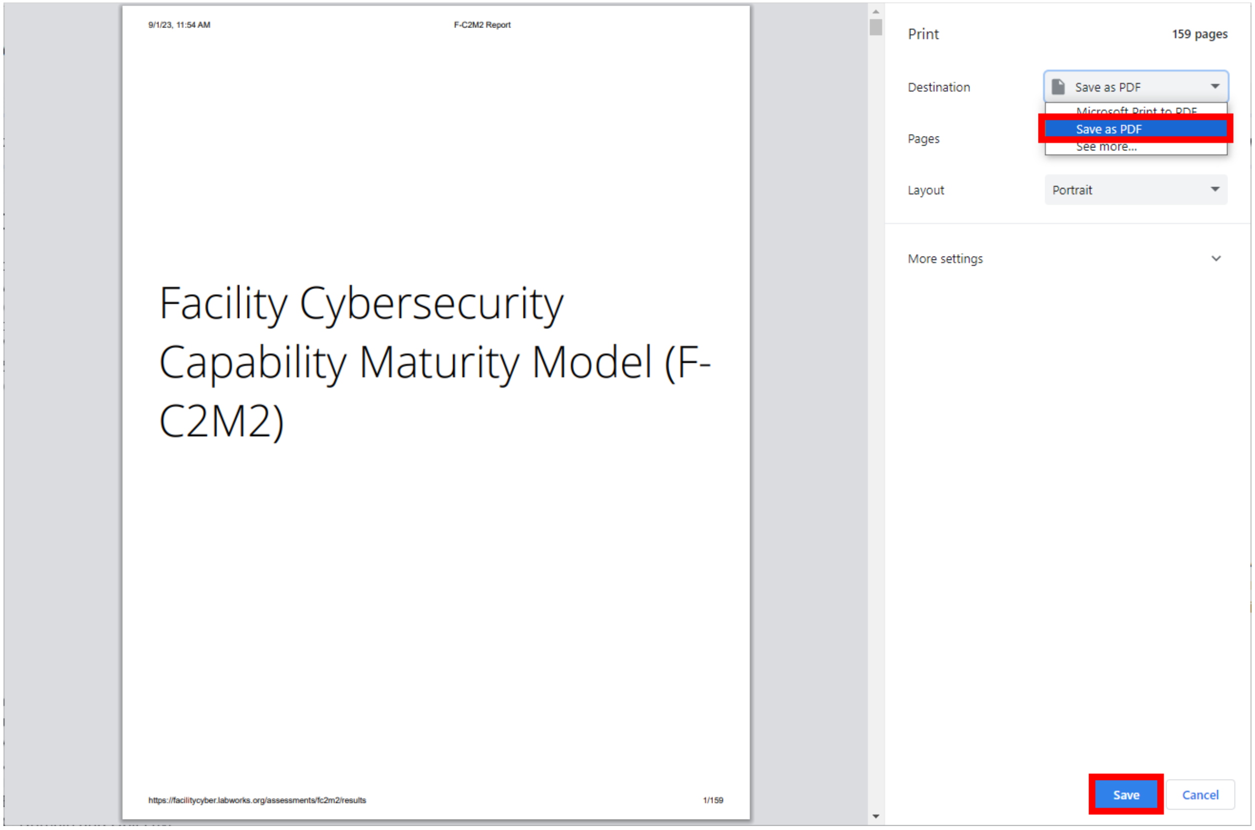
The scope defined for this assessment includes the following:

SCOPE:
No Information Entered

ASSESSMENT DATE(S)
No Information Entered

Figure 21: Print/Download Button

At this point users can choose to generate a PDF or proceed with actual printing as shown in **Figure 22**.



9/1/23, 11:54 AM F-C2M2 Report

Facility Cybersecurity Capability Maturity Model (F-C2M2)

https://facilitycyber.labworks.org/assessments/fc2m2/results 1/159

Print 159 pages

Destination: Save as PDF

Layout: Portrait

Figure 22: PDF Report

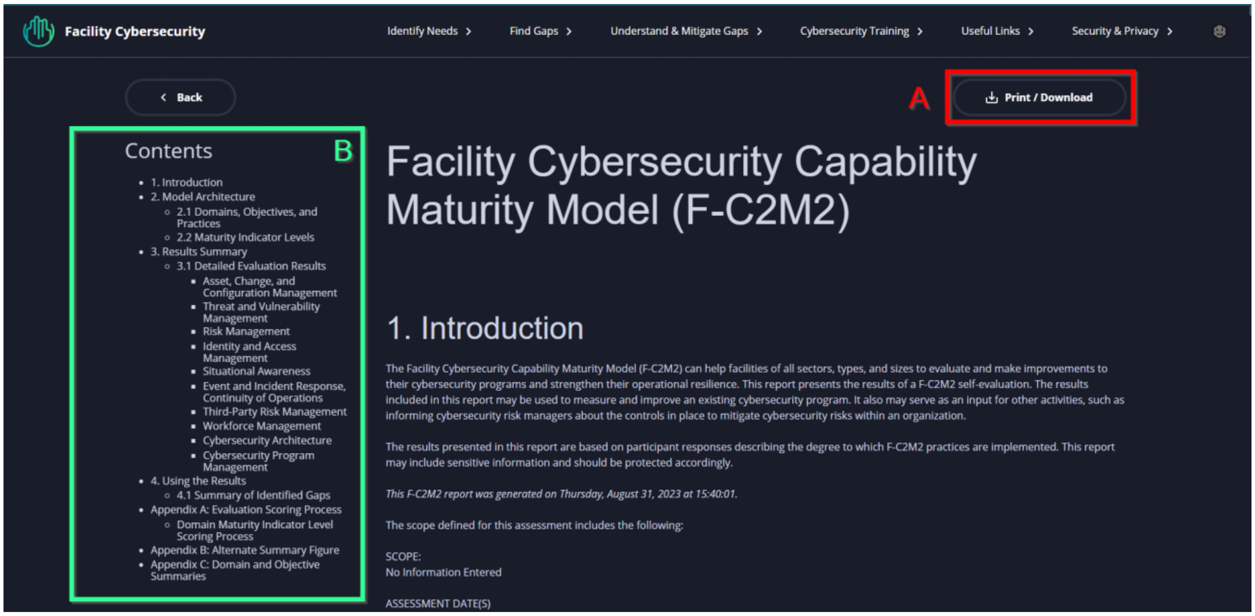
3.0 Interpreting F-C2M2 Assessment Report

Introduction and Model Architecture – Report Sections 1 and 2

Once users have successfully completed the F-C2M2 self-assessment, when clicking on the results section users will be taken to the introduction of the report. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization. The results presented in this report are based on participant responses describing the degree to which F-C2M2 practices are implemented within their facility. This report may include sensitive information and should be protected accordingly.

Save the report by clicking the "Print / Download" button in **Figure 23**, exhibit A.

The "Contents" section of the navigation pane exhibit B provide clickable headings for sections and subsections of the report for efficient report navigation.



Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

Facility Cybersecurity Capability Maturity Model (F-C2M2)

1. Introduction

The Facility Cybersecurity Capability Maturity Model (F-C2M2) can help facilities of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. This report presents the results of a F-C2M2 self-evaluation. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization.

The results presented in this report are based on participant responses describing the degree to which F-C2M2 practices are implemented. This report may include sensitive information and should be protected accordingly.

This F-C2M2 report was generated on Thursday, August 31, 2023 at 15:40:01.

The scope defined for this assessment includes the following:

SCOPE:
No Information Entered

ASSESSMENT DATE(S)

Figure 23: Report Introduction

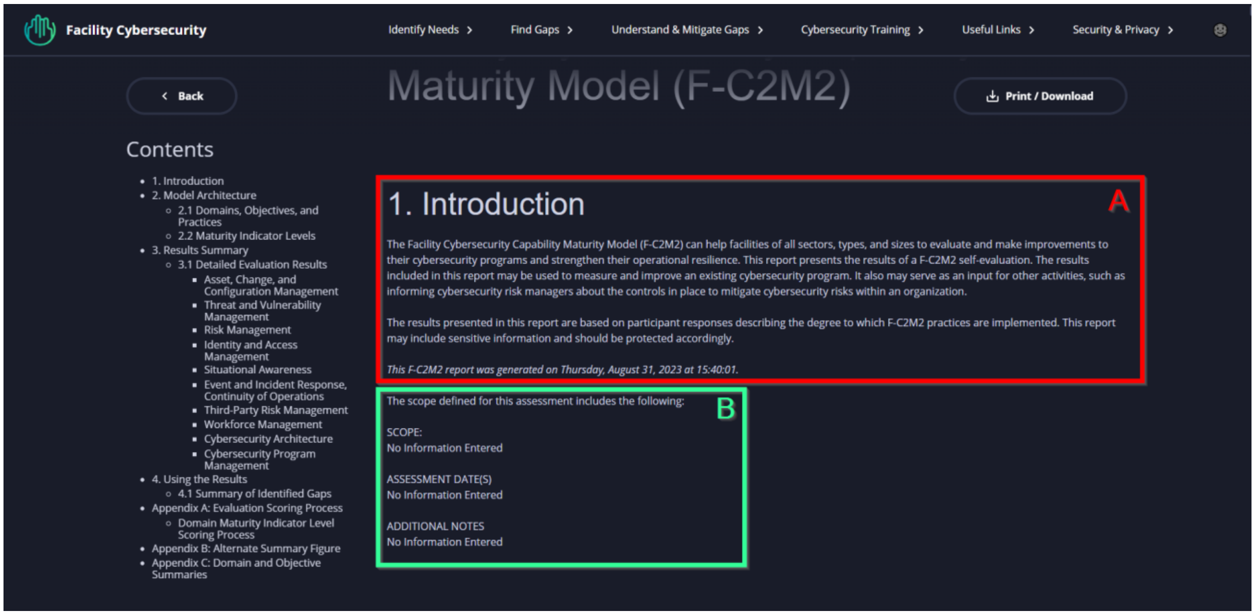
The key sections of the report are:

1. Introduction
2. Model Architecture
   - 2.1 Domains, Objectives, and Practices
   - 2.2 Maturity Indicator Levels
3. Results Summary
   - 3.1 Detailed Evaluation Results
     - Asset, Change, and Configuration Management
     - Threat and Vulnerability Management
     - Risk Management
     - Identity and Access Management
     - Situational Awareness
     - Event and Incident Response, Continuity of Operations

        - Third-Party Risk Management
        - Workforce Management
        - Cybersecurity Architecture
        - Cybersecurity Program Management

4. Using the Results
    - 4.1 Summary of Identified Gaps
        - Appendix A: Evaluation Scoring Process
        - Domain Maturity Indicator Level Scoring Process
        - Appendix B: Alternate Summary Figure
        - Appendix C: Domain and Objective Summaries

Section 1 Introduces The Facility Cybersecurity Capability Maturity Model (F-C2M2) and educates users on how this evaluation can help facilities of all sectors, types, and sizes evaluate and strengthen their operational resilience and cybersecurity programs (**Figure 24**, exhibit A)**.** Exhibit B contains the scope that was initially defined at the beginning of the assessment. It will reflect the Scope, Assessment Date(s) and any additional notes entered**.**



Maturity Model (F-C2M2)

Contents

- 1. Introduction
- 2. Model Architecture
    - 2.1 Domains, Objectives, and Practices
    - 2.2 Maturity Indicator Levels
- 3. Results Summary
    - 3.1 Detailed Evaluation Results
        - Asset, Change, and Configuration Management
        - Threat and Vulnerability Management
        - Risk Management
        - Identity and Access Management
        - Situational Awareness
        - Event and Incident Response, Continuity of Operations
        - Third-Party Risk Management
        - Workforce Management
        - Cybersecurity Architecture
        - Cybersecurity Program Management
- 4. Using the Results
    - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
    - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

1. Introduction

The Facility Cybersecurity Capability Maturity Model (F-C2M2) can help facilities of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. This report presents the results of a F-C2M2 self-evaluation. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization.

