C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2)

Version 2.0

July 2021

U.S. DEPARTMENT OF ENERGY

OFFICE OF
Cybersecurity, Energy Security,
and Emergency Response

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

This Cybersecurity Capability Maturity Model (C2M2) was developed through a collaborative effort between public- and private-sector organizations, sponsored by the United States Department of Energy (DOE), the Electricity Subsector Coordinating Council (ESCC), and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). The DOE thanks the organizations and individuals who provided the critiques, evaluations, and recommendations necessary to produce this document.

Program Lead

Fowad Muneer
Office of Cybersecurity, Energy Security, and Emergency Response
United States Department of Energy

Model, Version 2.0 Team and Contributors

Joseph Adams, Duke Energy	Aaron Hescox, Exelon	Nathan Mitchell, American Public Power Association (APPA)
Shola Anjous, Motiva	Paul Holgate, Benton PUD	Jason Nations, OGE Energy Corp.
Amy Batallones, ConEdison	Cynthia Hsu, NRECA	Louis Nguyen, SoCalGas
Dave Batz, Edison Electric Institute (EEI)	Ryan Hutton, Arizona Public Service (APS)	Erik Norland, Chelan County PUD
Howard Biddle, American Electric Power (AEP)	Brian Irish, Salt River Project (SRP)	Bonnie Norman, Colonial Pipeline
Shawn Bilak, Southern Company	Michael Isper, Interstate Natural Gas Association of America (INGAA)	Maggie O'Connell, American Fuel & Petrochemical Manufacturers (AFPM)
Steve Brain, Dominion Energy	John Jorgensen, Black Hills Energy	John Osborne, Knoxville Utilities Board
Jonathan Bransky, Dominion Energy	Nick Julian, Knoxville Utilities Board	Niyo Pearson, One Gas
Jeff Brausieck, Seattle City Light	Steve Keisner, Edison Electric Institute (EEI)	Jose Pena, Knoxville Utilities Board
Kaitlin Brennan, Edison Electric Institute (EEI)	Mark Kenner, Knoxville Utilities Board	Michael Perdunn, Omaha Public Power District
James Brosnan, Evergy	Sung Kim, CPS Energy	Chris Peters, Entergy
Juanita Buchanan, Exelon	Jordan King, Portland General Electric	Brandon Pixley, CPS Energy
Kenneth Carnes, New York Power Authority (NYPA)	Scott Klauminzer, Tacoma Power	Timothy Pospisil, Nebraska Public Power District (NPPD)
Shane Clancy, Santee Cooper	Matt Knight, Owensboro Municipal Utilities	Vijay Pounraj, CPS Energy

Model, Version 2.0 Team and Contributors (continued)

Emily Clark, American Petroleum Institute (API)	Dean Kovacs, Energy Northwest	Robert Prince, Sempra
James Clark, South Jersey Industries	Tom Lalonde, SoCalGas	Jody Raines, New Jersey Board of Public Utilities
Mark Coffey, Eversource	Tamara Lance, Atmos Energy	Kaila Raybuck, Edison Electric Institute (EEI)
Linda Conrad, Exelon	Suzanne Lemieux, American Petroleum Institute (API)	Laura Ritter, Duke Energy
Andrew Copeland, One Gas	Matt Light, Xcel Energy	Diana Lynn Rodriguez, Salt River Project (SRP)
Tim Corum, Knoxville Utilities Board	Jim Linn, American Gas Association (AGA) / DNG-ISAC	Brian Rudowski, Long Island Power Authority (LIPA)
Randy Crissman, New York Power Authority (NYPA)	Mujib Lodhi, Long Island Power Authority (LIPA)	David Sayles, Tri-State Generation and Transmission Association
Stephen Dake, Madison Gas and Electric (MGE)	Helen Lorimor, Southern California Edison (SCE)	Moin Shaikh, NRECA
Michael Fish, Salt River Project (SRP)	Jacob Maenner, Exelon	Curtis Stapleton, Enable Midstream Partners
Chris Folta, Benton PUD	Carter Manucy, Florida Municipal Power Agency	Jon Stitzel, Ameren
Kegan Gerard, Southern California Edison (SCE)	Shane Markley, Southwest Gas	Chris Taylor, Southern Company
Charles Glidden, Oncor	Paul Matthews, Dominion Energy	Michael Tomasiewicz, Omaha Public Power District
Patrick Glunz, Nebraska Public Power District (NPPD)	Joshua Mauk, Omaha Public Power District	Gerardo Trevino, EPRI
Geoff Goolsbay, One Gas	Dan Miller, Entergy	Tabice Ward, DTE Energy
Matt Harper, Devon Energy	Steve Miller, UGI Corp	Joy Weed, Southern California Edison (SCE)
Nicholas Harrison, Salt River Project (SRP)	Robert Mims, Southern Company	Spencer Wilcox, PNM Resources
Noelle Henrickson, Evergy	Krishna Mistry, ConEdison	Mark Wixon, Black Hills Energy

Advisory Contributors

Joshua Axelrod, Ernst and Young	Angela Haun, Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC)	Brenden Pavlica, Ernst and Young
Jason Christopher, Dragos	David Howard, DOE	S Pelletier, Dragos
Robert Di Pietro, PWC	Al Kaufmann, Nevermore Security	Maggy Powell, Amazon
Grayson Estes, Estes.io	Annabelle Lee, Nevermore Security	Mark Stacey, Dragos
Stu Goodwin, PWC	Samara Moore, Amazon	Ryan Subers, Ernst and Young
Walter Grudzinski, PWC	Mobolaji Moyosore, Clear Channel	Kai Thomsen, Dragos

Program Team and Contributors

Brian Benestelli, Carnegie Mellon University Software Engineering Institute - CERT Program	John Keenan, Idaho National Laboratory (INL)	Ron Savoury, MITRE
Eric Cardwell, Axio	Ismael Khokhar, ICF	Patrick Siebenlist, Nexight
Michael Cohen, MITRE	Lindsay Kishter, Nexight	Paul Skare, Pacific Northwest National Laboratory (PNNL)
Pamela Curtis, Axio	Josie Long, MITRE	Beth Slaninka, Nexight
Jack Eisenhauer, Nexight	Julia Mullaney, Carnegie Mellon University Software Engineering Institute - CERT Program	Morgan Smith, Nexight
Tricia Flinn, Carnegie Mellon University Software Engineering Institute - CERT Program	Bradley Nelson, Idaho National Laboratory (INL)	Darlene Thorsen, Pacific Northwest National Laboratory (PNNL)
John Fry, Axio	Jason Pearlman, Nexight	Hillary Tran, MITRE
Doug Gardner, Carnegie Mellon University Software Engineering Institute - CERT Program	Alexander Petrilli, Carnegie Mellon University Software Engineering Institute - CERT Program	David White, Axio
Clifford Glantz, Pacific Northwest National Laboratory (PNNL)	Jeanne Millet Petty, Appligent Document Solutions	Virginia Wright, Idaho National Laboratory (INL)
Sri Nikhil Gourisetti, Pacific Northwest National Laboratory (PNNL)	Jeff Pinkhard, Carnegie Mellon University Software Engineering Institute - CERT Program	Chris Yates, MITRE
Jessica Hedges, Carnegie Mellon University Software Engineering Institute - CERT Program	Rick Randall, MITRE	Walter Yamben, National Energy Technology Laboratory
Gavin T Jurecko, Carnegie Mellon University Software Engineering Institute - CERT Program	Paul Ruggiero, Carnegie Mellon University Software Engineering Institute - CERT Program	

Government Contributors

DOE recognizes the efforts and cooperation by the Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE), and other government partners within the Energy Sector Government Coordinating Council (EGCC).

CAUTIONARY NOTE

Intended Scope and Use of This Publication

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

NOTE TO READERS ON THE UPDATE

*****

This version of the C2M2 comprises significant updates and changes including a newly added domain (Cybersecurity Architecture) and substantially revised domains (Risk Management and Third-Party Risk Management). Industry pilot testing of the C2M2, V2.0 is taking place in June and July 2021. Any lessons learned and feedback from the pilots will be addressed by the Energy Sector C2M2 Working Group and integrated into the model by the end of 2021.

*****

Since the last update of the Cybersecurity Capability Maturity Model, both technology and threat actors have become more sophisticated, creating new attack vectors and introducing new risks. The C2M2, Version 2.0 is intended to address these challenges. Also, new cybersecurity standards have been developed and existing standards have been improved. The C2M2, Version 2.0 incorporates guidance from energy sector cybersecurity practitioners and enhancements to improve alignment with internationally recognized cyber standards and best practices, including the National Institute of Standards and Technology (NIST) Special Publication 800-53 and the NIST Cybersecurity Framework (CSF) Version 1.1 released in April 2018.

Table 1: Summary of Changes

Update	Description of Update
Alignment with NIST Cybersecurity Framework	Version 2.0 of the model has been enhanced to account for updates made to the NIST Cybersecurity Framework.
Improvement of existing practices	Practices in Version 1.1 were reviewed and updated to improve clarity and ease of implementation. A few examples of the changes resulting from this review include: • reduction in the number of management practices • reordering of the first four domains • reordering of Threat and Vulnerability Management, Workforce Management, and Risk Management approach objectives • rewording of existing practices • redistribution of Information Sharing and Communications practices throughout the model

Table 1: Summary of Changes (continued)

Update	Description of Update
New Cybersecurity Architecture domain	Version 2.0 of the model includes the new Cybersecurity Architecture domain to help ensure that organizations take appropriate measures to protect networks and data. This domain incorporates the cybersecurity architecture and secure software development practices that formerly were in the Cybersecurity Program Management domain.
Revisions to Risk Management domain	In response to feedback received from C2M2 users, revisions have been made to the Risk Management domain that are intended to make it easier to understand, more concrete, and easier to implement. The changes include a shift in focus from strategy and program management practices to identification, analysis, and risk response practices, more efficient management of risks through categorization and prioritization, and more granular impact analysis concepts.
Updates to Continuity of Operations	Version 2.0 of the model contains additional practices for the critical concept of continuity of operations. These practices include roles and responsibilities, as well as backup testing.
Renamed and revised Supply Chain and External Dependencies Management domain	To better reflect the need to identify, prioritize, and manage third parties in the protection of critical infrastructure, this domain has been renamed Third-Party Risk Management (THIRD-PARTIES) and its practices have been updated.

Table 2: Summary of Changes to Product Suite

Update	Description of Update
Additional guidance and usability	Guidance was added throughout the C2M2 product suite to improve the understanding of the model and the facilitation, consistency, and accuracy of the C2M2 self-evaluation. Information was added to assist in determining the function for the self-evaluation. The process DOE recommends for actioning the results from the C2M2 self-evaluation has been integrated into the model. Help text was enhanced or created for each practice.
Updated self-evaluation tool	The self-evaluation tool was updated to a new PDF format with additional reports to make the tool more robust and more useful. In addition, an HTML-based tool was developed. Both tools maintain all data on users' local machines.

1. INTRODUCTION

Repeated cyber intrusions into organizations of all types demonstrate the need for improved cybersecurity. Cyber threats continue to grow, and they represent one of the most serious operational risks facing modern organizations. National security and economic vitality depend on the reliable functioning of critical infrastructure and the sustained operation of organizations of all types in the face of such threats. The Cybersecurity Capability Maturity Model can help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience.

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

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

The C2M2 is designed for use with a self-evaluation methodology and tool (available by request) for an organization to measure and improve its cybersecurity program.[1] A self-evaluation using the tool can be completed in one day, but the tool could be adapted for a more rigorous evaluation effort. Additionally, the C2M2 can be used to guide the development of a new cybersecurity program.

The C2M2 provides descriptive rather than prescriptive guidance. The model content is presented at a high level of abstraction so that it can be interpreted by organizations of various types, structures, sizes, and industries. Broad use of the model by a sector can support benchmarking of the sector's cybersecurity capabilities. These attributes also make the C2M2 an easily scalable tool for implementing the NIST Cybersecurity Framework [NIST CSF].

1.1 Intended Audience

The C2M2 enables organizations to evaluate cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and prioritize cybersecurity investments. The model can be used by any organization, regardless of ownership, structure, size, or

[1] The C2M2 self-evaluation tools may be obtained by sending a request to C2M2@hq.doe.gov or by visiting https://www.energy.gov/C2M2.

industry. Within an organization, various stakeholders may benefit from familiarity with the model. This document specifically targets people in the following organizational roles:

- **Decision makers** (executives) who control the allocation of resources and the management of risk in organizations; these are typically senior leaders[2]
- **Leaders** with responsibility for managing organizational resources and operations associated with the domains of this model (See Section 4.1 for more information on the content of each C2M2 domain.)
- **Practitioners** with responsibility for supporting the organization in the use of this model (planning and managing changes in the organization based on the model)[3]
- **Facilitators** with responsibility for leading a self-evaluation of the organization based on this model and an evaluation tool and analyzing the self-evaluation results[4]

1.2 Document Organization

This document, along with several others, supports organizations in the effective use of the C2M2. It introduces the model and provides the C2M2's main structure and content.

- Section 2: Provides background about the stakeholders who collaborated on the C2M2 and themes that characterized its development.
- Section 3: Describes several core concepts that are important for interpreting the content and structure of the C2M2.
- Section 4: Describes the architecture of the C2M2.
- Section 5: Provides guidance on how to use the model.
- Section 6: Contains the model itself—its objectives and practices, organized into domains.
- Appendix A: Includes references that either were used in the development of this document or that provide further information.
- Appendix B: Is the glossary.
- Appendix C: Defines the acronyms used in this document.

Stakeholders may benefit by focusing on specific sections of this document, as outlined below. Beyond these recommendations, all readers may benefit from understanding the entire document.

- Decision makers: Sections 1, 2, and 3
- Leaders or managers: Sections 1, 2, 3, and 4
- Practitioners: Entire document
- Facilitators: Entire document

[2] The sponsor of the self-evaluation should be a decision maker from the organization. For more information about the sponsor role, refer to the *C2M2 Self-Evaluation Guide*. The *C2M2 Self-Evaluation Guide* may be downloaded from https://www.energy.gov/C2M2.