The results presented in this report are based on participant responses describing the degree to which F-C2M2 practices are implemented. This report may include sensitive information and should be protected accordingly.

This F-C2M2 report was generated on Thursday, August 31, 2023 at 15:40:01.

The scope defined for this assessment includes the following:

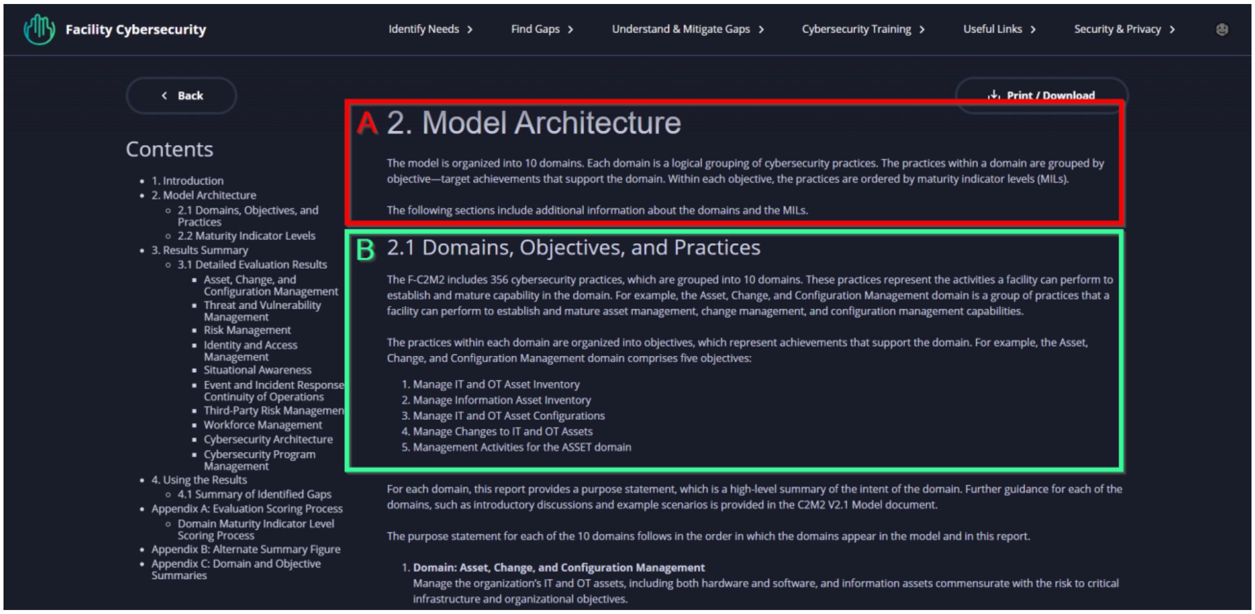
SCOPE:
No Information Entered

ASSESSMENT DATE(S)
No Information Entered

ADDITIONAL NOTES
No Information Entered

Figure 24: Introduction

The Model Architecture Section (Section 2) **Figure 25**, exhibit A defines how the model is organized into 10 domains. Each domain contains objectives and practices that are target achievements that support the domain. Within each objective, the practices are ordered by maturity indicator levels (MILs) which are explained in section 2.2.



Contents

2. Model Architecture

The model is organized into 10 domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective—target achievements that support the domain. Within each objective, the practices are ordered by maturity indicator levels (MILs).

The following sections include additional information about the domains and the MILs.

2.1 Domains, Objectives, and Practices

The F-C2M2 includes 356 cybersecurity practices, which are grouped into 10 domains. These practices represent the activities a facility can perform to establish and mature capability in the domain. For example, the Asset, Change, and Configuration Management domain is a group of practices that a facility can perform to establish and mature asset management, change management, and configuration management capabilities.

The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Asset, Change, and Configuration Management domain comprises five objectives:

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage IT and OT Asset Configurations
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

For each domain, this report provides a purpose statement, which is a high-level summary of the intent of the domain. Further guidance for each of the domains, such as introductory discussions and example scenarios is provided in the C2M2 V2.1 Model document.

The purpose statement for each of the 10 domains follows in the order in which the domains appear in the model and in this report.

1. **Domain: Asset, Change, and Configuration Management**
   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 25: Model Architecture and Domains, Objectives, and Practices

Domains, Objectives, and Practices (Section 2.1**) Figure 25** exhibit B: The F-C2M2 includes 356 cybersecurity practices that are grouped into 10 domains. These practices represent the activities a facility can perform to establish a mature capability in each domain. For example, the Asset, Change, and Configuration Management domain are a group of practices that a facility can perform to establish mature asset management, change management, and configuration management capabilities. The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Asset, Change, and Configuration Management domain contain five objectives:

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage IT and OT Asset Configurations
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

A purpose statement is provided for each domain, which is a high-level summary of the intent of the domain. Further guidance for each of the domains, such as introductory discussions and example scenarios are provided in the C2M2 V2.1 Model document.

The purpose statement for each of the 10 domains follows the order in which the domains appear in the model and in this report.

Domain: Asset, Change, and Configuration Management
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.

Domain: Threat and Vulnerability Management
Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to

the organization’s infrastructure (such as critical, IT, and operational) and organizational objectives.

Domain: Risk Management
Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Domain: Identity and Access Management
Create and manage identities for entities that may be granted logical or physical access to the organization’s assets. Control access to the organization’s assets, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Situational Awareness
Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization’s operational state and cybersecurity state.

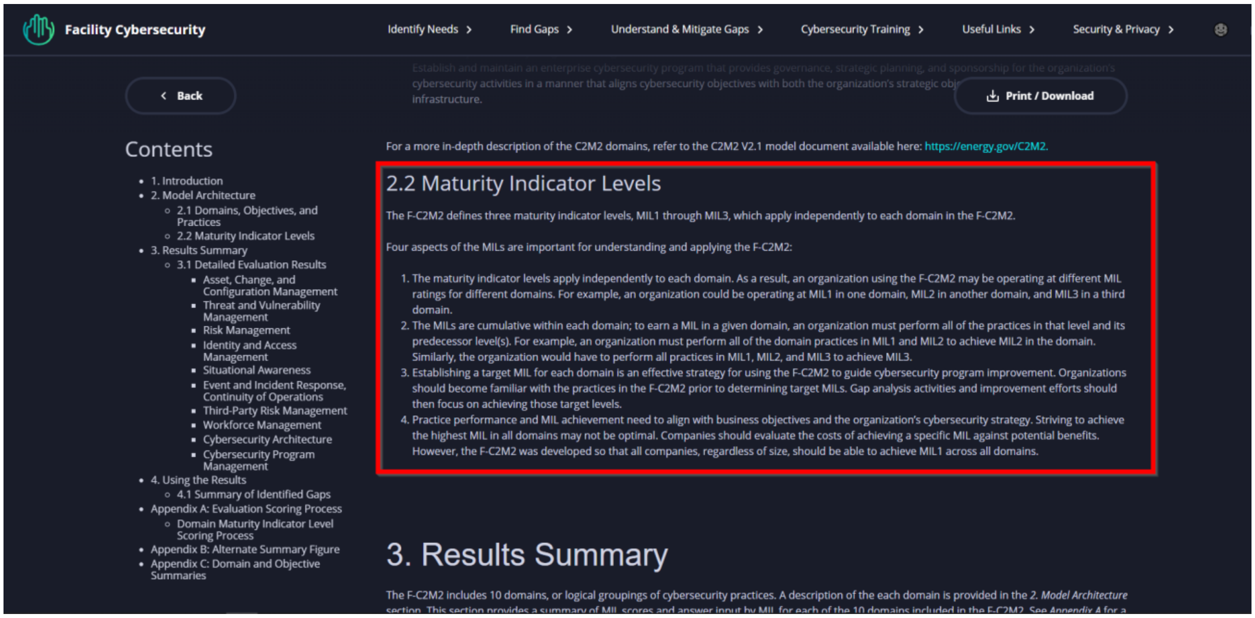
Domain: Event and Incident Response, Continuity of Operations
Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Third-Party Risk Management
Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Workforce Management
Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Cybersecurity Architecture
Establish and maintain the structure and behavior of the organization’s cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Cybersecurity Program Management
Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization’s strategic objectives and the risk to critical infrastructure.



Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic obj
infrastructure.

Contents

For a more in-depth description of the C2M2 domains, refer to the C2M2 V2.1 model document available here: https://energy.gov/C2M2.

2.2 Maturity Indicator Levels

The F-C2M2 defines three maturity indicator levels, MIL1 through MIL3, which apply independently to each domain in the F-C2M2.

Four aspects of the MILs are important for understanding and applying the F-C2M2:

1. The maturity indicator levels apply independently to each domain. As a result, an organization using the F-C2M2 may be operating at different MIL ratings for different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
2. The MILs are cumulative within each domain; to earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level(s). For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
3. Establishing a target MIL for each domain is an effective strategy for using the F-C2M2 to guide cybersecurity program improvement. Organizations should become familiar with the practices in the F-C2M2 prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.
4. Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the F-C2M2 was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

3. Results Summary

The F-C2M2 includes 10 domains, or logical groupings of cybersecurity practices. A description of the each domain is provided in the *2. Model Architecture* section. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the F-C2M2. See *Appendix A* for a

Figure 26: Maturity Indicator Levels

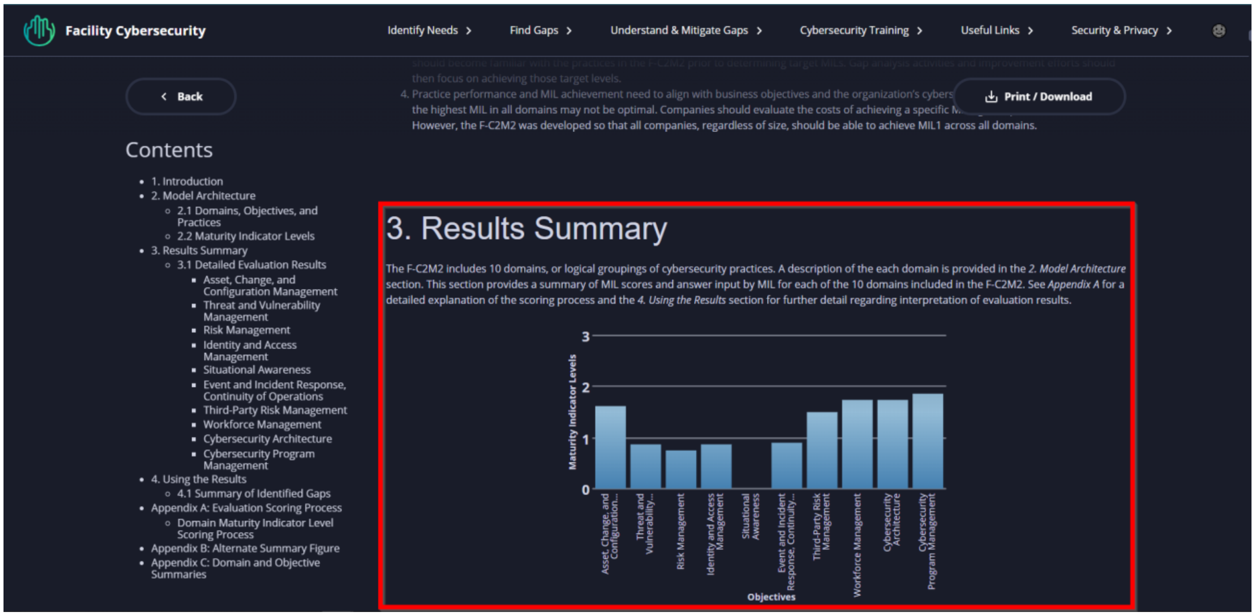
Maturity Indicator Levels (Section 2.2) **Figure 26**: The F-C2M2 provides information describing aspects of the three maturity indicator levels (MILs):MIL1, MIL2, and MIL3.

Four aspects of the MILs are important for understanding and applying the F-C2M2:

1. **The MILs apply independently to each domain**. As a result, an organization using the F-C2M2 may be operating at different MIL ratings for different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
2. **The MILs are cumulative within each domain;** to earn a MIL in each domain, an organization must perform all of the practices in that level and its predecessor level(s). For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
3. **Establishing a target MIL for each domain is an effective strategy for using the F-C2M2 to guide cybersecurity program improvement**. Organizations should become familiar with the practices in the F-C2M2 prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.
4. **Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy.** Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the F-C2M2 was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

Results Summary – Report Section 3

The results section provides a summary of MIL scores for each of the 10 domains included in the F-C2M2 self-assessment (**Figure 27**). The Y-axis of the graph represents the MIL level whereas the X-axis are the respective domain categories. A description of each domain is provided in Section 2.1 of this user guide.



should become familiar with the practices in the F-C2M2 prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.

4. Practice performance and MIL achievement need to align with business objectives and the organization's cybers the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific M However, the F-C2M2 was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

Contents

3. Results Summary

The F-C2M2 includes 10 domains, or logical groupings of cybersecurity practices. A description of the each domain is provided in the *2. Model Architecture* section. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the F-C2M2. See *Appendix A* for a detailed explanation of the scoring process and the *4. Using the Results* section for further detail regarding interpretation of evaluation results.

3
2
1
0
Maturity Indicator Levels
Asset, Change, and Configuration...
Threat and Vulnerability...
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity...
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
Objectives

Figure 27: Results Summary

See Appendix A of this user guide for a detailed explanation of the scoring process.

The results summary by MIL and Domain pie chart, (**Figure 28**) offers a visual representation of the responses contained within each domain. These responses are further categorized by the specific practices that fall under each objective contained in the specific domain. A color-coded legend is provided for a user-friendly interpretation.

🟦 Not Applicable

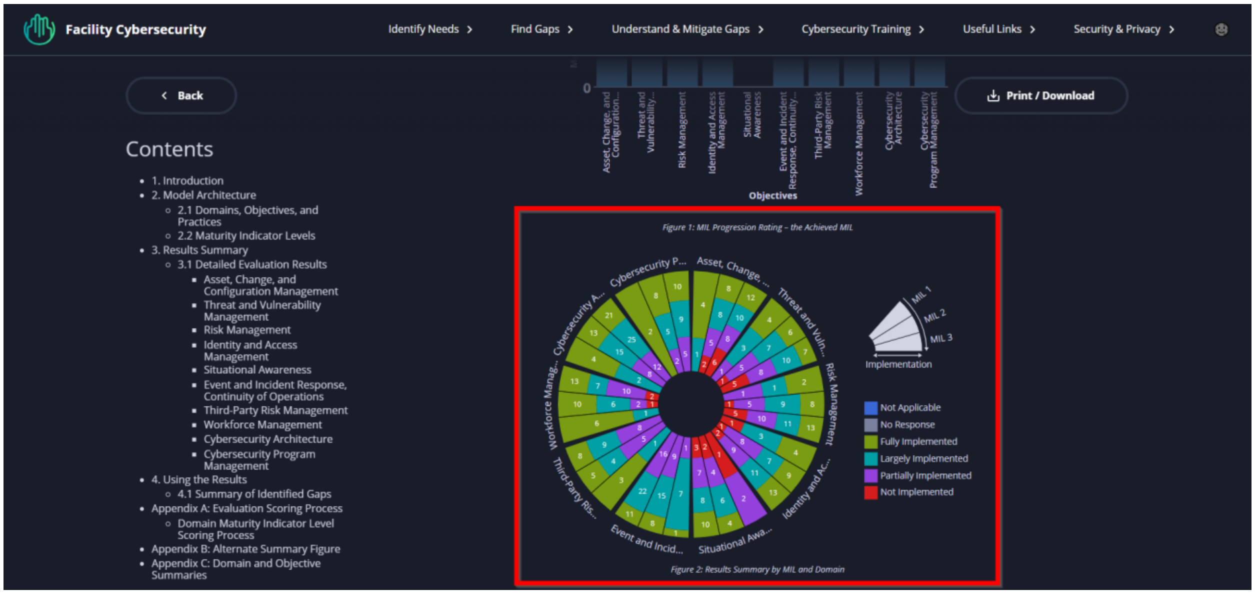
⬜ No Response

🟩 Fully Implemented

🟦 Largely Implemented

🟪 Partially Implemented

🟥 Not Implemented

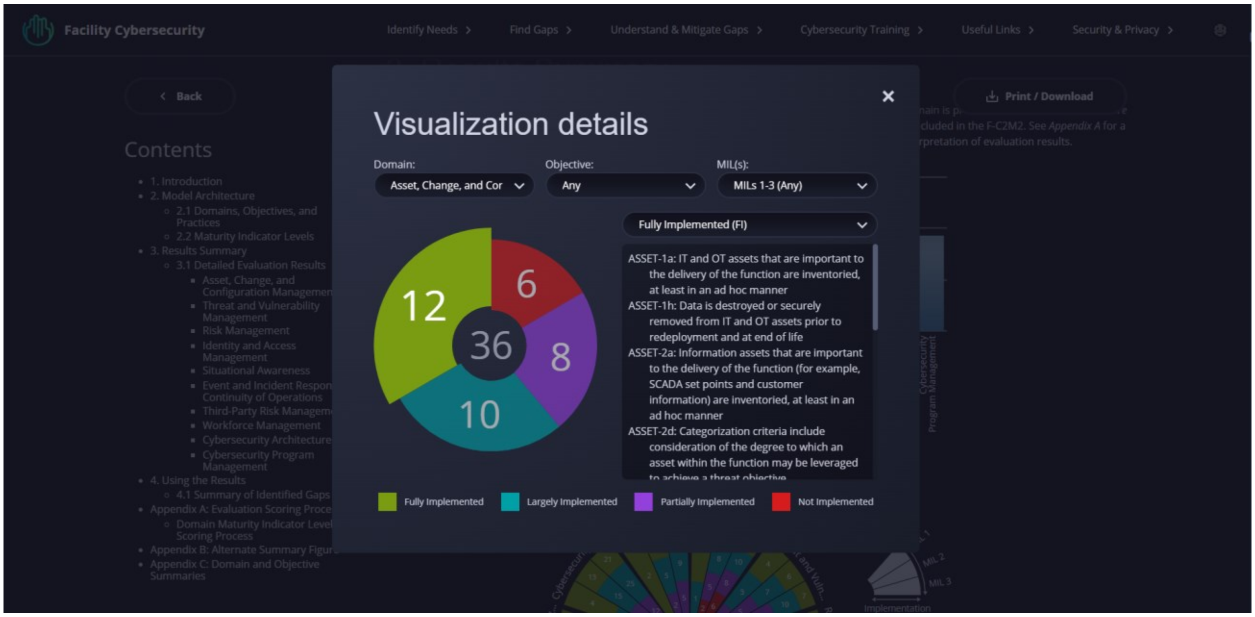


Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

Figure 28: Results Summary by MIL and Domain

The individual pie slices that apply to each domain are interactive and can be clicked on to see visualization details that provide a summary of the domain and the responses selected during the assessment. This allows for easy navigation of the results, showcasing where certain domains may need additional attention or which have reached the highest MIL level desired (**Figure 29**).