[3] Subject matter experts (SMEs) for the self-evaluation should be leaders or practitioners. For more information about the SME role, refer to the *C2M2 Self-Evaluation Guide*. The *C2M2 Self-Evaluation Guide* may be downloaded from https://www.energy.gov/C2M2.

[4] For more information about the facilitator role, refer to the *C2M2 Self-Evaluation Guide*. The *C2M2 Self-Evaluation Guide* may be downloaded from https://www.energy.gov/C2M2.

2. BACKGROUND

C2M2 was first released in 2012 and was updated in 2014 in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House initiative led by the DOE in partnership with the DHS and in collaboration with private- and public-sector experts and representatives of asset owners and operators within the electricity subsector. The initiative used the National Infrastructure Protection Plan framework as a public-private partnership mechanism to support the development of the model. The C2M2, Version 2.0 initiative leveraged and built upon existing efforts, models, and cybersecurity best practices to advance the model by adjusting to new technologies, practices, and environmental factors.

Since the previous releases, more strategic guidance has been provided by the White House through Presidential Executive Orders 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”[5] and 13636 “Improving Critical Infrastructure Cybersecurity.”[6] C2M2, Version 2.0 aligns to recent strategic guidance to strengthen and improve the nation’s cybersecurity posture and capabilities and to reinforce the need for action towards systematic security and resilience.

C2M2, Version 2.0 incorporates other enhancements to better align model domains and practices with internationally recognized cybersecurity standards and best practices, including the NIST Cybersecurity Framework Version 1.1 released in April 2018. Since C2M2 was last updated, new cybersecurity standards and frameworks have been developed, existing standards have improved, and technology has evolved. The energy sector has increasingly become a target of malicious actors as industry increases the use of networked technologies. These challenges and the evolution of cybersecurity practices necessitated the update.

2.1 Model Development Approach

C2M2, Version 2.0 builds upon initial development activities and is enhanced through the following approach:

- ***Public–private partnership:*** Numerous government, industry, and academic organizations participated in the development of the model, bringing a broad range of knowledge, skills, and experience to the team. The initial model was developed collaboratively with an industry advisory group through a series of working sessions, and the new version was revised based on feedback from more than 60 industry experts with extensive experience using Version 1.1.

[5] https://trumpwhitehouse.archives.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/
[6] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

- ***Best practices and sector alignment:*** The model builds upon and ties together a number of existing cybersecurity resources and initiatives and was informed by a review of cyber threats to the subsector. Leveraging related works shortened the development schedule and helped to ensure that the model would be relevant and beneficial to the subsector.
- ***Descriptive, not prescriptive:*** The model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be abstract so that they can be interpreted for organizations of various structures, functions, and sizes.

3. CORE CONCEPTS

This chapter describes several core concepts that are important for interpreting the content and structure of the model.

3.1 Maturity Models

A *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.

A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. Also, when a model is widely used in a particular industry and assessment results are anonymized and shared, organizations can benchmark their performance against other organizations. An industry can determine how well it is performing overall by examining the capability of its member organizations.

To measure progression, maturity models typically have “scaled levels.” C2M2 uses a scale of maturity indicator levels (MILs) 0–3, which are described in Section 4.2. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

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

3.2 Critical Infrastructure Objectives

The model makes regular reference to *critical infrastructure objectives*. These are objectives found in the sector-specific infrastructure protection plans[7] of the 16 United States critical infrastructure sectors defined in Presidential Policy Directive 21, “Critical Infrastructure Security and Resilience.”[8] The referenced objectives serve as a reminder that many of the functions provided by potential adopters of the model support the Nation’s critical infrastructure and that the broader cybersecurity objectives of the sector-specific plans should be considered.

Critical infrastructure objectives often transcend the business or operational objectives for an individual organization. Some organizations using the model may not be affiliated with any of the defined critical infrastructure sectors. For such organizations, the term *critical infrastructure*

[7] http://www.dhs.gov/sector-specific-plans

[8] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

objectives can be interpreted to mean industry objectives, community objectives, or any other objectives that transcend the specific business or operational objectives for the organization but which the organization has a role and interest in fulfilling.

3.3 Enterprise, Organization, and Function

The terms *enterprise*, *organization*, and *function* identify which part of an entity the text of the model is referring to. *Function* refers to the part of an entity to which the C2M2 will be applied (as described further in Section 3.3.1). *Organization* is a higher level administrative unit in which the function resides (e.g., an operating company). *Enterprise* refers to the highest level administrative unit within an entity using the C2M2 (e.g., a parent company).

It is also important to consider that the C2M2 model was designed to apply to a wide variety of entity types. Some enterprises may consist of multiple organizations (e.g., a holding company with one or more operating companies); other organizations may have a more homogenous structure that does not necessitate any differentiation between the terms *enterprise* and *organization*. For those organizations, *enterprise* and *organization* may be used interchangeably. Figure 1 depicts how the enterprise, organization, and function may be organized in a notional entity.

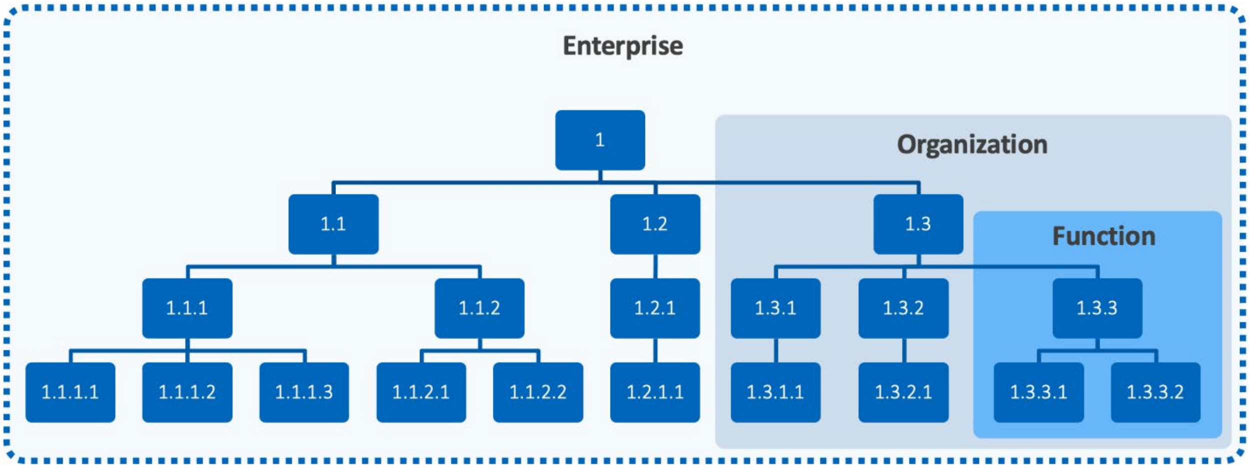


Figure 1: Example of the Structure of a Notional Entity

3.3.1 Function

In the model, the term *function* is used as a scoping mechanism; it refers to the operations of the organization that are being evaluated based on the model. It is common for an organization to use the model to evaluate a subset of its operations.

As stated earlier, the C2M2 focuses on the implementation and management of cybersecurity practices associated with information, information technology, and operations technology *assets* and the *environments* in which they operate. Selecting the function that will be the focus of a C2M2 evaluation determines both the specific assets and people to be evaluated. Together, they constitute the function's operating environment.

The model broadly defines the function to allow organizations the greatest degree of flexibility in determining the scope of the evaluation that is appropriate for them. Functions can align with organizational boundaries or they can align to a single product line or system that may cross organizational boundaries. They might include departments; lines of business; distinct facilities; network security zones; groupings of assets; or assets, processes and resources managed externally, such as assets that reside in the cloud. Examples of functions include Enterprise IT, Power Distribution, Power Generation, Plant Control and Monitoring System, E-Services, Bulk Electric SCADA System, ICS for Refinement Operations, Fuel Transportation, and Storage Terminals. To help clarify evaluation responses, organizations will sometimes limit the scope even further, based on whether the assets are regulated or unregulated or based on their location, such as by region or on-site versus off-site.

Some things to consider when defining the function are:

- its significance to the organization’s mission
- its stakeholders
- its supporting assets
- whether the organization has identifiable ownership (that is, authority) over its supporting assets

Organizations should select only functions that they can clearly determine based on the criteria above.

For example, an organization evaluates Plant Control and Monitoring systems. The organization describes the function’s criteria as follows:

- its significance to the organization’s mission
  - *The function directly supports our largest plant in the state.*

- its stakeholders
  - *Internally our finance department gets a report of our output per week.*
  - *Internally our parent organization requires access to collect information.*
  - *Externally the plant provides power for X number of people, Y cities, Z counties.*

- its supporting assets
  - *IT equipment that directly supports the function.*
  - *OT equipment that directly supports the function.*
  - *Information assets that directly support the function.*
  - *Finance and HQ receive reports directly from the system.*
  - *There are 3 stations that are staffed 24/7 with 4 people per shift for 4 shifts.*
  - *We have 2 vendors that can provide administrative support to the IT or OT systems via VPN.*
  - *The maintenance and engineering team has endpoint connection access to the equipment but not the control room.*
  - *The ICS system is redundant and can be swapped in by the control room.*

  - *There is a backup site about 100 miles away, which is connected through VPN and backs up the software and data on the network daily. ICS data files are backed up during maintenance periods every 6 months.*

- whether the organization has identifiable ownership (that is, authority) over its supporting assets
  - *Ownership is shared between the IT department (IT equipment and network) and the Plant (ICS and other OT equipment).*

When determining the function, one should try to avoid encompassing multiple organizations that have substantially different cybersecurity activities. For example, if an organization has a subsidiary whose cybersecurity activities are substantially different from those of headquarters, it is recommended that the organization perform separate evaluations for the subsidiary and headquarters. Combining these units in one evaluation may result in less accurate or actionable evaluation results for headquarters and the subsidiary.

3.4 Assets

Many C2M2 practices refer to *assets*. For the purposes of the model, assets are IT assets, OT assets, and information assets. Some practices specify particular asset types. IT and OT assets include both hardware and software, such as traditional and emerging enterprise IT assets and any industrial control system (ICS) devices, process control system devices and components, safety instrumented systems, Internet of things (IoT) devices, industrial Internet of things (IIoT) devices, supervisory control and data acquisition (SCADA) system devices and components, network and communications assets, and assets residing in the cloud. Information assets are produced and used by IT, OT, and people to support the delivery of the function. Examples of information assets include customer data, financial records, firewall configuration files, security information and event management (SIEM) log files, historian data, SCADA set points, and configuration files. When evaluating whether a practice is performed completely, all forms of assets that the function relies on should be considered.

To ensure a comprehensive evaluation, organizations should account for all types of assets that may be in scope for the self-evaluation, such as virtualized assets, regulated assets, cloud assets, and mobile assets. Additionally, each type of asset may have several unique variations. For example, cloud assets may include software as a service, platform as a service, infrastructure as a service, etc., and may be public, private, or hybrid.

Additionally, C2M2 refers to two other groupings of assets: assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective.

Assets that are important to the delivery of the function includes assets that are required for a normal state of operation of the function and output of the function's products or services. Loss of an asset that is considered important to the delivery of the function may not directly result in an inability to deliver the function but could result in operations being degraded. Identification of an important asset should focus on loss of the service or role performed by that asset and should not include consideration of asset redundancy or other protections applied to assets.

Assets within the function that may be leveraged to achieve a threat objective includes assets that may be used in the pursuit of the tactics or goals of a threat actor. Identification of assets within the function that may be leveraged to achieve a threat objective should focus on the techniques used by threat actors and assets that may be targeted or leveraged by threat actors. These are some examples of assets within the function that may be leveraged to accomplish a threat objective:

- public-facing assets that may serve as an initial access point
- individual systems that would allow lateral movement within an organization's network
- systems with administrative rights that would enable privilege escalation
- information such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed

Note that an organization's list of assets that are important to the delivery of the function might include assets within the function that may be leveraged to achieve a threat objective and vice versa. Identifying assets within the function that may be leveraged to achieve a threat objective enables the organization to view assets from the perspective of a threat actor. It is not the intention of the model that *all* assets be categorized as assets that might be leveraged to achieve a threat objective, but only those that a risk-based approach identifies as being worthy of attention and further analysis.

Because the assets noted above are the focus of a number of practices in C2M2, identifying which assets will be in scope for use of the C2M2 in advance of an evaluation will improve the pace and the accuracy of the evaluation.

4. 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.

4.1 Domains, Objectives, and Practices

The C2M2 includes 342 cybersecurity practices, which are grouped into 10 domains. These practices represent the activities an organization 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 an organization 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 Asset Configuration
4. Manage Changes to Assets
5. Management Activities

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 2 summarizes the elements of each domain.

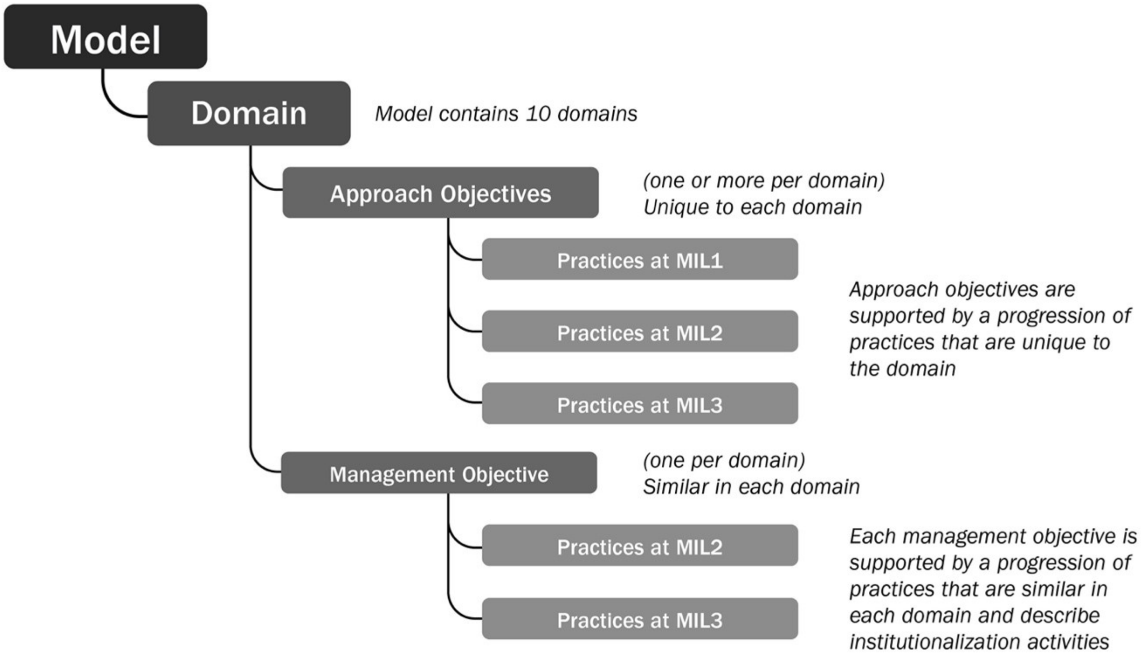

Model
Domain
Model contains 10 domains
Approach Objectives
(one or more per domain)
Unique to each domain
Practices at MIL1
Practices at MIL2
Practices at MIL3
Approach objectives are supported by a progression of practices that are unique to the domain
Management Objective
(one per domain)
Similar in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

Figure 2: Model and Domain Elements

For each domain, the model provides a purpose statement, which is a high-level summary of the intent of the domain, followed by introductory notes, which give context for the domain and introduce its practices. The purpose statement and introductory notes offer context for interpreting the practices in the domain.