Visualization details

Domain: Asset, Change, and Cor

Objective: Any

MIL(s): MILs 1-3 (Any)

Fully Implemented (FI)

ASSET-1a: IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner

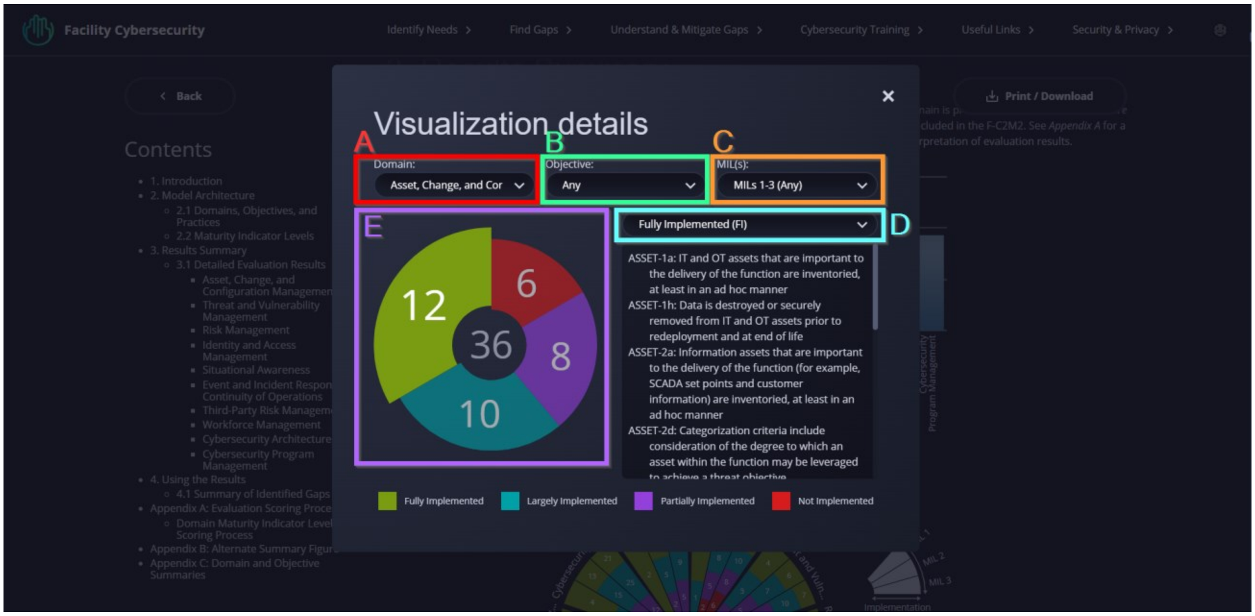
ASSET-1h: Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life

ASSET-2a: Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner

ASSET-2d: Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective

Figure 29: Visualization Details

Drop-down menus allow for easy navigation (**Figure 30**). The user can select the drop-down menu to see results by Domain (A), Objective (B), MIL(s) (C), or Implementation level (D). Users can also click on the colored numbers (E) in the pie chart to cycle through the different MIL levels in the current domain.



Domain: Asset, Change, and Cor

Objective: Any

MIL(s): MILs 1-3 (Any)

Fully Implemented (FI)

ASSET-1a: IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner

ASSET-1h: Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life

ASSET-2a: Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner

ASSET-2d: Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective

Figure 30: Visualization Details Navigation

A chart providing another view into the scoring results by each domain based off user responses can be found in the Pie Summary of Answer input by MIL and Domain (**Figure 31**). Users can also click on the colored numbers within the pie chart to bring up the Visualization details that provide the implementation level and summary of the practices and objectives contained within that domain.

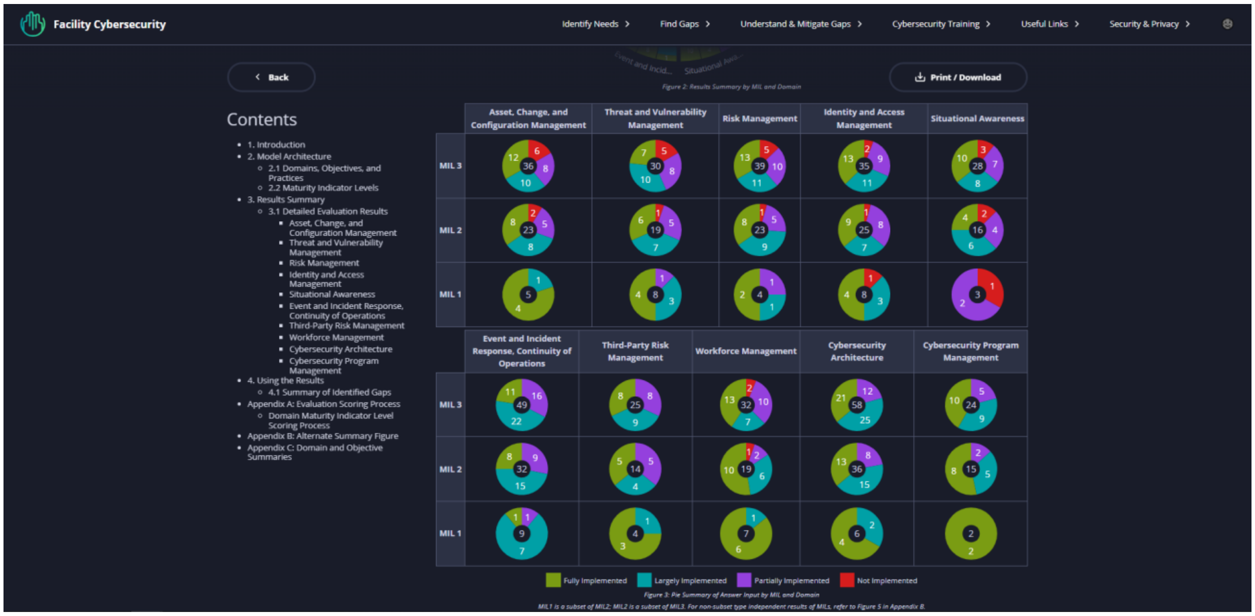
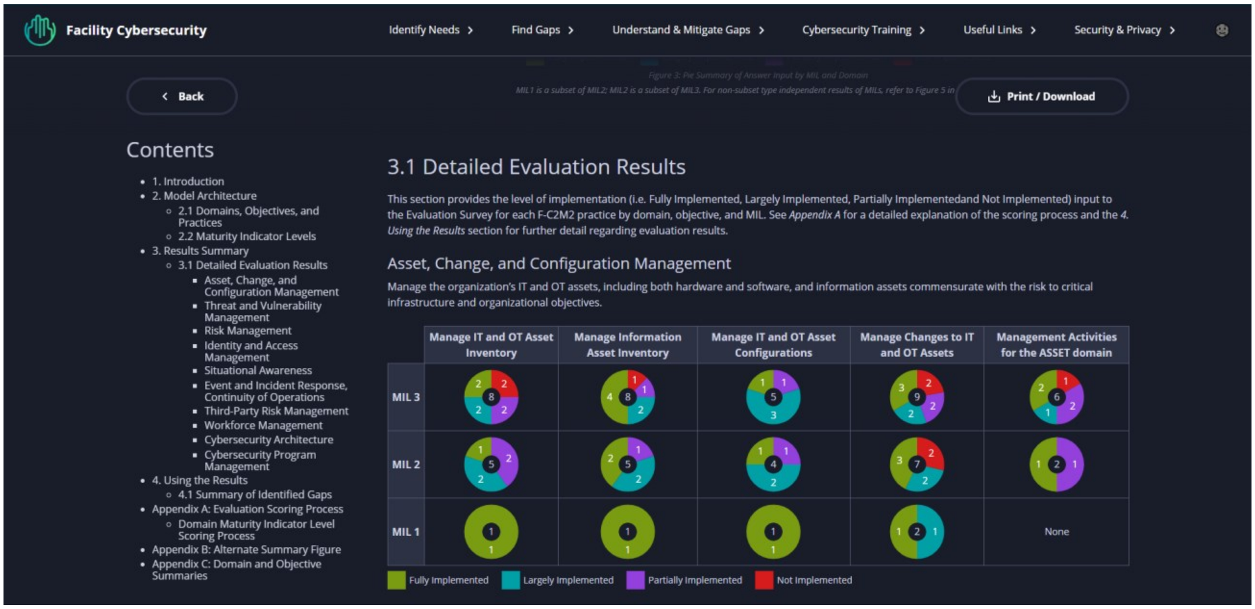

Facility Cybersecurity
Identify Needs
Find Gaps
Understand & Mitigate Gaps
Cybersecurity Training
Useful Links
Security & Privacy
Back
Print / Download
Contents
1. Introduction
2. Model Architecture
2.1 Domains, Objectives, and Practices
2.2 Maturity Indicator Levels
3. Results Summary
3.1 Detailed Evaluation Results
Asset, Change, and Configuration Management
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
4. Using the Results
4.1 Summary of Identified Gaps
Appendix A: Evaluation Scoring Process
Domain Maturity Indicator Level Scoring Process
Appendix B: Alternate Summary Figure
Appendix C: Domain and Objective Summaries
Figure 2: Results Summary by MIL and Domain
Asset, Change, and Configuration Management
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
MIL 3
12 6 36 8 10
7 5 30 8 10
13 5 39 10 11
13 2 35 9 11
10 3 28 7 8
MIL 2
8 2 23 5 8
6 1 19 5 7
8 1 23 5 9
9 1 25 8 7
4 2 16 4 6
MIL 1
1 5 4
4 1 8 3
2 1 4 1
4 1 8 3
1 3 2
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
MIL 3
11 16 49 22
8 8 25 9
13 2 32 10 7
21 12 58 25
10 5 24 9
MIL 2
8 9 32 15
5 5 14 4
1 2 10 19 6
13 8 36 15
2 8 15 5
MIL 1
1 1 9 7
1 4 3
1 7 6
2 6 4
2 2
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented
Figure 3: Pie Summary of Answer Input by MIL and Domain
MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to Figure 5 in Appendix B.

Figure 31: Pie Summary of Answer Input by MIL and Domain

Section 3.1 Contains Detailed Evaluation results (**Figure 32**). This section provides the level of implementation (i.e., Fully Implemented, Largely Implemented, Partially Implemented and Not Implemented) input to the Evaluation Survey results for each F-C2M2 practice by domain, objective, and MIL. This breaks each domain apart by objective and gives detailed visuals into the MIL levels assigned. These sections are also interactive and will display the visualization details pop up screen with explanations of the domains and objectives contained within.


Facility Cybersecurity
Identify Needs ›
Find Gaps ›
Understand & Mitigate Gaps ›
Cybersecurity Training ›
Useful Links ›
Security & Privacy ›
‹ Back
Print / Download
Figure 3: Pie Summary of Answer Input by MIL and Domain
MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to Figure 5 in

Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

3.1 Detailed Evaluation Results

This section provides the level of implementation (i.e. Fully Implemented, Largely Implemented, Partially Implementedand Not Implemented) input to the Evaluation Survey for each F-C2M2 practice by domain, objective, and MIL. See *Appendix A* for a detailed explanation of the scoring process and the *4. Using the Results* section for further detail regarding evaluation results.

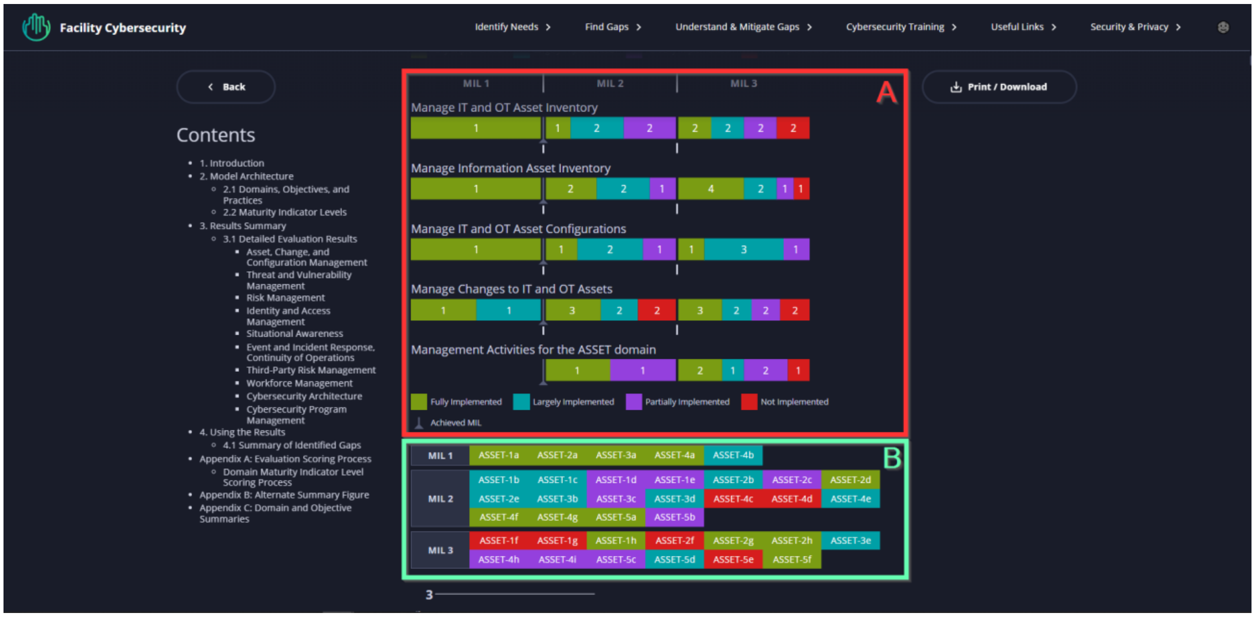
Asset, Change, and Configuration Management

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.

Manage IT and OT Asset Inventory
Manage Information Asset Inventory
Manage IT and OT Asset Configurations
Manage Changes to IT and OT Assets
Management Activities for the ASSET domain
MIL 3
MIL 2
MIL 1
None
Fully Implemented
Largely Implemented
Partially Implemented
Not Implemented

Figure 32: Detailed Evaluation Results

The results are further visualized using bar charts defined by MIL level achieved related to Objectives contained within the Domain (**Figure 33**) exhibit A. The results are also broken down by achieved MIL as it relates to each asset, exhibit B.



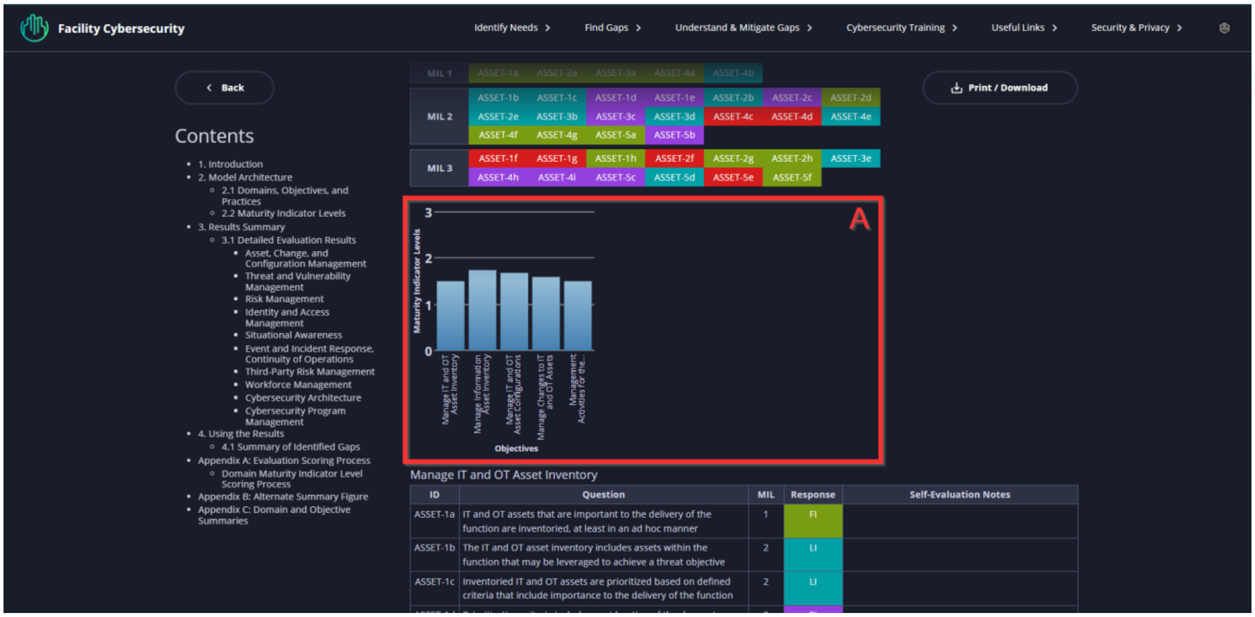
Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

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

Figure 33: Detailed Evaluation Results continued

A bar chart with the Y access representing maturity levels and the x axis assigned to objectives is just another way to easily understand and visually comprehend the MIL level as it applies to each objective displayed in exhibit A (**Figure 34**).


Facility Cybersecurity
Identify Needs >
Find Gaps >
Understand & Mitigate Gaps >
Cybersecurity Training >
Useful Links >
Security & Privacy >
< Back
Print / Download
A
3
2
1
0
Maturity Indicator Levels
Manage IT and OT Asset Inventory
Manage Information Asset Inventory
Manage IT and OT Asset Configurations
Manage Changes to IT and OT Assets
Management Activities for the...
Objectives

Contents

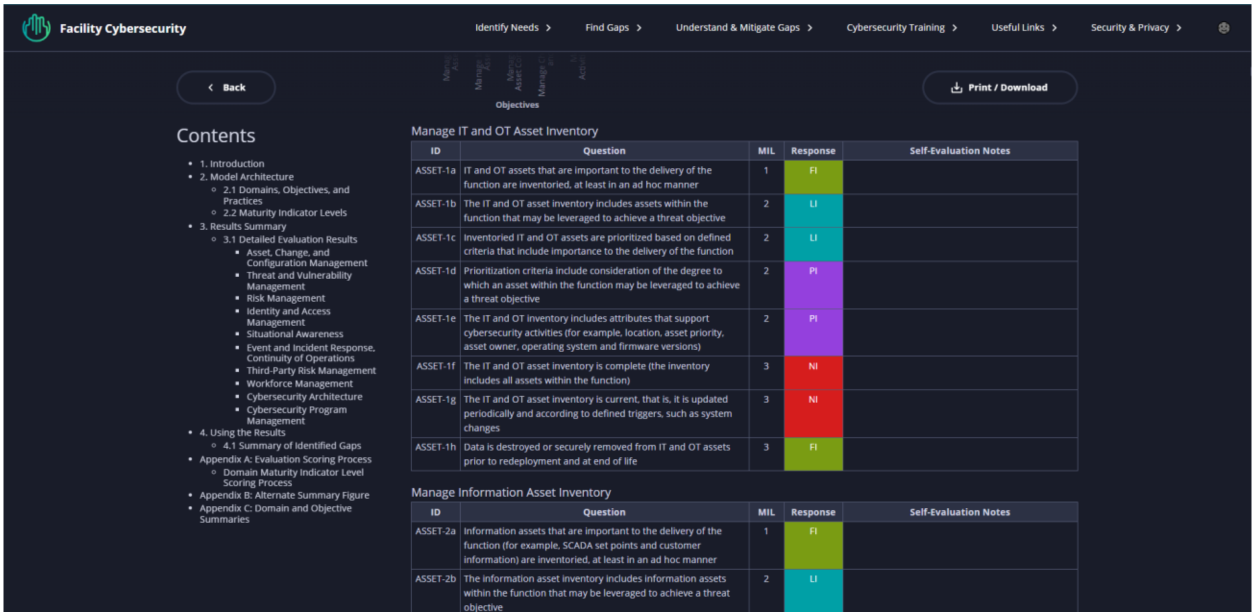
MIL 1	ASSET-1a	ASSET-2a	ASSET-3a	ASSET-4a	ASSET-4b		
MIL 2	ASSET-1b	ASSET-1c	ASSET-1d	ASSET-1e	ASSET-2b	ASSET-2c	ASSET-2d
	ASSET-2e	ASSET-3b	ASSET-3c	ASSET-3d	ASSET-4c	ASSET-4d	ASSET-4e
	ASSET-4f	ASSET-4g	ASSET-5a	ASSET-5b			
MIL 3	ASSET-1f	ASSET-1g	ASSET-1h	ASSET-2f	ASSET-2g	ASSET-2h	ASSET-3e
	ASSET-4h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

Manage IT and OT Asset Inventory

ID	Question	MIL	Response	Self-Evaluation Notes
ASSET-1a	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	1	FI	
ASSET-1b	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	2	LI	
ASSET-1c	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	2	LI	

Figure 34: Maturity level applied to objectives.

Each objective within a given domain is further broken down by their practice ID and the question that pertain to the practices implemented to control and mitigate potential threats. The response is color-coded indicating whether the suggested best practice and guidance has been Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), or Not Implemented (NI) (**Figure 35**). The self-evaluation notes entered over the course of the assessment are included for reference and tracking. This same format and breakdown occur for every domain in the assessment.



Contents

- 1. Introduction
- 2. Model Architecture
  - 2.1 Domains, Objectives, and Practices
  - 2.2 Maturity Indicator Levels
- 3. Results Summary
  - 3.1 Detailed Evaluation Results
    - Asset, Change, and Configuration Management
    - Threat and Vulnerability Management
    - Risk Management
    - Identity and Access Management
    - Situational Awareness
    - Event and Incident Response, Continuity of Operations
    - Third-Party Risk Management
    - Workforce Management
    - Cybersecurity Architecture
    - Cybersecurity Program Management
- 4. Using the Results
  - 4.1 Summary of Identified Gaps
- Appendix A: Evaluation Scoring Process
  - Domain Maturity Indicator Level Scoring Process
- Appendix B: Alternate Summary Figure
- Appendix C: Domain and Objective Summaries

Manage IT and OT Asset Inventory

ID	Question	MIL	Response	Self-Evaluation Notes
ASSET-1a	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	1	FI	
ASSET-1b	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	2	LI	
ASSET-1c	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	2	LI	
ASSET-1d	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	2	PI	
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)	2	PI	
ASSET-1f	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	3	NI	
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	3	NI	
ASSET-1h	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	3	FI	