The purpose statement for each of the 10 domains follows in the order in which the domains appear in the model. Next to each of the domain names, a short name is provided that is used throughout the model.

Asset, Change, and Configuration Management (ASSET)

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

Threat and Vulnerability Management (THREAT)

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.

Risk Management (RISK)

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.

Identity and Access Management (ACCESS)

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.

Situational Awareness (SITUATION)

Establish and maintain activities and technologies to collect, 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.

Event and Incident Response, Continuity of Operations (RESPONSE)

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.

Third-Party Risk Management (THIRD-PARTIES)

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.

Workforce Management (WORKFORCE)

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.

Cybersecurity Architecture (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.

Cybersecurity Program Management (PROGRAM)

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.

4.2 Maturity Indicator Levels

The model defines four maturity indicator levels (MILs), MIL0 through MIL3, which apply independently to each domain in the model. The MILs define a dual progression of maturity: an approach progression and a management progression, which are explained in the following sections.

Four aspects of the MILs are important for understanding and applying the model.

- The maturity indicator levels apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings in different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
- 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 must perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
- Establishing a target MIL for each domain is an effective strategy for using the model to guide cybersecurity program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Then, they can focus gap analysis activities and improvement efforts on achieving those target levels.
- Practice performance and MIL achievement need to align with business objectives and the organization’s cybersecurity program strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL versus its potential benefits. However, the model was designed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

4.2.1 Summary of MIL Characteristics

Table 4 summarizes the characteristics of each MIL. At MIL2 and MIL3, the characteristic associated with the approach progression is distinguished from the characteristics associated with the management progression.

Table 3: Summary of Maturity Indicator Level Characteristics

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Personnel performing the practices have adequate skills and knowledge • Responsibility, accountability, and authority for performing the practices are assigned • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

4.3 Approach Progression

The domain-specific objectives and practices describe the progression of the approach to cybersecurity for each domain in the model. Approach refers to the completeness, thoroughness, or level of development of an activity in a domain. As an organization progresses from one MIL to the next, it will have more complete or more advanced implementations of the core activities in the domain. At MIL1, while only the initial set of practices for a domain is expected, an organization is not precluded from performing additional practices at higher MILs.

To achieve MIL1, these initial activities may be performed in an ad hoc manner, but they must be performed. If an organization were to start with no capability in managing cybersecurity, it should focus initially on implementing the MIL1 practices.

In the context of the model, *ad hoc* (that is, formed or used for a special purpose without policy or a plan for repetition) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much organizational guidance, such as a prescribed plan, policy, or training. The quality of the outcome may vary significantly depending on who performs the practice, when it is performed, the context of the problem being addressed, the methods, tools, and techniques used, and the priority given a particular instance of the practice. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, at this MIL, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization. It is important to note that, while documented policies or procedures are not essential to the performance of a practice in an ad hoc manner, the effective performance of many practices would result in documented artifacts such as a documented asset inventory or a documented cybersecurity program strategy.

Table 5 provides an example of the approach progression, Objective 1, in the Asset, Change, and Configuration Management domain. At MIL1, an inventory of IT and OT assets exists in any form and only for assets that are important to the delivery of the function. MIL2 adds more requirements to the inventory, including additional assets beyond those important to the delivery of the function and asset attributes. Finally, in addition to requiring performance of all MIL1 and MIL2 practices, MIL3 requires that the inventory includes all assets used for the delivery of the function and is updated based on defined triggers.

Table 4: Example of Approach Progression in the ASSET Domain

1. Manage IT and OT Asset Inventory

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

4.4 Management Progression

The management progression describes the extent to which a practice or activity is ingrained in an organization’s operations (or *institutionalized*). The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the practice over time, the practice will be retained under times of stress, and the outcomes of the practice will be consistent, repeatable, and of high quality.

The progression of imbedding an activity in an organization’s operations is described by a set of practices that can be performed to institutionalize the domain-specific practices. These practices are similar across domains and are called the Management Activities. Table 6 provides an example of the Management Activities in the ASSET domain.

Table 5: Example of Management Activities in the ASSET Domain

5. Management Activities

MIL1	No practice at MIL1
MIL2	a. Documented procedures are established, followed, and maintained for activities in the ASSET domain b. Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain
MIL3	c. Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain d. Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities e. Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel f. The effectiveness of activities in the ASSET domain is evaluated and tracked

4.5 Example Lists Included in Practices

Several practices within the domains include lists of examples to help illustrate the meaning of the practices. These example lists appear in line with practice text and are introduced by parenthetical statements "(for example,…)" or with the phrase "such as." The purpose of these example lists is to better communicate the intended meaning of practices. Example lists should not be interpreted as a description of how a practice should be implemented. Each organization and function to which the model is applied is likely to have a unique risk profile and operating environment, and so the provided examples may not be applicable to all organizations and functions. Users of the C2M2 may leverage example lists to generate ideas about what considerations may be applicable, but should not interpret an example lists as indicating a minimum baseline or as an exhaustive list of what might be considered for implementation of a practice.

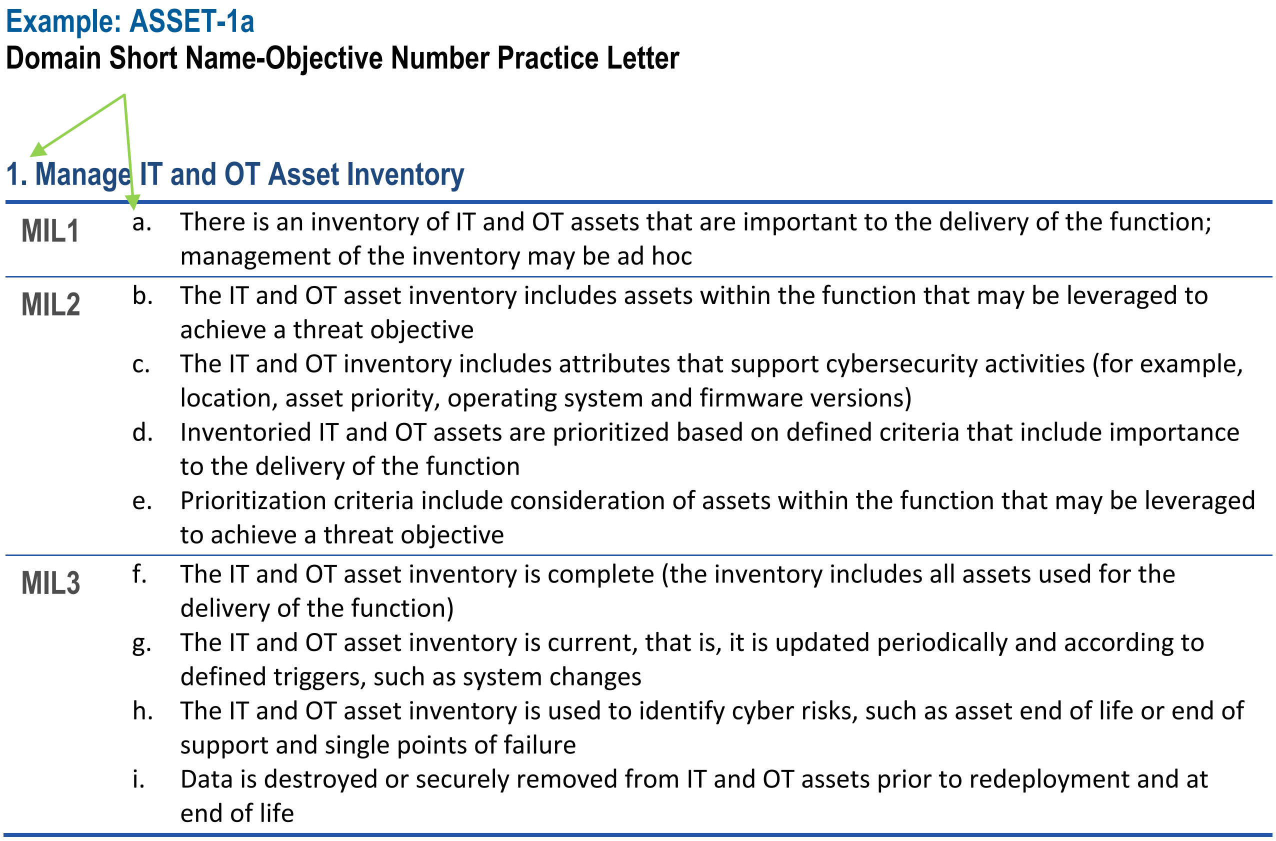
Example: ASSET-1c

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

Figure 3: Example List in Practice ASSET-1c

4.6 Practice Reference Notation

A number of practices within the domains are related to other model practices. When this occurs, the related practice is referenced using a notation that begins with the domain short name, a hyphen, the objective number, and the practice letter. Figure 4 shows an example from the first objective in the Asset, Change, and Configuration Management domain. The objective's first practice, "There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc," would be referenced elsewhere in the model using the notation "ASSET-1a."



Example: ASSET-1a

Domain Short Name-Objective Number Practice Letter

1. Manage IT and OT Asset Inventory

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

Figure 4: Example of Referencing an Individual Practice: ASSET-1a

5. USING THE MODEL

The C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. Figure 5 summarizes a potential approach for using the model. An organization performs an evaluation against the model, uses that 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.

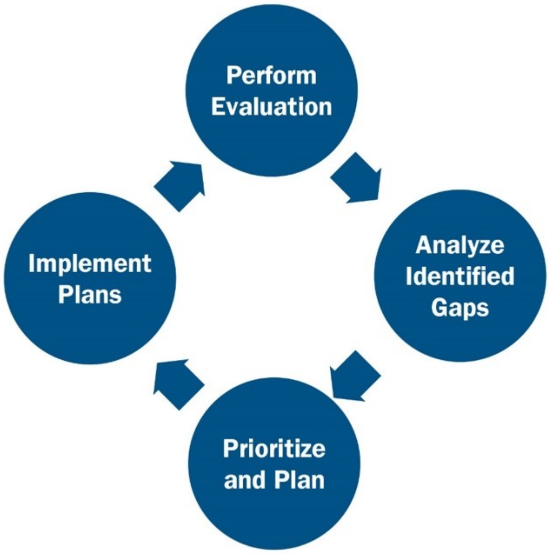


Figure 5: Potential Approach for Using the Model

5.1 Step 1: Perform an Evaluation

Performing a C2M2 self-evaluation provides a measurement of the implementation of cybersecurity activities within an organization. A design goal of the model is to enable organizations to complete a self-evaluation for a single function in one day without extensive study or preparation. To begin preparation, the organization first establishes the scope of the model application, or the *function*. Next, the organization should identify IT, OT, and information assets that are important to the delivery of the function.

The organization should select the appropriate personnel to evaluate the in scope function against the model practices. An effective facilitator who is familiar with model content should be identified to guide the self-evaluation. Participation by stakeholders from across the organization yields the best results and enables internal information sharing about the model practices. Personnel selected to participate in the self-evaluation should include operational personnel, management stakeholders, and any others who could provide useful information on the organization's performance of cybersecurity practices in the model. Through open dialog and consensus, self-evaluation workshop participants decide on an implementation level for the practices in each domain. Responses are chosen from a four-point scale: Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented. Table 6 includes a description for each self-evaluation response option.

Table 6: Description of Self-Evaluation Response Options

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

Responses are recorded using one of the free C2M2 self-evaluation tools available from the DOE[9] or using another tool. Upon completion of the self-evaluation, a scoring report is generated that provides summary-level depictions of performance relative to the model, as well as practice-level implementation status. This report provides a point-in-time view of the cybersecurity posture of the in-scope function. The report should be reviewed with the self-evaluation workshop participants, and any discrepancies or questions should be addressed. More thorough guidance on using the model, selecting a facilitator, and scoping the evaluation can be found in the supporting *C2M2 Self-Evaluation Guide*.[10]

5.2 Step 2: Analyze Identified Gaps

The scoring report from the self-evaluation will identify gaps in the performance of model practices. The first analysis step for the organization is to determine whether these gaps are meaningful and important for the organization to address.

It is not typically optimal for an organization to strive to achieve the highest MIL in all domains. Rather, the organization should determine the level of practice performance and MIL achievement for each domain that best enables it to meet its business objectives and cybersecurity strategy. The organization should identify its desired capability profile—a target MIL rating for each domain in the model. This collection of desired capabilities is the organization's target profile.

[9] The C2M2 self-evaluation tools may be obtained by sending a request to C2M2@hq.doe.gov or by visiting https://www.energy.gov/C2M2.
[10] The *C2M2 Self-Evaluation Guide* may be downloaded from https://www.energy.gov/C2M2.

For organizations using the model for the first time, a target profile is typically identified after the initial self-evaluation. This gives the organization an opportunity to develop more familiarity with the model. Organizations that have more experience with the model have often identified a target profile before undergoing an evaluation. The appropriate organizational stakeholders should select the target profile. This might be a single individual with expertise in the function's operations and management, but it is likely to be a collection of individuals.