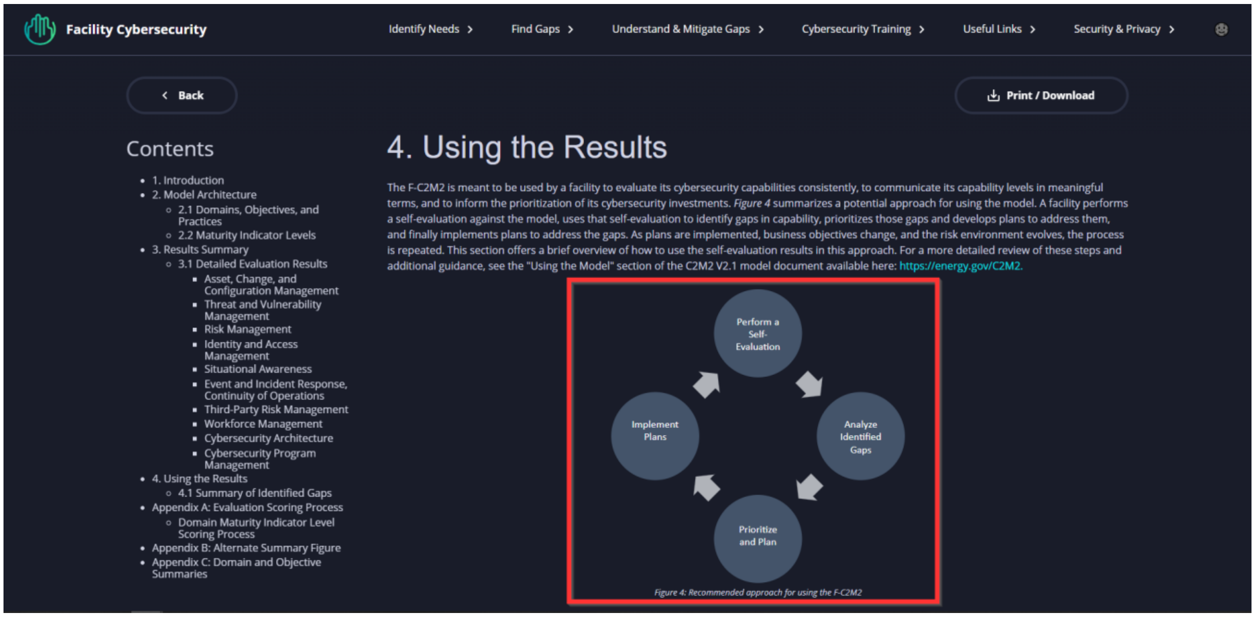
Manage Information Asset Inventory

ID	Question	MIL	Response	Self-Evaluation Notes
ASSET-2a	Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	1	FI	
ASSET-2b	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective	2	LI	

Figure 35: Questions applied to ASSET IDs

Using the Results – Report Section 4

The F-C2M2 is meant to be used by a facility to evaluate its cybersecurity capabilities on a routine or periodic basis, to communicate and document capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. **Figure 36** summarizes a potential approach for using the model. A facility performs a self-evaluation against the model, uses that self-evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. This section offers a brief overview of how to use the self-evaluation results in this approach. For a more detailed review of these steps and additional guidance, see the "Using the Model" section of the C2M2 V2.1 model document available here: https://energy.gov/C2M2.



Contents

4. Using the Results

The F-C2M2 is meant to be used by a facility to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. *Figure 4* summarizes a potential approach for using the model. A facility performs a self-evaluation against the model, uses that self-evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. This section offers a brief overview of how to use the self-evaluation results in this approach. For a more detailed review of these steps and additional guidance, see the "Using the Model" section of the C2M2 V2.1 model document available here: https://energy.gov/C2M2.

Figure 4: Recommended approach for using the F-C2M2

Figure 36: Recommended approach for using the F-C2M2

This report summarizes the results of the facility’s self-evaluation conducted in Step 1, Perform a Self-Evaluation.

It provides a point-in-time view of the cybersecurity posture of the in-scope function. Self-evaluation workshop participants should review this report and collectively address, and any discrepancies or questions before the next step.

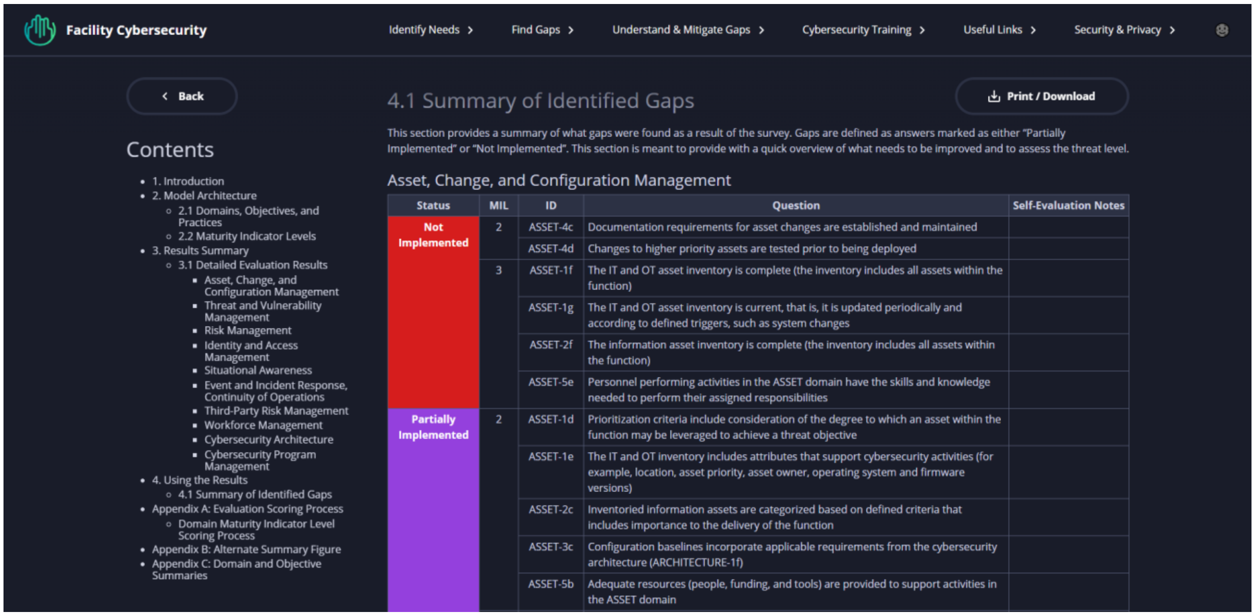
In Step 2, Analyze Identified Gaps, the organization identifies gaps in the performance of model practices by examining the self-evaluation results against its target profile — the desired profile that represents the facility’s target MIL rating for each domain in the model. Organizations using the model for the first time may identify the target profile after performing a self-evaluation, while others often identify a target profile before conducting a self-evaluation. For more information on setting targets, see Appendix D, "Setting Targets" in the C2M2 Self-Evaluation Guide available here: https://energy.gov/C2M2.

In Step 3, Prioritize and Plan, the organization uses the gap analysis to prioritize the actions needed to fully implement the practices in the target profile. A cost-benefit analysis may help to inform the prioritization of actions needed. The organization should then develop a plan to address the selected gaps and assign ownership of the plan to an individual with sufficient authority to oversee implementation.

Regular reviews by organizational leadership should be conducted to evaluate status, clear obstacles, and identify any necessary course corrections as implementation progresses.

In Step 4, Implement Plans and Periodically Reevaluate, plans developed in the previous step should be implemented to address the identified gaps. Subsequent model self-evaluations are particularly useful in tracking implementation and should be conducted periodically to ensure that desired progress is achieved. Reevaluations should also be considered in response to major changes in business, technology, market, or threat environments to ensure that the current profile matches the facility's desired state.

Section 4.1 provides a Summary of Identified Gaps. This is convenient as it allows the facility and stakeholders to easily identify ASSETS that have no resilience or maturity built in, or those that are partially, implemented and may need attention (**Figure 37**).



Contents

4.1 Summary of Identified Gaps

This section provides a summary of what gaps were found as a result of the survey. Gaps are defined as answers marked as either "Partially Implemented" or "Not Implemented". This section is meant to provide with a quick overview of what needs to be improved and to assess the threat level.

Asset, Change, and Configuration Management

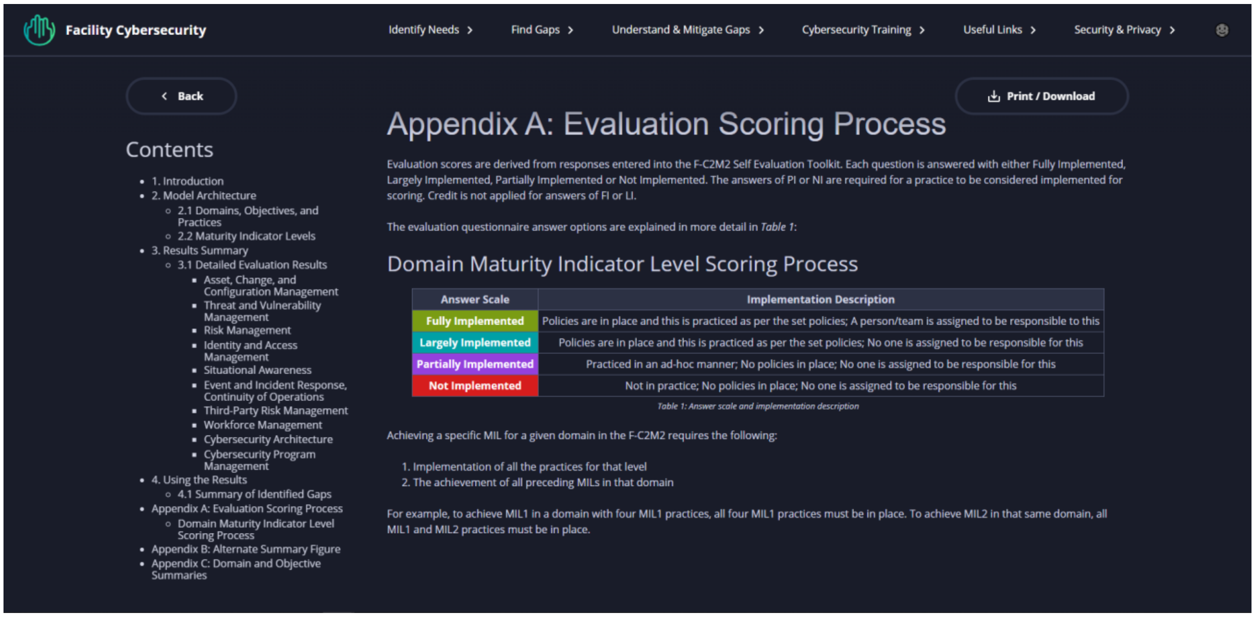
Status	MIL	ID	Question	Self-Evaluation Notes
Not Implemented	2	ASSET-4c	Documentation requirements for asset changes are established and maintained	
		ASSET-4d	Changes to higher priority assets are tested prior to being deployed	
	3	ASSET-1f	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	
		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	
		ASSET-2f	The information asset inventory is complete (the inventory includes all assets within the function)	
		ASSET-5e	Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities	
Partially Implemented	2	ASSET-1d	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	
		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)	
		ASSET-2c	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	
		ASSET-3c	Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f)	
		ASSET-5b	Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain	

Figure 37: Summary of Identified Gaps

Appendices

Appendix A: Evaluation Scoring Process

Evaluation scores are derived from responses entered into the F-C2M2 Self Evaluation Toolkit. Each question is answered with either Fully Implemented, Largely Implemented, Partially Implemented or Not Implemented . The answers of PI or NI are required for a practice to be considered implemented for scoring. Credit is not applied for answers of FI or LI. A color-coded system summarized in **Table 3** is provided based on the response type.



Contents

Appendix A: Evaluation Scoring Process

Evaluation scores are derived from responses entered into the F-C2M2 Self Evaluation Toolkit. Each question is answered with either Fully Implemented, Largely Implemented, Partially Implemented or Not Implemented. The answers of PI or NI are required for a practice to be considered implemented for scoring. Credit is not applied for answers of FI or LI.

The evaluation questionnaire answer options are explained in more detail in *Table 1*:

Domain Maturity Indicator Level Scoring Process

Answer Scale	Implementation Description
Fully Implemented	Policies are in place and this is practiced as per the set policies; A person/team is assigned to be responsible to this
Largely Implemented	Policies are in place and this is practiced as per the set policies; No one is assigned to be responsible for this
Partially Implemented	Practiced in an ad-hoc manner; No policies in place; No one is assigned to be responsible for this
Not Implemented	Not in practice; No policies in place; No one is assigned to be responsible for this

Table 1: Answer scale and implementation description

Achieving a specific MIL for a given domain in the F-C2M2 requires the following:

1. Implementation of all the practices for that level
2. The achievement of all preceding MILs in that domain

For example, to achieve MIL1 in a domain with four MIL1 practices, all four MIL1 practices must be in place. To achieve MIL2 in that same domain, all MIL1 and MIL2 practices must be in place.

Figure 38: Answer Scale and Implementation Description

The answers of FI or LI are required for a practice to be considered implemented for scoring. Credit is not applied for answers of PI or NI. A color-coded system summarized in **Table 3** is provided based on the response type.

Answer Scale	Implementation Description
Fully Implemented (FI)	Policies are in place, and this is practiced as per the set policies; A person/team is assigned and responsible for this
Largely Implemented (LI)	Policies are in place, and this is practiced as per the set policies; Not one person is assigned to be responsible for this.
Partially Implemented (PI)	Practiced in an ad-hoc manner; No policies in place; No one is assigned to be responsible for this
Not Implemented (NI)	Not in practice; No policies in place; No one is assigned to be responsible for this

Table 3: Answer Scale and implementation description

Achieving a specific MIL for a given domain in the F-C2M2 requires the following:

1. Implementation of all the practices for that level
2. The achievement of all preceding MILs in that domain

For example, to achieve MIL1 in a domain with four MIL1 practices, all four MIL1 practices must be in place. To achieve MIL2 in that same domain, all MIL1 and MIL2 practices must be in place.

Appendix B: Alternate Summary Figure

The appendix B offers an alternate view of answers input by MIL and Domain (**Figure 39**). If users click on a given donut, it will provide a pop-up window allowing the user to separate the total responses based on domains, maturity levels, and objectives.

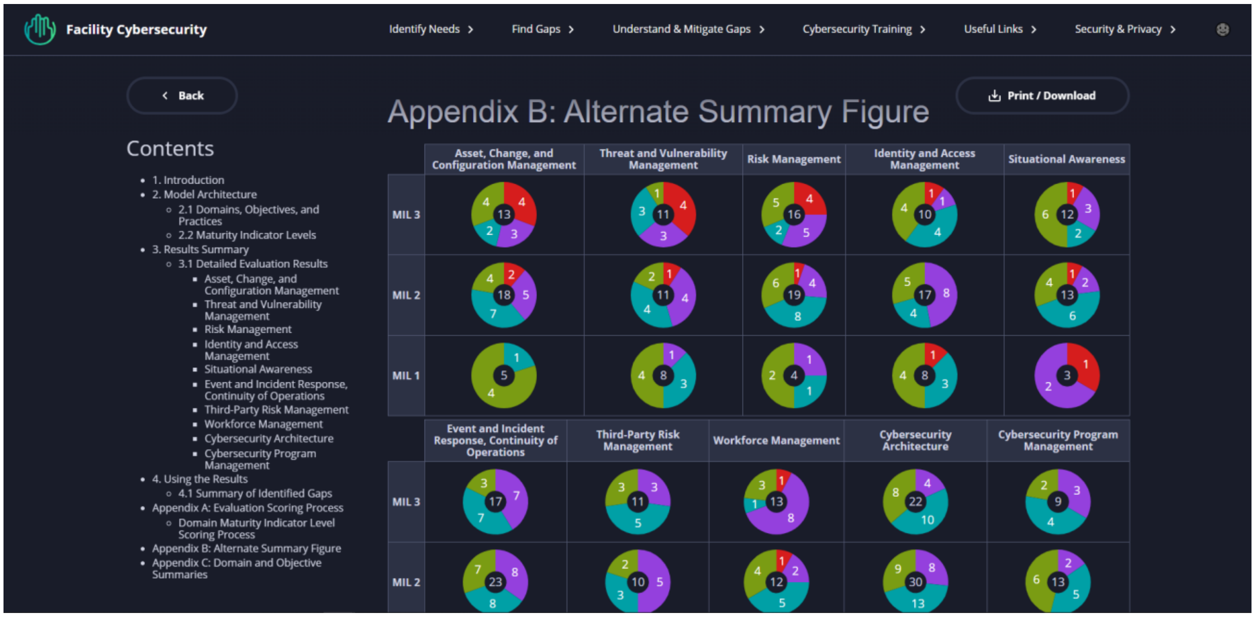

Facility Cybersecurity
Identify Needs >
Find Gaps >
Understand & Mitigate Gaps >
Cybersecurity Training >
Useful Links >
Security & Privacy >
< Back
Print / Download
Appendix B: Alternate Summary Figure
Contents
1. Introduction
2. Model Architecture
2.1 Domains, Objectives, and Practices
2.2 Maturity Indicator Levels
3. Results Summary
3.1 Detailed Evaluation Results
Asset, Change, and Configuration Management
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
4. Using the Results
4.1 Summary of Identified Gaps
Appendix A: Evaluation Scoring Process
Domain Maturity Indicator Level Scoring Process
Appendix B: Alternate Summary Figure
Appendix C: Domain and Objective Summaries
Asset, Change, and Configuration Management
Threat and Vulnerability Management
Risk Management
Identity and Access Management
Situational Awareness
MIL 3
4 13 4 2 3
3 1 11 4 3
5 16 4 2 5
4 1 10 1 4
6 1 12 3 2
MIL 2
4 2 18 5 7
2 1 11 4 4
6 1 19 4 8
5 17 8 4
4 1 13 2 6
MIL 1
1 5 4
4 1 8 3
2 1 4 1
4 1 8 3
3 1 2
Event and Incident Response, Continuity of Operations
Third-Party Risk Management
Workforce Management
Cybersecurity Architecture
Cybersecurity Program Management
MIL 3
3 17 7 7
3 11 3 5
3 1 1 13 8
8 4 22 10
2 9 3 4
MIL 2
7 23 8 8
2 10 5 3
4 1 12 2 5
9 30 8 13
2 6 13 5

Figure 39: Alternate Pie Summary of Answer Input by MIL and Domain

Appendix C: Domain and Objective Summaries

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:

- Manage IT and OT Asset Inventory
- Manage Information Asset Inventory
- Manage Asset Configuration
- Manage Changes to Assets
- 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.

Threat and Vulnerability Management

Purpose: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

A cybersecurity threat is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, or other organizations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats to information, IT, OT, and communication infrastructure assets vary and may include malicious actors, malware (such as viruses and worms) and distributed denial-of-service (DDoS) attacks.

A cybersecurity vulnerability is a weakness or flaw in IT, OT, communications systems or devices, procedures, or internal controls that could be exploited by a threat.

The Threat and Vulnerability Management (THREAT) domain comprises three objectives:

- Reduce Cybersecurity Vulnerabilities
- Respond to Threats and Share Threat Information
- Management Activities

Threat identification and response begins with collecting useful threat information from reliable sources, interpreting that information in the context of the organization and function, and responding to threats that have the means, motive, and opportunity to affect the delivery of services. A threat profile includes characterization of likely intent, capability, and target of threats to the function. The threat profile can be used to guide the identification of specific threats, the risk analysis process described in the Risk Management domain, and the building of the operational and cyber status described in the Situational Awareness domain.

Reducing cybersecurity vulnerabilities begins with collecting and analyzing vulnerability information. Vulnerability discovery may be performed using automatic scanning tools, network penetration tests, cybersecurity exercises, and audits. Vulnerability analysis should consider the vulnerability's local impact (the potential effect of the vulnerability on the exposed asset) as well as the importance of the exposed asset to the delivery of the function. Vulnerabilities may be addressed by implementing mitigating controls, monitoring threat status, applying cybersecurity patches, or performing other activities.

Risk Management

Purpose: Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Cyber risk is defined as risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, IT, or OT assets. Cyber risk is one component of the overall business risk environment and feeds into an organization's enterprise risk management strategy and program. Cyber risk cannot be completely eliminated, but it can be managed through informed decision-making processes.

The Risk Management (RISK) domain comprises five objectives:

- Establish and Maintain Cyber Risk Management Strategy and Program
- Identify Cyber Risk
- Analyze Cyber Risk
- Respond to Cyber Risk
- Management Activities

Managing cyber risk involves framing, identifying, assessing, responding to (accepting, avoiding, mitigating, transferring), and monitoring risks in a manner that aligns with the needs of the organization. Key to performing these activities is a common understanding of the cyber risk management strategy discussed above. With defined risk criteria, organizations can consistently respond to and monitor identified risks. A risk register—a list of identified risks and associated attributes—facilitates this process. Other domains in this model (Situational Awareness and Event and Incident Response, Continuity of Operations) refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cyber risk management program.

A cyber risk management strategy is a high-level strategy that provides direction for analyzing and prioritizing cyber risk and defines risk tolerance. The cyber risk management strategy includes a risk assessment methodology, risk monitoring strategy, and cybersecurity governance program. This includes defining the enterprise risk criteria (for example, impact thresholds and risk response approaches) that guide the cybersecurity program discussed in the Cybersecurity Program Management domain later in this model. The cyber risk management strategy should align with the enterprise risk management strategy to ensure that cyber risk is managed in a manner that is consistent with the organization's mission and business objectives.

Identity and Access Management

Purpose: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

For the purposes of this domain, access control applies to logical access to assets used in the delivery of the function, physical access to cyber assets relevant to the function, and automated access control systems (logical or physical) relevant to the function. Improper access management practices can lead to unauthorized use, disclosure, destruction, or modification, as well as unnecessary exposure to cybersecurity risks.

The Identity and Access Management (ACCESS) domain comprises four objectives:

- Establish and Maintain Identities
- Control Logical Access
- Control Physical Access
- Management Activities

Establishing and maintaining identities begins with the provisioning and deprovisioning (removing available identities when they are no longer required) of identities to entities. Entities may include individuals (internal or external to the organization) as well as devices, systems, or processes that require access to assets. In some cases, organizations may need to use shared identities. Management of shared identities may require compensatory measures to ensure an appropriate level of security. Maintenance of identities includes traceability (ensuring that all known identities are valid) as well as deprovisioning.