The target profile can then be examined against the results from the self-evaluation workshop to identify gaps that are important to the organization because they represent differences from the desired capability profile.

5.3 Step 3: Prioritize and Plan

After the gap analysis is complete, the organization should prioritize the actions needed to fully implement the practices that enable achievement of the desired capability in specific domains. The prioritization should be done using criteria such as how gaps affect organizational objectives, the importance of the business objective supported by the domain, the cost of implementing the necessary practices, and the availability of resources to implement the practices. A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed.

Next, a plan should be developed to address the selected gaps. Planning should follow standard organizational planning processes and align to the strategic objectives of the organization and cybersecurity program. These plans can span a period of weeks, months, or years, depending on the extent of improvements needed to close the selected gaps and achieve the desired capability. An individual with sufficient authority to carry out the plan should be identified and assigned as the plan owner. Regular reviews by organizational leadership should be conducted to evaluate status, clear obstacles, and identify any necessary course corrections as implementation progresses.

5.4 Step 4: Implement Plans and Periodically Reevaluate

Plans developed in the previous step should be implemented to address the identified gaps. Model self-evaluations are particularly useful in tracking implementations 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 organization's desired state.

Table 7: Inputs, Activities, and Outputs: Breakdown of Potential Approach

	Inputs	Activities	Outputs
1. Perform Evaluation	1. C2M2 self-evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct C2M2 self-evaluation workshop with appropriate attendees	C2M2 self-evaluation report
2. Analyze Identified Gaps	1. C2M2 self-evaluation report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
3. Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Conduct cost-benefit analysis (CBA) on actions 3. Prioritize actions 4. Plan to implement prioritized actions	Prioritized implementation plan
4. Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

6. MODEL DOMAINS

6.1 Asset, Change, and Configuration Management (ASSET)

Purpose: 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.

An asset is something of value to an organization. For the purposes of the 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 cyber 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 and ensuring that 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.

Example: Asset Change and Configuration Management

Anywhere Inc. identifies and prioritizes IT, OT, and information assets based on importance to the generation function. This information is stored in an asset database that includes attributes to support cybersecurity activities. Attributes include asset priority, hardware and software versions, physical location, cybersecurity requirements (business needs for the asset's confidentiality, integrity, and availability), category based on the sensitivity of the asset, asset owner, and version of applied configuration baseline.

Anywhere Inc. uses this information for cyber risk management activities, including identifying which systems may be affected by software vulnerabilities, prioritizing cybersecurity incident response, and planning disaster recovery.

To maintain change traceability and consistency, Anywhere Inc.'s change management activities ensure that the asset database remains current as configurations change. All important decisions about assets are communicated to stakeholders, including the asset owner, so that potential impacts to the function are efficiently managed.

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.

Objectives and Practices

1. Manage IT and OT Asset Inventory

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

2. Manage Information Asset Inventory

MIL1	a.	There is an inventory of information assets that are important to the delivery of the function (for example, SCADA set points and customer information); management of the inventory may be ad hoc
MIL2	b.	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective
	c.	The information asset inventory includes attributes that support cybersecurity activities (for example, backup locations and frequencies, storage locations, cybersecurity requirements)
	d.	Inventoried information assets are categorized based on a defined scheme that includes importance to the delivery of the function
	e.	Categorization criteria include consideration of assets within the function that may be leveraged to achieve a threat objective

2. Manage Information Asset Inventory (continued)

MIL3

f. The information asset inventory is complete (the inventory includes all assets used for the delivery of the function)
g. The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes
h. The information asset inventory is used to identify cyber risks, such as risk of disclosure, risk of destruction, and risk of tampering
i. Information assets are sanitized or destroyed at the end of life using techniques appropriate to their cybersecurity requirements

3. Manage Asset Configuration

MIL1

a. Configuration baselines are established, at least in an ad hoc manner

MIL2

b. Configuration baselines are used to configure assets at deployment and restoration

MIL3

c. The design of configuration baselines includes cybersecurity objectives
d. Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1e)
e. Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles
f. Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture

4. Manage Changes to Assets

MIL1

a. Changes to inventoried assets are evaluated and approved before being implemented, at least in an ad hoc manner
b. Changes to inventoried assets are logged, at least in an ad hoc manner

MIL2

c. Changes to assets are tested prior to being deployed
d. Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)

MIL3

e. Changes to assets are tested for cybersecurity impact prior to being deployed
f. Change logs include information about modifications that impact the cybersecurity requirements of assets

5. Management Activities

MIL1

No practice at MIL1

MIL2

a. Documented procedures are established, followed, and maintained for activities in the ASSET domain
b. Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain

5. Management Activities (continued)

MIL3	c.	Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain
	d.	Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel
	f.	The effectiveness of activities in the ASSET domain is evaluated and tracked

6.2 Threat and Vulnerability Management (THREAT)

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 (such as critical, IT, and 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, 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:

1. Reduce Cybersecurity Vulnerabilities
2. Respond to Threats and Share Threat Information
3. Management Activities

Example: Threat and Vulnerability Management

Anywhere Inc. examined the types of threats that it normally responds to, including malicious software, denial-of-service attacks, and activist cyber-attack groups. This information has been used to develop Anywhere Inc.'s documented threat profile. Anywhere Inc. has identified reliable sources of information to enable rapid threat identification and is able to consume and analyze published threat information from sources such as the Cybersecurity and Infrastructure Security Center (CISA), Information Sharing and Analysis Centers (ISACs), and industry associations, and begin effective response.

When reducing cybersecurity vulnerabilities, Anywhere Inc. uses the Forum of Incident Response and Security Teams (FIRST) Common Vulnerability Scoring System (CVSS) to better identify the potential impacts of known software vulnerabilities. This allows the organization to prioritize reduction activities according to the importance of the vulnerabilities.

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 asset to the delivery of the function. Vulnerabilities may be addressed by implementing mitigating controls, monitoring threat status, applying cybersecurity patches, replacing outdated equipment, or performing other activities.

Objectives and Practices

1. Reduce Cybersecurity Vulnerabilities

MIL1	a.	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner
	b.	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner
	c.	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner
	d.	Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner
MIL2	e.	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored (ASSET-1d)
	f.	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events
	g.	Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly
	h.	Operational impact to the function is evaluated prior to deploying patches
	i.	Information on any discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders
MIL3	j.	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function
	k.	Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management program for response
	l.	Vulnerability monitoring activities include review and confirmation of actions taken in response to cybersecurity vulnerabilities where appropriate

2. Respond to Threats and Share Threat Information

MIL1	a.	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner
	b.	Cybersecurity threat information is gathered and interpreted for the function, at least in an ad hoc manner
	c.	Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner
MIL2	d.	A threat profile for the function is established (for example, characterization of potential threat actors, motives, intent, capabilities, and targets)
	e.	Threat information sources that collectively address all components of the threat profile are prioritized and monitored
	f.	Identified threats are analyzed and prioritized and are addressed accordingly
	g.	Threat information is exchanged with stakeholders (for example, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs], internal entities) based on risk to critical infrastructure

2. Respond to Threats and Share Threat Information (continued)

MIL3

h. The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events

i. Threats that pose ongoing risk to the function are referred to the risk management program for action

j. Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3h)

k. Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action

3 Management Activities

MIL1

No practice at MIL1

MIL2

a. Documented procedures are established, followed, and maintained for activities in the THREAT domain

b. Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain

MIL3

c. Up-to-date policies or other organizational directives define requirements for activities in the THREAT domain

d. Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities

e. Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel

f. The effectiveness of activities in the THREAT domain is evaluated and tracked

6.3 Risk Management (RISK)

Purpose: 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.

Cyber risk is defined as the possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. Cyber risk is one component of the overall 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:

1. Establish and Maintain Cyber Risk Management Strategy and Program
2. Identify Cyber Risk
3. Analyze Cyber Risk
4. Respond to Cyber Risk
5. Management Activities

Managing cyber risk involves framing, identifying and 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. A cyber risk management strategy provides direction for analyzing and prioritizing cyber risk and defines risk tolerance. The cyber risk management strategy may include a risk analysis methodology, risk monitoring strategy, and a description of how the cyber risk program will be governed. 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.

Example: Risk Management

Anywhere Inc. has developed an enterprise risk management strategy that identifies its risk tolerance and strategy for assessing, responding to, and monitoring cyber risks. The Board of Directors reviews this strategy annually to ensure that it remains aligned with the strategic objectives of the organization.

Within this program, risk tolerances, including compliance risk and risk to the delivery of essential services, are identified and documented. Identified risks are recorded in a risk register to ensure that they are monitored and responded to in a timely manner and to identify trends.

Anywhere Inc. uses information from their current cybersecurity architecture to analyze how critical assets are connected and which ones are exposed to the Internet. Resources like Web servers that take requests from the Internet are considered at higher risk than those that do not. Assets that directly support other assets with direct exposure, like the database server behind a Web server, are in the second risk tier and so on. An asset's base risk is then refined depending on how it is protected by security controls.

The final risk for each asset is a combination of the asset's importance in delivering essential services and its exposure based on the network and cybersecurity architectures.

Risks are identified, categorized, and prioritized in a way that helps the organization consistently respond to and monitor risks. A risk register—a list of identified risks and associated attributes—also facilitates this process. Consolidation of risks into categories enables the organization to develop a risk register that is reflective of the current risk environment and can be managed effectively with available resources. Other domains in the model (Situational Awareness, Event and Incident Response, Continuity of Operations, and Cybersecurity Architecture) refer to risk practices and illustrate how the practices in the model are strengthened as they connect through a cyber risk management program. And information generated through activities in the Threat and Vulnerability Management and Third-Party Risk Management domains is used to update cyber risks and identify new risks.

Objectives and Practices

1. Establish and Maintain Cyber Risk Management Strategy and Program

MIL1	a.	The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner
MIL2	b.	A strategy for cyber risk management is established and maintained to support the organization’s cybersecurity program strategy (PROGRAM-1b) and enterprise architecture
	c.	Information from RISK domain activities is communicated to relevant stakeholders
	d.	Governance for the cyber risk management program is established and maintained
MIL3	e.	A cyber risk management program is established and maintained to implement and perform activities in the RISK domain in alignment with the organization’s mission and objectives
	f.	The cyber risk strategy and program activities are coordinated with the organization’s enterprise-wide risk management strategy and program

2. Identify Cyber Risk

MIL1	a.	Cyber risks are identified, at least in an ad hoc manner
MIL2	b.	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level
	c.	Cyber risk identification leverages multiple risk identification techniques and information sources
	d.	Stakeholders from appropriate operations and business areas participate in the identification of cyber risks
	e.	Cyber risk categories and cyber risks are documented in a risk register or other artifact
	f.	Cyber risk categories and cyber risks are assigned to risk owners
	g.	Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events
MIL3	h.	Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain
	i.	Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from new or unmitigated vulnerabilities)
	j.	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks
	k.	Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks
	l.	Conformance gaps between as built systems and networks and the cybersecurity architecture are used to update cyber risks and identify new risks (ARCHITECTURE-1h)
	m.	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interconnected organizations

3. Analyze Cyber Risk

MIL1	a.	Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner
MIL2	b.	Defined criteria are used to prioritize cyber risk categories and cyber risks (for example, impact, likelihood, susceptibility, risk tolerance)
	c.	A defined method is used to estimate impact for higher priority cyber risk categories and cyber risks (for example, comparison to actual events, risk quantification)
	d.	Defined methods are used to analyze higher priority cyber risk categories and cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility)
	e.	Organizational stakeholders from appropriate operations and business functions support the analysis of higher priority cyber risk categories and cyber risks
	f.	Cyber risk categories and cyber risks are retired when they no longer require tracking or response
MIL3	g.	Cyber risk analyses are updated periodically and according to defined triggers, such as system changes and external events

4. Respond to Cyber Risk

MIL1	a.	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and cyber risks, at least in an ad hoc manner
MIL2	b.	A defined method is used to select and implement risk responses based on analysis and prioritization
MIL3	c.	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks
	d.	Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated and risk tolerances are not exceeded
	e.	Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate

5. Management Activities

MIL1	No practice at MIL1	
MIL2	a.	Documented procedures are established, followed, and maintained for activities in the RISK domain
	b.	Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain

5. Management Activities (continued)

MIL3

c. Up-to-date policies or other organizational directives define requirements for activities in the RISK domain

d. Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities

e. Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel

f. The effectiveness of activities in the RISK domain is evaluated and tracked

6.4 Identity and Access Management (ACCESS)

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 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 cyber risks.

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

1. Establish and Maintain Identities
2. Control Logical Access
3. Control Physical Access
4. 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.

Example: Identity and Access Management

Anywhere Inc. decides to migrate multiple identity and access management (IAM) systems to a system that is capable of supporting multifactor authentication. The organization believes that reducing the number of IAM systems that it manages will enable more effective access management.

As Anywhere Inc. prepares to migrate legacy systems to the new IAM system, it discovers that some former employees still have active accounts, some current employees have more access than is required for their role, and some employees who have changed roles within the organization still have active accounts on systems to which they no longer require access.

Anywhere Inc. updates its identity management processes to include coordination with the organization's HR processes to help ensure that whenever a user changes roles or leaves the organization, his or her access will be reviewed and updated appropriately.

Anywhere Inc. also institutes a quarterly review to ensure that access granted to the organization's assets aligns with access requirements.

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. 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.

Objectives and Practices

1. Establish and Maintain Identities

MIL1	a.	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities)
	b.	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner
	c.	Identities are deprovisioned, at least in an ad hoc manner, when no longer required
MIL2	d.	Identity repositories are reviewed and updated to ensure accuracy, periodically and according to defined triggers, such as system changes and changes to organizational structure
	e.	Identities are deprovisioned within organization-defined time thresholds when no longer required
	f.	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)

2. Control Logical Access

MIL1	a.	Logical access controls are implemented, at least in an ad hoc manner
	b.	Logical access is revoked when no longer needed, at least in an ad hoc manner
MIL2	c.	Logical access requirements are determined (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters)
	d.	Logical access requirements incorporate the principle of least privilege
	e.	Logical access requirements incorporate separation of duties
	f.	Logical access requests are reviewed and approved by the asset owner
	g.	Logical access that poses higher risk to the function receives additional scrutiny and monitoring
MIL3	h.	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges
	i.	Anomalous access attempts are monitored as indicators of cybersecurity events

3. Control Physical Access

MIL1	a.	Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner
	b.	Physical access is revoked when no longer needed, at least in an ad hoc manner
	c.	Physical access logs are maintained, at least in an ad hoc manner
MIL2	d.	Physical access requirements are determined (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)
	e.	Physical access requirements incorporate the principle of least privilege
	f.	Physical access requests are reviewed and approved by the asset owner
	g.	Physical access that poses higher risk to the function receives additional scrutiny and monitoring
MIL3	h.	Physical access privileges are reviewed and updated
	i.	Physical access is monitored to identify potential cybersecurity events

4. Management Activities

MIL1	No practice at MIL1	
MIL2	a.	Documented procedures are established, followed, and maintained for activities in the ACCESS domain
	b.	Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain
MIL3	c.	Up-to-date policies or other organizational directives define requirements for activities in the ACCESS domain
	d.	Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel
	f.	The effectiveness of activities in the ACCESS domain is evaluated and tracked

6.5 Situational Awareness (SITUATION)

Purpose: 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.

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:

1. Perform Logging
2. Perform Monitoring
3. Establish and Maintain Situational Awareness
4. 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, security, and threat 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

Example: Situational Awareness

Anywhere Inc. monitors its important systems for unusual activity that may indicate cyber events. Additionally, personnel monitor a number of resources that provide reliable cybersecurity information, including its vendors and NCCIC.

Further, Anywhere Inc. determined that indicators of an emerging threat often reside in different parts of the organization. Building security tracks visitors, the helpdesk responds to strange laptop behavior, shipping knows about packages, and the security team monitors network events and external sources. Each day, the security team gathers information from other departments, adds their own data, and produces a situational awareness report for the rest of the organization. Situational awareness reports may summarize the current state of operations using a color-coded scale and be posted on the wall of the control room as well as on the corporate intranet site.

When the situational awareness suggests a need for heighted security, visitors are screened more carefully, the IT helpdesk conducts malware scans on misbehaving laptops, and IT Security sends out reminders about phishing. Senior management can review the situational awareness information and be prepared should extraordinary action—for example, shutting down the website—be required. At the highest state of alert, firewall rule sets can be changed to restrict nonessential protocols, such as video conferencing, to delay non-emergency change requests, and put the cybersecurity incident response team on standby.

other graphical displays, they are not necessarily required to achieve the goal.

Objectives and Practices

1. Perform Logging

MIL1	a.	Logging is occurring for assets important to the delivery of the function, at least in an ad hoc manner (ASSET-1a, ASSET-2a)
MIL2	b.	Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible
	c.	Logging requirements are established and maintained for assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)
	d.	Log data are being aggregated within the function
MIL3	e.	More rigorous logging is performed for higher priority assets (ASSET-1d)

2. Perform Monitoring

MIL1	a.	Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner
	b.	IT and OT environments are monitored for anomalous activity that may indicate a cybersecurity event, at least in an ad hoc manner
MIL2	c.	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data
	d.	Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments
	e.	Alarms and alerts are configured and maintained to support the identification of cybersecurity events
	f.	Monitoring activities are aligned with the threat profile (THREAT-2d)
MIL3	g.	More rigorous monitoring is performed for higher priority assets (ASSET-1d)
	h.	Continuous monitoring is performed across IT and OT environments to identify anomalous activity
	i.	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity
	j.	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events

3. Establish and Maintain Situational Awareness

MIL1	No practice at MIL1
MIL2	a. Methods of communicating the current state of cybersecurity for the function are established and maintained b. Monitoring data are aggregated to provide an understanding of the operational state of the function c. Relevant information from across the organization is available to enhance situational awareness
MIL3	d. Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders e. Monitoring data are aggregated and analyzed to provide near-real-time understanding of the cybersecurity state of the function f. Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness g. Procedures are in place to analyze received cybersecurity information in support of situational awareness h. Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains (THREAT-2j, RESPONSE-3k)

4. Management Activities

MIL1	No practice at MIL1
MIL2	a. Documented procedures are established, followed, and maintained for activities in the SITUATION domain b. Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain
MIL3	c. Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain d. Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities e. Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel f. The effectiveness of activities in the SITUATION domain is evaluated and tracked

6.6 Event and Incident Response, Continuity of Operations (RESPONSE)

Purpose: 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.

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 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:

1. Detect Cybersecurity Events
2. Analyze Cybersecurity Events and Declare Incidents
3. Respond to Cybersecurity Events and Incidents
4. Address Cybersecurity in Continuity of Operations
5. 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. Cybersecurity events may originate with or impact third parties necessitating coordination in response planning, execution, and communications.

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.

Example: Event and Incident Response, Continuity of Operations

Anywhere Inc. purchased a helpdesk tracking system to log and track important cybersecurity events. On the wall in their shared working area, Anywhere Inc. posted a chart that identifies criteria for declaring cybersecurity incidents, which are based on potential impact to Anywhere's most important systems. When the organization experiences a cybersecurity incident, the incident response plan requires that the incident be logged and communicated to key stakeholders. The reporting process includes those responsible for communicating the current state of cybersecurity for the function as described in the Situational Awareness domain.

Anywhere Inc. tests its incident response plan annually to ensure that its procedures are adequately addressing all phases of the incident lifecycle.

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.

Objectives and Practices

1. Detect Cybersecurity Events

MIL1	a.	Detected cybersecurity events are reported to a specified person or role and logged, at least in an ad hoc manner
MIL2	b.	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)
	c.	Cybersecurity events are logged based on the established criteria
MIL3	d.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features
	e.	Cybersecurity event detection activities are adjusted based on identified risks (RISK-2a) and the organization’s threat profile (THREAT-2d)
	f.	Situational awareness for the function is monitored to support the identification of cybersecurity events

2. Analyze Cybersecurity Events and Declare Incidents

MIL1	a.	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner
	b.	Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner
MIL2	c.	Cybersecurity incident declaration criteria are formally established based on the potential impact to the function
	d.	Cybersecurity events are declared to be incidents based on established criteria
	e.	Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats
	f.	There is a repository where cybersecurity events and incidents are logged and tracked to closure
	g.	Cybersecurity stakeholders (for example, government, connected organizations, vendors, sector organizations, regulators, and internal entities) are identified and notified of events and incidents based on situational awareness reporting requirements (SITUATION-3d)

2. Analyze Cybersecurity Events and Declare Incidents (continued)

MIL3

h. Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b)

i. Cybersecurity incidents are correlated to support the discovery of patterns, trends, and other common features

3. Respond to Cybersecurity Events and Incidents

MIL1

a. Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner

b. Responses to cybersecurity events and incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations

c. Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner

MIL2

d. Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained

e. Cybersecurity event and incident response is executed according to defined plans and procedures

f. Cybersecurity event and incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events

g. Cybersecurity event and incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan

MIL3

h. Cybersecurity event and incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan

i. Cybersecurity event and incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation

j. Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations

k. Cybersecurity event and incident responses leverage and trigger predefined states of operation (SITUATION-3h)

4. Address Cybersecurity in Continuity of Operations

MIL1

a. Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner

b. Data backups are available and tested, at least in an ad hoc manner

c. IT and OT assets requiring spares are identified, at least in an ad hoc manner

MIL 2

d. An analysis of the impacts from potential cybersecurity events informs the development of continuity plans

e. The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans

f. Continuity plans address IT, OT, and information assets important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets (ASSET-1a, ASSET-2a)

g. Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events

4. Address Cybersecurity in Continuity of Operations (continued)

MIL 2	h. Data backups are protected with at least the same controls as source data i. Data backups are logically or physically separated from source data j. Spares for selected IT and OT assets are available k. Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets important to the delivery of the function are incorporated into continuity plans (ASSET-1a, ASSET-2a) l. Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel
MIL 3	m. Continuity plans are aligned with identified risks (RISK-2a) and the organization's threat profile (THREAT-2d) to ensure coverage of identified risk categories and threats n. Continuity plan exercises address higher priority risks (RISK-3a) o. The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly p. Cybersecurity incident content within continuity plans is periodically reviewed and updated q. Continuity plans are periodically reviewed and updated

5. Management Activities

MIL1	No practice at MIL1
MIL2	a. Documented procedures are established, followed, and maintained for activities in the RESPONSE domain b. Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain
MIL3	c. Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain d. Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities e. Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel f. The effectiveness of activities in the RESPONSE domain is evaluated and tracked

6.7 Third-Party Risk Management (THIRD-PARTIES)

Purpose: 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.

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

The model classifies third-party dependencies as external parties on which the delivery of the function depends, including operating partners. These relationships may vary in importance because the function may have a greater reliance on specific third parties, particularly if a third party has access to, control of, or custody of an asset. Third parties include entities such as suppliers, vendors, service providers, infrastructure dependencies (e.g., telecommunications, water), and governmental organizations (e.g., emergency response services, federal 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.

Example: Third-Party Risk Management

Anywhere Inc. receives products and services from multiple vendors. Recently, the organization began to work with a new vendor that, during the normal course of business, will have access to sensitive data and systems.

Within the contract for the project, Anywhere Inc. mandated the nondisclosure of sensitive data. Anywhere Inc. also specified cybersecurity requirements for the handling, communication, and storage of its information, requiring that it would be encrypted both in transit and in storage. The cybersecurity requirements also stated that passwords and cryptographic keys would be properly managed, and they specified strict limits and controls on the vendor personnel and systems that will have access to Anywhere Inc.'s systems and data during deployment, operations, and maintenance. Additionally, Anywhere Inc. conducted a review of the vendor's practices (including the vendor's cybersecurity practices with respect to its suppliers), participated in a security design review of the vendor's proposed system, and plans to conduct periodic audits of the delivered system to ensure that the vendor continues to meet its obligations.

When the vendor supplied equipment, Anywhere Inc. carried out an inspection to verify that the hardware, software, and firmware were authentic and that initial configurations were as agreed upon. To accomplish this, Anywhere Inc. conducted random sample audits, which included visually confirming serial numbers with the hardware manufacturer (to help detect counterfeits), verifying digital signatures for associated software and firmware, and checking initial configuration settings for conformance.

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

1. Identify and Prioritize Third Parties
2. Manage Third-Party Risk
3. Management Activities

Identifying third parties involves establishing and maintaining a comprehensive understanding of the key external relationships required for the delivery of the function. After identification, third parties should be prioritized to determine which third-party dependencies are most critical to the delivery of the function. Prioritization criteria should consider the risk to the function that is introduced by third-party relationships.

Managing third-party 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 cyber 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.

Objectives and Practices

1. Identify and Prioritize Third Parties

MIL1	a.	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner
	b.	Third parties that have access to, control of, or custody of any IT, OT, or information assets important to the delivery of the function are identified, at least in an ad hoc manner
MIL2	c.	Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts)
	d.	Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access)
MIL3	e.	Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events

2. Manage Third-Party Risk

MIL1

a. The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner

b. The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner

MIL2

c. A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties

d. A defined method is followed to evaluate and select suppliers and other third parties

e. More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties

f. Cybersecurity requirements are formalized in agreements with suppliers and other third parties where applicable

g. Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements

MIL3

h. Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate

i. Selection criteria include consideration of end-of-life and end-of-support timelines

j. Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services

k. Acceptance testing of procured assets includes testing for cybersecurity requirements

3. Management Activities

MIL1

No practice at MIL1

MIL2

a. Documented procedures are established, followed, and maintained for activities in the THIRD-PARTIES domain

b. Adequate resources (people, funding, and tools) are provided to support activities in the THIRD-PARTIES domain

MIL3

c. Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain

d. Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities

e. Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel

f. The effectiveness of activities in the THIRD-PARTIES domain is evaluated and tracked

6.8 Workforce Management (WORKFORCE)

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:

1. Assign Cybersecurity Responsibilities
2. Develop Cybersecurity Workforce
3. Implement Workforce Controls
4. Increase Cybersecurity Awareness
5. 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. Cybersecurity responsibilities are not restricted to traditional IT roles; for example, engineers, control room operators, and field technicians 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

Example: Workforce Management

Anywhere Inc. determines that it will invest in advanced digital technology. Part of this investment will be a long-term program for workforce training and management to help personnel keep the new systems running efficiently and securely. Anywhere Inc. finds it much harder than expected to recruit, train, and retain personnel with the necessary skill sets, particularly personnel with cybersecurity education and experience. Furthermore, the organization finds that its brand of new digital technology has been compromised at another company due to poor security practices.

Anywhere Inc. analyzes this information through a risk management assessment of its systems, practices, and policies. The organization determines that employee training is paramount to addressing system and social engineering vulnerabilities as well as insider threats to the company's goals and objectives. As a result, Anywhere Inc. begins investing in technical and security training and certification for management and personnel to instill the awareness and skills necessary to manage and protect the company's assets, which may also contribute to the protection of interconnected critical infrastructure external to the organization.

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.

Objectives and Practices

1. Assign Cybersecurity Responsibilities

MIL1	a.	Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner
	b.	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner
MIL2	c.	Cybersecurity responsibilities are assigned to specific roles, including external service providers
	d.	Cybersecurity responsibilities are documented
MIL3	e.	Cybersecurity responsibilities and job requirements are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure
	f.	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning

2. Develop Cybersecurity Workforce

MIL1	a.	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner
	b.	Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs, at least in an ad hoc manner
MIL2	c.	Training, recruiting, and retention efforts are aligned to address identified workforce gaps
	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function
MIL3	e.	The effectiveness of training programs is evaluated periodically, and improvements are made as appropriate
	f.	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities

3. Implement Workforce Controls

MIL1	a.	Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner
	b.	Personnel separation procedures address cybersecurity, at least in an ad hoc manner
MIL2	c.	Personnel vetting is performed periodically for positions that have access to the assets required for delivery of the function
	d.	Personnel transfer procedures address cybersecurity
	e.	Users are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets
MIL3	f.	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk
	g.	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures

4. Increase Cybersecurity Awareness

MIL1	a.	Cybersecurity awareness activities occur, at least in an ad hoc manner
MIL2	b.	Objectives for cybersecurity awareness activities are established and maintained
	c.	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2d)
MIL3	d.	Cybersecurity awareness activities are aligned with the predefined states of operation (SITUATION-3h)
	e.	The effectiveness of cybersecurity awareness activities is evaluated periodically and according to defined triggers, such as system changes and external events, and improvements are made as appropriate

5. Management Activities

MIL1	No practice at MIL1
MIL2	a. Documented procedures are established, followed, and maintained for activities in the WORKFORCE domain b. Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain
MIL3	c. Up-to-date policies or other organizational directives define requirements for activities in the WORKFORCE domain d. Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities e. Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel f. The effectiveness of activities in the WORKFORCE domain is evaluated and tracked

6.9 Cybersecurity Architecture (ARCHITECTURE)

Purpose: 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.

Establishing a cybersecurity architecture involves identifying cybersecurity requirements for the organization's assets and designing appropriate controls to protect them. The cybersecurity architecture serves as a reference to guide how cybersecurity is to be implemented to meet the objectives of the cybersecurity program strategy.

The Cybersecurity Architecture (ARCHITECTURE) domain comprises six objectives:

1. Establish and Maintain Cybersecurity Architecture Strategy and Program
2. Implement Network Protections as an Element of the Cybersecurity Architecture
3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture
4. Implement Software Security as an Element of the Cybersecurity Architecture
5. Implement Data Security as an Element of the Cybersecurity Architecture
6. Management Activities

The cybersecurity architecture helps an organization 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 controls to, for example, detect, resist, react to, and recover from attacks. Such tactics include segmentation, choice of hosting solutions, cryptographic controls, and audit trails, and they can be allied with availability controls such as monitoring, rollback, and redundancy.

To be effective, the cybersecurity architecture must be sufficiently documented so that it can be communicated to

Example: Cybersecurity Architecture

Anywhere Inc. has recognized that its approach to cybersecurity has become outdated because it relies heavily on the point solutions provided by its current set of vendor products. To modernize its cybersecurity posture, Anywhere Inc. has documented a target cybersecurity architecture. Anywhere plans to use the architecture as part of the assessment of vendor proposals received in response to its cybersecurity modernization RFP.

The cybersecurity architecture permits reasoning about the capabilities of prospective vendor solutions in the context of Anywhere's cybersecurity program. It provides a comprehensive picture of how system components and their interactions will handle responsibilities such as application and data security. It facilitates the creation of integrated end-to-end scenarios by which the quality of a proposed vendor solution may be evaluated. Anywhere has already devised a set of scenarios ranging from rip-and-replace access controls to cloud-enabled mobility.

By its architecture-centric approach to modernization, Anywhere is able to understand the tradeoffs involved in making design choices. For example, the desirability of layered defenses (VPN, firewalls, and controlled access) can be weighed against the overall performance or usability of the system. Similarly, the interactions among trusted and non-trusted system elements (for example, the interface to the internet) can be used to weigh the desirability of information sharing against the need to provide resilience against attacks. In this way, Anywhere can make informed choices about vendor solutions that best fit the functional and behavioral requirements embodied in the architecture.

stakeholders. It must also be governed such that those responsible for the cybersecurity architecture are included in planning and decision-making processes when changes to the organization, IT systems, or OT systems are being considered. In this way, changes to the organization can be reviewed to address security concerns and align with the organization's cyber risk tolerance.

Objectives and Practices

1. Establish and Maintain Cybersecurity Architecture Strategy and Program

MIL1	a.	The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner
MIL2	b.	A strategy for cybersecurity architecture is established and maintained to support the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture
	c.	A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization
	d.	Governance for cybersecurity architecture (such as an architecture review board) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process
	e.	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets
	f.	Cybersecurity controls are selected and implemented to meet cybersecurity requirements
MIL3	g.	The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program
	h.	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events
	i.	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2d)
	j.	The cybersecurity architecture addresses predefined states of operation (SITUATION-3h)

2. Implement Network Protections as an Element of the Cybersecurity Architecture

MIL1	a.	The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner
MIL2	b.	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements (ASSET-1a, ASSET-2a)
	c.	Network protections incorporate the principles of least privilege and least functionality
	d.	Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices)
	e.	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])

2. Implement Network Protections as an Element of the Cybersecurity Architecture (continued)

MIL2	f.	Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking)
MIL3	g.	All assets are segmented into distinct security zones based on cybersecurity requirements
	h.	Isolated networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication
	i.	OT systems are operationally independent from IT systems so that OT operations are unimpeded by an outage of IT systems
	j.	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)
	k.	Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control [NAC])
	l.	The cybersecurity architecture enables the isolation of compromised assets

3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

MIL1	a.	Cybersecurity controls are implemented for assets important to the delivery of the function, at least in an ad hoc manner
MIL2	b.	More rigorous cybersecurity controls are implemented for higher priority assets (ASSET-1d)
	c.	The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced
	d.	The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced
	e.	Secure configurations are implemented as part of the asset deployment process where feasible
	f.	Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls)
	g.	The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives)
	h.	Cybersecurity controls, including physical access controls, are implemented for all assets used for the delivery of the function (ASSET-1f) either at the asset level or as compensating controls where asset-level controls are not feasible
MIL3	i.	Configuration of and changes to firmware are controlled throughout the asset lifecycle
	j.	Controls are implemented to prevent the execution of unauthorized code

4. Implement Software Security as an Element of the Cybersecurity Architecture

MIL1		No practice at MIL1
MIL2	a.	Software developed in-house for deployment on higher priority assets (ASSET-1d) is developed using secure software development practices
	b.	The selection of procured software for deployment on higher priority assets (ASSET-1d) includes consideration of the vendor's secure software development practices
	c.	Secure software configurations are required as part of the software deployment process

4. Implement Software Security as an Element of the Cybersecurity Architecture (continued)

MIL3

d. All software developed in-house is developed using secure software development practices
e. The selection of all procured software includes consideration of the vendor's secure software development practices
f. The architecture review process evaluates the security of new and revised applications prior to deployment
g. The authenticity of all software and firmware is validated prior to deployment
h. Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events

5. Implement Data Security as an Element of the Cybersecurity Architecture

MIL1

a. Sensitive data is protected at rest, at least in an ad hoc manner

MIL2

b. All data at rest is protected for selected data categories (ASSET-2d)
c. All data in transit is protected for selected data categories (ASSET-2d)
d. Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ASSET-2d)
e. Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls
f. Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented

MIL3

g. The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen
h. The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data

6. Management Activities

MIL1

No practice at MIL1

MIL2

a. Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain
b. Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain

MIL3

c. Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain
d. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities
e. Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel
f. The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked

6.10 Cybersecurity Program Management (PROGRAM)

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 both 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 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:

1. Establish Cybersecurity Program Strategy
2. Sponsor Cybersecurity Program
3. 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.

Example: Cybersecurity Program Management

Anywhere Inc. decided to establish an enterprise cybersecurity program. To begin, Anywhere Inc. formed a board with representation from each of the functional areas. This cybersecurity governance board will develop a cybersecurity program strategy for the organization and recruit a new vice president of cybersecurity to implement a program based on the strategy. The vice president will also report to the board of directors and will work across the enterprise to engage business and technical management and personnel to address cybersecurity.

The new vice president's first action will be to expand and document the cybersecurity program strategy for Anywhere Inc., ensuring that it remains aligned to the organization's business strategy and addresses its risk to critical infrastructure. After the strategy is approved by the board, the new vice president will begin implementing the program by reorganizing some existing compartmentalized cybersecurity teams and recruiting additional team members to address skill gaps in the organization.

The head of customer service and vice president of accounting will depend on the new program to address both immediate and collateral damage from potential incidents and the public relations issues that follow. The head of IT and the vice president for engineering will expect guidance on systems development and methods to mitigate risks.

Objectives and Practices

1. Establish Cybersecurity Program Strategy

MIL1

a. The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner

MIL2

b. The cybersecurity program strategy defines goals and objectives for the organization’s cybersecurity activities
c. The cybersecurity program strategy and priorities are documented and aligned with the organization’s strategic objectives and risk to critical infrastructure
d. The cybersecurity program strategy defines the organization’s approach to provide program oversight and governance for cybersecurity activities
e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program
f. The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program
g. The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, NIST guidelines, Payment Card Industry Data Security Standard, ISO, CMMC, and the California Consumer Privacy Act)

MIL3

h. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (THREAT-2d)

2. Sponsor Cybersecurity Program

MIL1

a. Resources (people, funding, and tools) are provided, at least in an ad hoc manner, to establish the cybersecurity program
b. Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner

MIL2

c. The cybersecurity program is established according to the cybersecurity program strategy
d. Adequate resources (people, funding, and tools) are provided to operate a cybersecurity program aligned with the program strategy
e. Senior management sponsorship for the cybersecurity program is visible and active
f. Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies
g. Responsibility for the cybersecurity program is assigned to a role with sufficient authority
h. Stakeholders for cybersecurity program management activities are identified and involved

MIL3

i. Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy
j. Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes
k. The cybersecurity program addresses and enables the achievement of regulatory compliance, as appropriate
l. The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies

3. Management Activities

MIL1	No practice at MIL1	
MIL2	a.	Documented procedures are established, followed, and maintained for activities in the PROGRAM domain
	b.	Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain
MIL3	c.	Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain
	d.	Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel
	f.	The effectiveness of activities in the PROGRAM domain is evaluated and tracked

APPENDIX A: REFERENCES

The C2M2 was derived from the ES-C2M2. The DOE acknowledges the electricity subsector standards, guidelines, white papers, and frameworks that informed the development of the first iteration of the model. The general references below were either used in the development of this document or may serve as a source for further information regarding the practices identified within the model.

[Bass 2013]
Bass, L., Clements, P., & Kazman, R. *Software Architecture in Practice (3rd ed.).* Reading, MA: Addison Wesley 2013.

[CERT CSIRT FAQ]
Software Engineering Institute, Carnegie Mellon University. 2017. *CSIRT Frequently Asked Questions (FAQ)*. Retrieved May 30, 2019, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652

[CERT CSIRTs]
West Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, Mark. 2003. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305

[CERT-RMM]
Caralli, R. A., Allen, J. H., & White, D. W., Young, L. R., Mehravari, N., Curtis, P. D., *CERT® Resilience Management Model, Version 1.2*, CERT Program, Software Engineering Institute, Carnegie Mellon University, Feb. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=508084

[CERT SGMM]
The SGMM Team. 2011, version 1.2. *Smart Grid Maturity Model: Model Definition* (CMU/SEI-2011-TR-025). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10035

[CERT State of the Practice of CSIRTs]
Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. 2003. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571

[CNSSI 4009]
Committee on National Security Systems. 2010. *National Information Assurance (IA) Glossary* (CNSS Instructions No. 4009). Retrieved May 30, 2019, from https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[DHS Cross-Sector Roadmap]
Industrial Control Systems Joint Working Group. 2011, revision 3.0. *Cross-Sector Roadmap for Cybersecurity of Control Systems*. United States Computer Emergency Readiness Team.

[DHS-DOE Energy Sector]
U.S. Department of Homeland Security and U.S. Department of Energy. 2015. *Energy Sector-Specific Plan*. Retrieved June 17, 2019, from https://www.dhs.gov/publication/nipp-ssp-energy-2015

[DHS ICS]
Department of Homeland Security. 2019. *Cybersecurity and Infrastructure Security Agency--Industrial Control Systems.* Retrieved May 30, 2019, from https://ics-cert.us-cert.gov/

[DHS ICSJWG]
Department of Homeland Security. 2019. *Industrial Control Systems Joint Working Group.* Retrieved May 30, 2019, from https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

[DHS NIPP]
Department of Homeland Security. 2013. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience.* Retrieved June 17, 2019, from https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[DHS PCII]
Department of Homeland Security. 2019. *Protected Critical Infrastructure Information (PCII) Program.* Retrieved May 30, 2019, from https://www.dhs.gov/pcii-program

[DHS Procurement]
U.S. Department of Homeland Security, Control Systems Security Program, National Cyber Security Division. 2009. *U.S. Department of Homeland Security: Cyber Security Procurement Language for Control Systems.*

[DOE Framework Implementation]
U.S. Department of Energy. 2015. *Energy Sector Cybersecurity Framework Implementation Guide.* Retrieved June 17, 2019, from https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

[DOE RMP]
U.S. Department of Energy. 2012. *Cybersecurity Risk Management Process (RMP) Guideline – Final (May 2012).* Retrieved June 17, 2019, from https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012

[DOE Roadmap]
U.S. Department of Energy. 2011. *Roadmap to Achieve Energy Delivery Systems Cybersecurity – 2011.* Retrieved June 17, 2019, from https://www.energy.gov/ceser/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011

[FIRST]
Forum of Incident Response and Security Teams (FIRST). 2012. *CSIRT Case Classification (Example for Enterprise CSIRT).* Retrieved May 30, 2019, from https://www.first.org/resources/guides/csirt_case_classification.html

[HSPD-7]
U.S. Department of Homeland Security. n.d. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Retrieved May 30, 2019, from https://www.cisa.gov/homeland-security-presidential-directive-7

[IACCM BRM3]
International Association for Contract & Commercial Management (IACCM). 2003. *The IACCM Business Risk Management Maturity Model (BRM3).*

[ISA 99]
International Society of Automation (ISA). 2009. *Industrial Automation and Control Systems Security: Establishing an Industrial Automation and Control Systems Security Program* (ANSI/ISA-99.02.01-2009).

[ISACs]
National Council of Information Sharing and Analysis Centers (ISACs). 2019. Retrieved May 30, 2019, from https://www.nationalisacs.org/

[ISO/IEC 2:2004]
International Organization for Standardization. 2004. *Standardization and Related Activities – General Vocabulary* (ISO/IEC 2:2004).

[ISO 27005:2011]
International Organization for Standardization. 2011. *Information Security Risk Management* (ISO 27005:2011)

[ISO/IEC 21827:2008]
International Organization for Standardization. 2008. *Systems Security Engineering – Capability Maturity Model (SSE-CMM)* (ISO/IEC 21827:2008).

[ISO/IEC 27001:2005]
International Organization for Standardization. 2008. *Information Security Management Systems* (ISO/IEC CD 27001:2005).

[ISO/IEC 27002:2005]
International Organization for Standardization. 2008. *Code of Practice for Information Security Management* (ISO/IEC27002:2005).

[ISO 28001:2007]
International Organization for Standardization. n.d. *Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance* (ISO/ IEC20001:2007).

[MIT SCMM]
Rice, Jr., J. B., & Tenney, W. 2007. "How risk management can secure your business future." *Massachusetts Institute of Technology Supply Chain Strategy, 3(5), 1-4*. Retrieved May 30, 2019, from http://web.mit.edu/scresponse/repository/rice_tenney_SCS_RMM_june-july_2007.pdf

[MITRE 2021]
The MITRE Corporation. 2021. MITRE ATT&CK. Retrieved May 18, 2021, from https://attack.mitre.org

[NDIA ESA]
National Defense Industrial Association, System Assurance Committee. 2008. *Engineering for System Assurance, Version 1.0.*

[NIST CSF]
National Institute of Standards and Technology. 2018. *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Retrieved May 30, 2019, from https://www.nist.gov/cyberframework/framework

[NIST Framework]
National Institute of Standards and Technology. 2012. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.* Retrieved May 30, 2019, from https://www.nist.gov/sites/default/files/documents/smartgrid/NIST_Framework_Release_2-0_corr.pdf

[NIST Security Considerations in SDLC]
Ross, R., McEvilley, M. Carrier Oren, J. 2016. *Systems Security* Engineering (NIST SP 800-160 Volume 1). National Institute of Standards and Technology. Retrieved June 19, 2020 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[NIST SP800-16]
Toth, P., & Klein, P. 2014. *A Role-Based Model for Federal Information Technology/Cybersecurity Training* (3rd Draft) (NIST Special Publication 800-16, Revision 1.0, 3rd Draft). National Institute of Standards and Technology. Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2014-03-14

[NIST SP800-37]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (NIST Special Publication 800-37 Revision 2). Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[NIST SP800-40]
Souppaya, M., Scarfone, K. 2013. *Guide to Enterprise Patch Management Technologies* (NIST Special Publication 800-40, Revision 3). National Institute of Standards and Technology. Retrieved June 19, 2020 from https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

[NIST SP800-50]
Wilson, M., & Hash, J. 2003. *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-50/final

[NIST SP800-53]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2009. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Revision 4). Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[NIST SP800-61]
Cichonski, P., Millar, T., Grance, T., & Scarfone, K. 2012. *Computer Security Incident Handling Guide* (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[NIST SP800-64]
Ross, R., McEvilley, M., Oren, J. 2018. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (NIST Special Publication 800-160, Volume 1). National Institute of Standards and Technology. Retrieved June 19, 2010 from https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

[NIST SP800-82]
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. *Guide to Industrial Control Systems (ICS) Security*, pg. B-14 (NIST Special Publication 800-82, Revision 2). National Institute of Standards and Technology. Retrieved May 3, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[NIST SP800-83]
Souppaya, M., Scarfone, K. 2013. *Guide to Malware Incident Prevention and Handling* (NIST Special Publication 800-83 Revision 1). National Institute of Standards and Technology. Retrieved June 19, 2019, from https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final

[NIST SP800-128]
National Institute of Standards and Technology. 2011. *Guide for Security-Focused Configuration Management of Information Systems* (NIST Special Publication 800-128). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-128/final

[NIST SP800-137]
Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Stine, K. 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST Special Publication 800-137). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-137/final

[NIST SP800-150]
Johnson, C., Badger, M., Waltermire, D., Snyder, J., Skorupka, C. 2016. *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-150/final

[NIST SP800-160]
Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. 2019. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* (NIST Special Publication 800-160 Volume 2). National Institute of Standards and Technology. Retrieved March 8, 2021, from https://csrc.nist.gov/publications/detail/sp/800-160/final

[NIST NVD]
National Institute of Standards and Technology. 2019. *National Vulnerability Database.* Retrieved May 30, 3019, from https://nvd.nist.gov/vuln-metrics/cvss

[NISTIR 7622]
Boyens, J., Paulsen, C., Bartol, N., Shankles, S., & Moorthy, R. 2012. *Notional Supply Chain Risk Management Practices for Federal Information Systems* (NISTIR 7622). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7622/final

[NISTIR 7628 Vol. 1]
The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cybersecurity, Volume 1: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* (NISITIR 7628). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[NISTIR 7628 Vol. 3]
The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cybersecurity, Volume 3: Supportive Analyses and References* (NISITIR 7628 *).* National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[NISTIR 8053]
Garfinkel, S. L. 2015. *De-Identification of Personal Information* (NIST Internal Report 8053). National Institute of Standards and Technology. Retrieved May 3, 2021, from https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

[OECD Reducing Systemic Cybersecurity Risk]
Sommer, P., & Brown, I. 2011. *Reducing Systemic Cybersecurity Risk.* Organisation for Economic Co-operation and Development. Retrieved May 30, 2019, from http://www.oecd.org/governance/risk/46889922.pdf

[SEI CMM]
Paulk, M., Weber, C., Garcia, S., Chrissis, M.B., & Bush, M. 1993. *Key Practices of the Capability Maturity Model* (Version 1.1, Technical Report CMU/SEI-93-TR-25). Software Engineering Institute, Carnegie Mellon University. Retrieved May 30, 2019, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11965

[SCADA AU RMF]
IT Security Expert Advisory Group. 2012. *Generic SCADA Risk Management Framework for Australian Critical Infrastructure.* Retrieved May 30, 2019, from http://www.tisn.gov.au/Documents/SCADA-Generic-Risk-Management-Framework.pdf

[Situation Awareness in Dynamic Systems]
Endsley, M. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems." Human Factors, pp. 32-64.

[Supply Chain Risk Management Awareness]
Filsinger, J., Fast, B., Wolf, D.G., Payne, J.F.X., & Anderson, M. 2012. *Supply Chain Risk Management Awareness.* Armed Forces Communication and Electronics Association Cyber Committee. Retrieved May 30, 2019, from http://www.afcea.org/committees/cyber/documents/Supplychain.pdf

APPENDIX B: GLOSSARY

Term	Definition	Source
access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	Adapted from CNSSI 4009
access control	Limiting access to organizational assets only to authorized entities, such as users, programs, processes, or other systems. See *asset*.	Adapted from CNSSI 4009
access management	Management processes to ensure that access granted to the organization's assets is commensurate with the risk to critical infrastructure and organizational objectives. See *access control* and *asset*.	Adapted from CERT-RMM
ad hoc	In the context of the model, *ad hoc* (that is, formed or used for a special purpose without policy or a plan for repetition) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance, such as a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice; when it is performed; the context of the problem being addressed; the methods, tools, and techniques used; and the priority given a particular instance of the practice. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, because, in an ad hoc practice, lessons learned are typically not captured at the organizational level, approaches and outcomes are difficult to repeat or improve across the organization. It is important to note that, while documented policies or procedures are not essential to the performance of a practice in an ad hoc manner, the effective performance of many practices would result in documented artifacts such as a documented asset inventory or a documented cybersecurity program strategy.	C2M2
all assets used for the delivery of the function	All assets that are used in the normal state of operation of the function. Expands the scope of an inventory beyond assets that are *important* to the delivery of the function to any IT, OT, or information asset that is related to the delivery of the function.	C2M2
anomalous	Inconsistent with or deviating from what is usual, normal, or expected.	Merriam-Webster.com
Architecture (ARCHITECTURE)	The C2M2 domain with the purpose to 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.	C2M2
architecture	See *cybersecurity architecture.*	

Term	Definition	Source
assessment	See *risk assessment.*	
asset	Something of value to the organization. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of the model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.	
Asset, Change, and Configuration Management (ASSET)	The C2M2 domain with the purpose to 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.	C2M2
asset owner	A person or organizational unit, internal or external to the organization that has primary responsibility for the viability, productivity, and resilience of an organizational asset.	CERT-RMM
assets important to the delivery of the function	The subset of assets that is required for a normal state of operation of the function and output of the function's products or services. Loss of an asset that is considered "important to the delivery of the function" may not directly result in an inability to deliver the function, but could result in operations being degraded. Identification of an important asset should focus on loss of the service or role performed by that asset and should not include consideration of asset redundancy or other protections applied to assets.	C2M2
assets required for minimum operation of the function	A subset of assets that the organization has identified as being needed to maintain a minimum level of operation while operations have been degraded.	C2M2
assets within the function that may be leveraged to achieve a threat objective	Assets that may be used in the pursuit of the tactics or goals of a threat actor. Identification of assets within the function that may be leveraged to achieve a threat objective should focus on the techniques used by threat actors and the potential for those techniques to be applied to the organization's assets. These are some examples of assets within the function that may be leveraged to accomplish a threat objective: • public-facing assets that may serve as an initial access point • individual systems that would allow lateral movement within an organization's network • systems with administrative rights that would enable privilege escalation • information such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed See also *threat objective*.	

Term	Definition	Source
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to IT, OT, or information assets.	DOE Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline
availability	Ensuring timely and reliable access to and use of information. For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed.	DOE RMP & CERT-RMM
change management	A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption.	CERT-RMM
confidentiality	The preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For an information asset, confidentiality is the quality of being accessible only to authorized people, processes, and devices.	DOE RMP & Adapted from CERT-RMM
configuration baseline	A documented set of specifications for an IT or OT system or asset, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which should be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and changes.	Adapted from NIST 800-53 Glossary
configuration management	A collection of activities focused on establishing and maintaining the integrity of assets, through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their lifecycle.	NIST SP 800-128
controls	The management, operational, and technical methods, policies, and procedures—manual or automated—(that is, safeguards or countermeasures) prescribed for IT and OT assets to protect the confidentiality, integrity, and availability of those assets and their associated information assets.	DOE RMP
critical infrastructure	Assets that provide the essential services that underpin society. Nations possess key resources whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through terrorist attack could have a debilitating effect on security and economic well-being.	HSPD-7
current	Updated at an organization-defined frequency, such as in the asset inventory is kept “current,” that is selected such that the risks to critical infrastructure and organization objectives associated with being out-of-date by the maximum interval between updates are acceptable to the organization and its stakeholders.	C2M2

Term	Definition	Source
cyber attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information.	DOE RMP
cybersecurity	Prevention and limitation of unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, and information assets to ensure their confidentiality, integrity, and availability.	Adapted from [NIST SP800-37]
cybersecurity architecture	How cybersecurity practices and controls are structured and implemented to maintain the confidentiality, integrity, and availability of the organization's assets and services. See also *enterprise architecture*.	C2M2
cybersecurity controls	The administrative, operational, and technical measures (i.e., processes, policies, devices, practices, or other actions) prescribed for IT, OT, and information assets to manage their associated risk.	Adapted from [NIST SP800-82] and [NISTIR 8053]
cybersecurity event	See *event*.	C2M2
cybersecurity impact	The effect on the measures that are in place to protect from and defend against cyber attacks.	C2M2
cybersecurity incident	See *incident.*	
cybersecurity incident lifecycle	See *incident lifecycle.*	
cybersecurity program	A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization 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.	C2M2
Cybersecurity Program Management (PROGRAM)	The C2M2 domain with the purpose to 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.	C2M2
cybersecurity program strategy	A plan of action designed to achieve the performance targets that the organization sets to accomplish its mission, vision, values, and purpose for the cybersecurity program.	CERT-RMM
cybersecurity requirements	Requirements levied on IT and OT systems that are derived from organizational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, and procedures) to ensure the confidentiality, integrity, and availability of the services being provided by the organization and the information being processed, stored, or transmitted.	Adapted from DOE RMP
cybersecurity responsibilities	Obligations for ensuring the organization's cybersecurity requirements are met.	C2M2

Term	Definition	Source
cyber risk	The possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. Cyber risk is a function of impact, likelihood, and susceptibility.	C2M2
data	A collection of bits that may be processed, stored, or transmitted by an IT or OT system.	C2M2
data at rest	Data that is in some kind of storage, such as a hard drive or a server.	C2M2
data in transit	Data that is being transmitted via some kind of network, such as a private network or the internet.	C2M2
data protection	A strategy that encompasses avoiding, detecting, minimizing, responding to, and recovering from data loss and the consequences of data loss.	Adapted from NIST SP800-160
defined practice	A practice that is planned (that is, described, explained, made definite and clear, and standardized) and is executed in accordance with the plan.	Adapted from CERT-RMM
dependency risk	Dependency risk is measured by the likelihood and severity of damage if an IT or OT system is compromised due to a supplier or other third party on which delivery of the function depends. Evaluating dependency risk includes an assessment of the importance of the potentially compromised system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. See also *supply chain risk.*	Adapted from NIST 7622, pg. 10
deprovisioning	To revoke or remove an identity's access to organizational assets. See also *provision.*	CERT-RMM
domain	In the context of the model structure, a domain is a logical grouping of cybersecurity practices.	C2M2
domain objectives	The practices within each domain are organized into *objectives*. The objectives represent achievements that support the domain (such as "Manage Asset Configuration" for the ASSET domain and "Increase Cybersecurity Awareness" for the WORKFORCE domain). Each of the objectives in a domain comprises a set of practices, which are ordered by maturity indicator level.	C2M2
enterprise	The highest level organizational unit that encompasses the part of the organization using the C2M2. Some enterprises may consist of multiple organizations (e.g., a holding company with one or more operating companies). Other organizations may have a more homogenous structure that does not necessitate any differentiation between the terms *enterprise* and *organization*. For those organizations, *enterprise* and *organization* may be used interchangeably. See also *organization.*	C2M2
enterprise architecture	The design and description of an enterprise's entire set of IT and OT assets: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. See also *cybersecurity architecture*.	Adapted from DOE RMP

Term	Definition	Source
entity	In the context of identity and access management, someone or something having separate or distinct existence (such as a person, object, system, or process) that requires access to an asset.	Merriam-Webster.com Adapted from CERT-RMM
establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, “Establish and maintain identities” means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.	CERT-RMM
event	Any anomalous occurrence in a system or network that is related to a cybersecurity requirement. Depending on their potential impact, some events need to be declared as incidents. See also *cybersecurity requirements*.	NIST 800-61
Event and Incident Response, Continuity of Operations (RESPONSE)	The C2M2 domain with the purpose to 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.	C2M2
function	In C2M2, *function* is used as a scoping mechanism; it refers to the operations of the organization that are being evaluated based on the model. A function may or may not align with organizational boundaries. For example, the function might be a line of business, a network security zone, or a single facility.	C2M2
governance	An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT-RMM
guidelines	A set of recommended practices produced by a recognized authoritative source representing subject matter experts and community consensus or produced internally by an organization. See also *standard*.	C2M2
identity	The set of attribute values (that is, characteristics) by which a person or entity is recognizable and that, within the scope of an identity manager’s responsibility, is sufficient to distinguish that person or entity from any other.	Adapted from CNSSI 4009
Identity and Access Management (ACCESS)	The C2M2 domain with the purpose to 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.	C2M2

Term	Definition	Source
impact	Negative consequences of an event or action. Impact is a key component in understanding the severity of a particular risk. Impact from cybersecurity incidents might include, for example, response costs, regulatory fines, and lost income from reputation damage.	C2M2
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit impact. Criteria for declaration of an incident are determined by the organization. See also *event.*	Adapted from CERT-RMM
incident lifecycle	The stages of an incident from detection to closure. Collectively, the incident lifecycle includes the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents. Events also follow the incident lifecycle.	Adapted from CERT-RMM
information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.	NIST SP800-39
information assets	Information of value to the organization, such as business data, information, intellectual property, customer information, and contracts, security logs, metadata, set points, and operational data. Information Assets may be in digital or non-digital form.	Adapted from CERT-RMM
Information Sharing and Analysis Center (ISAC)	An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants on infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning.	Adapted from Electricity Sector Information Sharing and Analysis Center website home page
information technology (IT)	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.	DOE RMP
institutionalization	The extent to which a practice or activity is ingrained into the way an organization operates and is followed routinely as part of corporate culture. The more an activity becomes part of how an organization operates, the more likely it is that the activity will continue to be performed over time, with a consistently high level of quality. See also *maturity indicator level.*	C2M2 & CERT-RMM
integrity	Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner.	DOE RMP & CERT-RMM

Term	Definition	Source
least privilege	A security control that addresses the potential for abuse of authorized privileges. The organization employs the concept of least privilege by allowing only authorized access for users (and processes acting on behalf of users) who require it to accomplish assigned tasks in accordance with organizational missions and business functions. Organizations employ the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary to achieving least privilege. Organizations also apply least privilege concepts to the design, development, implementation, and operations of IT and OT systems.	Adapted from NIST 800-53
logging	Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. Logging may also refer to keeping a manual record, such as a sign-in sheet, of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace. Regular review and audit of logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness, such as through the detection of cybersecurity events or weaknesses.	C2M2
logical control	A software, firmware, or hardware feature (that is, computational logic, not a physical obstacle) within an IT or OT system that restricts access to and modification of assets only to authorized entities. For contrast, see *physical control*.	Adapted from CNSSI 4009 definition of “internal security controls”
maturity	The extent to which an organization has implemented and institutionalized the cybersecurity practices of the model.	C2M2
maturity indicator level (MIL)	A measure of the cybersecurity maturity of an organization in a given domain of the model. The model currently defines four maturity indicator levels (MILs). Each of the four defined levels is designated by a number (0 through 3) and a name, for example, “MIL3: managed.” A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out cybersecurity practices, to organizational policies and procedures that institutionalize those practices, making them repeatable with a consistently high level of quality. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the activities in the domain.	C2M2
monitoring	Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT-RMM (Monitoring and Risk Management)

Term	Definition	Source
monitoring requirements	The requirements established to determine the information gathering and distribution needs of stakeholders.	CERT-RMM
multifactor authentication	Use of two or more factors to achieve verification of an identity. Factors include (1) something you know, such as a password or PIN, (2) something you have, such as a cryptographic identification device or token, (3) something you are, such as a biometric marker, and (4) something that indicates that you are where you say you are, such as a GPS token. See also *authentication*.	Adapted from NIST 800-53
objectives	*See domain objectives* and *organizational objectives*.	
operational resilience	The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. See the related term *operational risk*.	CERT-RMM
operating states	See *predefined states of operation*.	C2M2
operational risk	The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. In the context of the model, the focus is on operational risk from cybersecurity threats.	Adapted from CERT-RMM
operations technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial control systems, building management systems, fire control systems, process control systems, safety instrumented systems, Internet of things (IoT) devices, and physical access control mechanisms.	C2M2
organization	In the context of the model, the organization is the part of the enterprise that encompasses the function selected for C2M2 evaluation or improvement. In smaller enterprises, the terms *enterprise* and *organization* are often interchangeable. See also *function* and *enterprise*.	Adapted from DOE RMP
organizational objectives	Performance targets set by an organization. See also *strategic objectives*.	Adapted from CERT-RMM
periodic review/activity	A review or activity that occurs at specified, regular time intervals, where the organization-defined frequency is commensurate with risks to organizational objectives and critical infrastructure.	Adapted from SEI CMM Glossary
physical control	A type of control that prevents physical access to and modification of information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods.	CERT-RMM
plan	A detailed formulation of a program of action.	Merriam-Webster.com

Term	Definition	Source
policy	A documented description of roles, responsibilities, and expected or required actions related to a particular area of organizational activity, such as asset management.	C2M2
position description	A set of responsibilities that describe a role or roles filled by an employee. Also known as a job description.	C2M2
practice	An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organizational objectives.	C2M2
predefined states of operation	Distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resiliency, reliability, or cybersecurity. For example, a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity. The high-security operating state may trade off efficiency and ease of use in favor of increased security by blocking remote access and requiring a higher level of authentication and authorization for certain commands until a return to the normal state of operation is deemed safe.	C2M2
privacy	The assurance that information about an individual is collected, used, and disclosed only as authorized by that individual or as permitted under privacy laws and regulations.	C2M2
procedure	In the model, *procedure* is synonymous with *process*.	
process	A series of discrete activities or tasks that contribute to the fulfillment of a task or mission.	CERT-RMM (business process)
provision	To assign or activate an identity profile and its associated roles and access privileges. See also *deprovisioning*.	CERT-RMM
recovery point objectives (RPO)	The point in time to which data is restored after an incident. The point to which information used by the function must be restored to enable the activity to operate on resumption.	C2M2
recovery time objectives (RTO)	The period of time within which systems, applications, or functions must be recovered after an incident. RTO includes the time required for assessment, execution and verification. The period of time following an incident within which a product or service or function or an activity must be resumed, or resources must be recovered.	C2M2
risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence. See also *cyber risk*.	DOE RMP

Term	Definition	Source
risk analysis	A risk management activity focused on understanding the likelihood and potential impact of risks, prioritizing risks, and determining a path for addressing risks. Analysis determines the importance of each identified risk and is used to facilitate the organization's response to the risk.	Adapted from CERT-RMM
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, and reputation), resources, other organizations, and the Nation, resulting from the operation of IT and OT systems.	DOE RMP
risk criteria	Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches.	C2M2
risk management program	The program and supporting processes to manage cyber risk to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation. It includes (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.	DOE RMP
Risk Management (RISK)	The C2M2 domain with the purpose to 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.	C2M2
risk management strategy	Strategic-level decisions on how senior executives manage risk to an organization's operations, resources, and other organizations.	DOE RMP
risk mitigation	Prioritizing, evaluating, and implementing appropriate risk-reducing controls.	DOE RMP
risk register	A structured repository where identified risks are recorded to support risk management.	C2M2
risk response	Accepting, avoiding, mitigating, or transferring risk to organizational operations, resources, and other organizations.	DOE RMP
risk taxonomy	A structured description of categories of risk that the organization is subject to and must manage.	Adapted from CERT-RMM
secure software development	Developing software using recognized processes, secure coding standards, best practices, and tools that have been demonstrated to minimize security vulnerabilities in software systems throughout the software development lifecycle. An essential aspect is to engage programmers and software architects who have been trained in secure software development.	C2M2
security zone	A grouping of systems and components with similar cybersecurity requirements. Zone access is restricted by network and security devices.	C2M2

Term	Definition	Source
separation of duties	[A security control that] "addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example, (i) dividing mission functions and information system support functions among different individuals or roles; (ii) conducting information system support functions with different individuals, such as system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Organizations with significant personnel limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls."	NIST 800-53, pp. 31, F-13
service level agreement (SLA)	Defines the specific responsibilities of a service provider, including the satisfaction of any relevant cybersecurity requirements, and sets the customer's expectations regarding the quality of service to be provided.	Adapted from CNSSI 4009
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision making with respect to activities that depend on or affect how well a system functions. It involves the collection of data, such as via sensor networks, data fusion, and data analysis (which may include modeling and simulation) to support automated or human decision making (for example, concerning OT system functions). Situational awareness also involves appropriate use of alarms and the presentation of the results of the data analysis in some form, such as using data visualization techniques, that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision making.	Adapted from SGMM Glossary
Situational Awareness (SITUATION)	The C2M2 domain with the purpose to establish and maintain activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP), commensurate with the risk to critical infrastructure and organizational objectives.	C2M2
sponsorship	Enterprise-wide support of cybersecurity objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the cybersecurity program along with provision of resources. Senior management monitors the performance and execution of the cybersecurity program and is actively involved in the ongoing improvement of all aspects of the cybersecurity program.	C2M2
stakeholder	An external organization or an internal or external person or group that has a vested interest in the organization's cybersecurity practices, such as government, vendors, sector organizations, regulators, and internal business lines. Stakeholders may be involved in performing a given practice or may oversee, benefit from, or be dependent upon the quality with which the practice is performed.	Adapted from CERT-RMM

Term	Definition	Source
standard	A standard is a document, established by consensus, which provides rules, guidelines, or characteristics for activities or their results. See also *guidelines*.	Adapted from ISO/IEC Guide 2:2004
states of operation	See *predefined states of operation.*	
strategic objectives	The performance targets that the organization sets to accomplish its mission, vision, values, and purpose.	CERT-RMM
strategic planning	The process of developing strategic objectives and plans for meeting these objectives.	CERT-RMM
supply chain	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. The supply chain encompasses the full product lifecycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain.	NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA]
supply chain risk	Supply chain risk is measured by the likelihood and severity of damage if an IT or OT system is compromised by a supply chain attack, and takes into account the importance of the system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the lifecycle. Supply chain attacks are typically conducted or facilitated by individuals or organizations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system or infrastructure, or disabling of mission-critical operations. See also *risk and supply chain*.	Adapted from NIST 7622, p. 7 & p. 10
Third-Party Risk Management (THIRD-PARTIES)	The C2M2 domain with the purpose to 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.	C2M2
susceptibility	The probability that an event, once initiated or attempted, will succeed and lead to the realization of a risk. Susceptibility is a component of the overall probability of a risk and is the component of probability that the organization has the most control over.	C2M2
threat	Any actor, circumstance, or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, or denial of service.	Adapted from DOE RMP

Term	Definition	Source
Threat and Vulnerability Management (THREAT)	The C2M2 domain with the purpose to 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, operational, and organizational objectives.	C2M2
threat objective	A specific goal of a potential adversary (for example, extortion, data manipulation, IP theft, customer data theft, sabotage). In the broadest sense, such objectives include tactics like those defined in the MITRE ATT&CK framework [MITRE 2021] that would enable attackers to achieve their ultimate goals.	C2M2
threat profile	A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT, OT, and information assets of an organization and to the organization itself, identifying feasible threats, describing the nature of the threats, and evaluating their severity.	C2M2
threat source	An intent and method targeted at the intentional exploitation of a vulnerability or a situation, or a method that may accidentally exploit a vulnerability.	DOE RMP
traceability	The ability to determine whether or not a given attribute of the current state is valid, such as the current configuration of a system or the purported identity of a user, based on the evidence maintained in a historical record showing how the attribute was originally established and how it has changed over time.	C2M2
triggers	Events (such as a change to IT infrastructure) and time intervals (such as monthly or yearly) that are used to indicate when an activity should occur, such as a review and possible update of the risk management strategy.	C2M2
validation	Collection and evaluation of evidence to confirm or establish the quality of something, such as information, a model, a product, a system, or component, with respect to its fitness for a particular purpose.	C2M2
vulnerability	A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source.	Adapted from NISTIR 7628 Vol. 1, pp. 8
vulnerability assessment	Systematic examination of an IT or OT asset to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.	DOE RMP

Term	Definition	Source
workforce lifecycle	For the purpose of the model, the workforce lifecycle comprises the distinct phases of workforce management that apply to personnel both internal and external to the organization. Specific cybersecurity implications and requirements are associated with each lifecycle phase. The workforce lifecycle includes recruiting, hiring, onboarding, skill assessments, training and certification, assignment to roles (deployment), professional growth and development, re-assignment and transfers, promotions and demotions, succession planning, and termination or retirement. The phases may not be in strict sequences, and some phases (like training, re-assignment, and promotions) may recur.	C2M2
Workforce Management (WORKFORCE)	The C2M2 domain with the purpose to 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.	C2M2

APPENDIX C: ACRONYMS

Acronym	Definition
AGA	American Gas Association
C2M2	Cybersecurity Capability Maturity Model
CERT®-RMM	CERT® Resilience Management Model
CISA	Cybersecurity and Infrastructure Security Center
COTS	commercial off-the-shelf
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DOE	Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
FIRST	Forum of Incident Response and Security Teams
FERC	Federal Energy Regulatory Commission
HR	human resources
IAM	identity and access management
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
IT	information technology
MIL	maturity indicator level
NERC	North American Electric Reliability Corporation
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NYPA	New York Power Authority
OT	operations technology
RPO	recovery point objective
RTO	recovery time objective
RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline

Acronym	Definition
SCADA	supervisory control and data acquisition
SEI	Software Engineering Institute
SLA	service level agreement
US-CERT	United States Computer Emergency Readiness Team

NOTICE

C2M2 was created with the funding and support of DOE under the Federal Government Contract Number FA8702-15-D-0002 between the U.S. Department of Defense and Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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

During the creation of the original C2M2, Capability Maturity Model® and CMM® were registered trademarks of Carnegie Mellon University. Information Systems Audit and Control Association, Inc. (ISACA) is the current owner of these marks but did not participate in the creation of C2M2.