Controlling logical and physical access includes determining access requirements, granting access to assets based on those requirements, and revoking access when it is no longer required. Logical and physical access requirements are associated with each asset or assets within a given area and provide guidance for the types of entities or individuals allowed to access the asset, the limits of allowed access and, for logical access, authentication parameters. For example, the logical access requirements for a specific asset might allow remote access by a vendor only during specified and planned maintenance intervals and might also require multifactor authentication for such access. Access restrictions based on physical access requirements are communicated through visible means, such as signage. At higher maturity indicator levels, more scrutiny is applied to the access being granted. Logical and physical access is granted only after considering risk to the function, and regular reviews of access are conducted.

Situational Awareness

Purpose: Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other C2M2 domains, to form a common operating picture (COP).

Situational awareness involves developing near-real-time knowledge of a dynamic operating environment. In part, this is accomplished through the logging and monitoring of IT, OT, and communication infrastructure assets essential for the delivery of the function. It is equally important to maintain knowledge of relevant, current cybersecurity events external to the enterprise. Once an organization develops situational awareness, it can align predefined states of operation to changes in the operating environment. The ability to shift from one predefined state to another can enable faster and more effective response to cybersecurity events or changes in the threat environment.

The Situational Awareness (SITUATION) domain comprises four objectives:

- Perform Logging
- Perform Monitoring
- Establish and Maintain Situational Awareness
- Management Activities

Logging should be enabled based on an asset's potential impact to the function. For example, the greater the potential impact of a compromised asset, the more data an organization might collect about the asset.

Monitoring and analyzing data collected in logs and through other means enables the organization to understand the function's operational and cybersecurity status. Effectively communicating the operational and cybersecurity status to relevant decision makers is the essence of situational awareness (sometimes referred to as a common operating picture). While many situational awareness implementations may include visualization tools, such as dashboards, maps, and other graphical displays, they are not necessarily required to achieve the goal.

Event and Incident Response, Continuity of Operations

Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

A cybersecurity event in a system or network is any observable occurrence that is related to a cybersecurity requirement (confidentiality, integrity, or availability of assets). A cybersecurity incident is an event or series of events that significantly affects or could significantly affect critical infrastructure and/or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts.

The Event and Incident Response, Continuity of Operations domain comprises five objectives:

- Detect Cybersecurity Events
- Analyze Cybersecurity Events and Declare Incidents
- Respond to Cybersecurity Events and Incidents
- Address Cybersecurity in Continuity of Operations
- Management Activities

Detecting cybersecurity events includes designating a forum for reporting events and establishing criteria for event prioritization. These criteria should align with the cyber risk management strategy discussed in the Risk Management domain, ensure consistent valuation of events, and provide a means to determine what constitutes a cybersecurity event, when cybersecurity events are to be escalated, and the conditions that warrant the declaration of cybersecurity incidents.

Escalating cybersecurity events involves applying the criteria discussed in the Detect Cybersecurity Events objective to determine when an event should be escalated and when an incident should be declared. Both cybersecurity events and cybersecurity incidents should be managed according to a response plan. Cybersecurity events and declared incidents may trigger external obligations, including reporting to regulatory bodies or notifying customers.

Correlating multiple cybersecurity events and incidents and other records may uncover systemic problems within the environment.

Responding to cybersecurity incidents requires the organization to have a process to limit the impact of cybersecurity incidents to its functional and organizational units. The process should describe how the organization manages all phases of the incident lifecycle, such as triage, handling, communication, coordination, and closure. Conducting lessons-learned reviews as a part of cybersecurity event and incident response and continuity of operations helps the organization eliminate the exploited vulnerability that led to the incident.

Planning for continuity involves the necessary activities to sustain the function in the event of an interruption, such as a severe cybersecurity incident or a disaster. Ensuring that continuity plans address potential cybersecurity incidents requires consideration of known cyber threats and identified categories of cyber risk. Continuity plan testing should include cybersecurity incident scenarios to ensure that plans will function as intended during such incidents.

Third-Party Risk Management

Purpose: Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

As the interdependencies among infrastructures, operating partners, suppliers, service providers, and customers increase, establishing and maintaining a comprehensive understanding of key relationships and managing their associated cybersecurity risks are essential for the secure, reliable, and resilient delivery of the function.

This model classifies external dependencies as supplier or customer. Supplier dependencies are external parties on which the delivery of the function depends, including operating partners. Customer dependencies are external parties that depend on the delivery of the function, including operating partners.

Supply chain risk is a noteworthy example of a supplier dependency. The cybersecurity characteristics of products and services vary widely. Without proper risk management, they pose serious threats, including software of unknown provenance and counterfeit (possibly malicious) hardware. Organizations' requests for proposal often give suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance. The autonomy organizations often give to their individual business units further increases the risk unless procurement activities are constrained by plan or policy to include cybersecurity requirements.

The Third-Party Risk Management (THIRD-PARTIES) domain comprises three objectives:

- Identify and Prioritize Third Parties
- Manage Third-Party Risk
- Management Activities

Identifying dependencies involves establishing and maintaining a comprehensive understanding of the key external relationships required for the delivery of the function.

Managing dependency risk includes approaches such as independent testing, code review, scanning for vulnerabilities, and reviewing demonstrable evidence from the vendor that a secure software development process has been followed. Contracts binding the organization to a relationship with a partner or vendor for products or services should be reviewed and approved for cybersecurity risk mitigation, such as contract language that establishes vendor responsibilities for meeting or exceeding specified cybersecurity standards or guidelines. Service level agreements can specify monitoring and audit processes to verify that vendors and service providers meet cybersecurity and other performance measures.

Workforce Management

Purpose: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

As organizations increasingly adopt advanced digital technology, it is a challenge to enhance the skill sets of their existing workforce and hire personnel with the appropriate level of cybersecurity experience, education, and training. Organizations' reliance on advanced technology for digital communications and control continues to grow, and workforce issues are a crucial aspect of successfully addressing cybersecurity and risk management for these systems.

Collective bargaining agreements may challenge some aspects of the practices in this domain as written, so organizations may need to implement alternative practices that meet the intent of the model practices and align with those agreements.

The Workforce Management (WORKFORCE) domain comprises five objectives:

- Assign Cybersecurity Responsibilities
- Develop Cybersecurity Workforce
- Implement Workforce Controls
- Increase Cybersecurity Awareness
- Management Activities

An important aspect of assigning cybersecurity responsibilities is ensuring adequacy and redundancy of coverage. For example, specific workforce roles with significant cybersecurity responsibilities are often easy to determine, but they can be challenging to maintain. It is vital to develop plans for key cybersecurity workforce roles such as system administrators to provide appropriate training, testing, redundancy, and evaluations of performance. Of course, cybersecurity responsibilities are not restricted to traditional IT roles; for example, some operations engineers may have cybersecurity responsibilities.

Developing the cybersecurity workforce includes training and recruiting to address identified skill gaps. For example, hiring practices should ensure that recruiters and interviewers are aware of cybersecurity workforce needs. Also, personnel (and contractors) should receive periodic security awareness training to reduce their vulnerability to social engineering and other threats. The effectiveness of training and awareness activities should be evaluated, and improvements should be made as needed.

Implementing workforce controls includes personnel vetting, such as background checks, with extra vetting performed for positions that have access to assets needed to deliver an essential service. For example, system administrators typically have the ability to change configuration settings, modify or delete log files, create new accounts, and change passwords on critical systems, and specific measures are taken for protection of these systems from accidental or malicious behavior by this category of personnel.

Increasing the cybersecurity awareness of the workforce is as important as technological approaches for improving the cybersecurity of the organization. The threat of a cyber-attack to an organization often starts with gaining some foothold into a company's IT or OT systems—for example, by gaining the trust of an unwary employee or contractor who then introduces media or devices into the organization's networks. The organization should share information with its workforce on methods and techniques to identify suspicious behavior, avoid spam and spear phishing, and recognize social engineering attacks to avoid providing information about the organization to potential adversaries. For example, an internal website could provide information about new threats and vulnerabilities in the industry. If no information on threats, vulnerabilities, and best practices is shared with the workforce, personnel may become lax about security processes and procedures.

Cybersecurity Architecture

Purpose: Establish and maintain the structure and behavior of the organization's cybersecurity controls, processes, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

Establishing a cybersecurity architecture involves identifying an organization's critical assets and designing an appropriate set of controls to protect them. The efficacy of those controls is gauged by how well they achieve, both individually and collectively, the cybersecurity objectives for the function. Cybersecurity requirements are either enabled or inhibited by how security controls are designed and applied to assets within the function, in other words, by the cybersecurity architecture.

The Cybersecurity Architecture (ARCHITECTURE) domain comprises six objectives:

- Establish and Maintain Cybersecurity Architecture Strategy and Program
- Implement Network Protections as an Element of the Cybersecurity Architecture
- Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture
- Implement Application Security as an Element of the Cybersecurity Architecture
- Implement Data Security as an Element of the Cybersecurity Architecture
- Management Activities

The cybersecurity architecture provides an overarching plan for how security is to be engineered in a way that transcends point solutions for individual assets such as identity management or access control. It enables reasoning about the security of critical applications and data in terms of known architectural tactics to, for example, detect, resist, react to, and recover from attacks.

Such tactics include segmentation, cryptographic controls, monitoring and redundancy. Additionally, because a cybersecurity architecture is a forward-looking tool for planning, consideration should be given not only to current technology trends but also to potential future developments such as quantum computing and the associated risks it may pose to existing encryption systems. For the cybersecurity architecture to be effective, those responsible for it must be included in planning and decision-making processes when changes to the organization, IT systems, or OT systems are being considered.

Cybersecurity Program Management

Purpose: Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.

A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or the function. A cybersecurity program may be implemented at either the organization or the function level, but a higher-level implementation and enterprise viewpoint may benefit the organization by integrating activities and leveraging resource investments across the entire enterprise.

The Cybersecurity Program Management (PROGRAM) domain comprises three objectives:

- Establish Cybersecurity Program Strategy
- Sponsor Cybersecurity Program
- Management Activities

The cybersecurity program strategy is established as the foundation for the program. In its simplest form, the program strategy should include a list of cybersecurity objectives and a plan to meet them. At higher levels of maturity, the program strategy will be more complete and include priorities, a governance approach, structure and organization for the program, and more involvement by senior management in the design of the program.

Sponsorship is important for implementing the program in accordance with the strategy. The fundamental form of sponsorship is to provide resources (people, tools, and funding). More advanced forms of sponsorship include visible involvement by senior leaders and designation of responsibility and authority for the program. Further, sponsorship includes organizational support for establishing and implementing policies or other organizational directives to guide the program.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov