C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2)

Version 2.1

June 2022

U.S. DEPARTMENT OF ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response

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 2.1 Team and Contributors

Joseph Adams, Duke Energy	Aaron Hescox, Exelon	Jason Nations, OGE Energy
Shola Anjous, Motiva	Paul Holgate, Benton PUD	Louis Nguyen, Southern California Gas
Amy Batallones, Con Edison	Ryan Hutton, Arizona Public Service	Erik Norland, Chelan County PUD
Dave Batz, Edison Electric Institute	William Hutton, National Rural Electric Cooperative Association	Bonnie Norman, Colonial Pipeline
Howard Biddle, American Electric Power	Brian Irish, Salt River Project	Maggie O'Connell, American Fuel & Petrochemical Manufacturers
Shawn Bilak, Southern Company	Michael Isper, Interstate Natural Gas Association of America	John Osborne, Knoxville Utilities Board
Steve Brain, Dominion Energy	John Jorgensen, Black Hills Energy	Niyo Little Thunder Pearson, ONE Gas
Jonathan Bransky, Dominion Energy	Nick Julian, Knoxville Utilities Board	Jose Pena, Knoxville Utilities Board
Jeff Brausieck, Seattle City Light	Steve Keisner, Edison Electric Institute	Michael Perdunn, Omaha Public Power District
Kaitlin Brennan, Edison Electric Institute	Mark Kenner, Knoxville Utilities Board	Chris Peters, Entergy
James Brosnan, Evergy	Sung Kim, CPS Energy	Brandon Pixley, CPS Energy
Juanita Buchanan, Exelon	Jordan King, Portland General Electric	Timothy Pospisil, Nebraska Public Power District

Model, Version 2.1 Team and Contributors (continued)

Kenneth Carnes, New York Power Authority	Scott Klauminzer, Tacoma Power	Vijay Pounraj, CPS Energy
Shane Clancy, Santee Cooper	Matt Knight, Owensboro Municipal Utilities	Robert Prince, Sempra
Emily Clark, American Petroleum Institute	Dean Kovacs, Energy Northwest	Jody Raines, New Jersey Board of Public Utilities
James Clark, South Jersey Industries	Tom Lalonde, Southern California Gas	Kaila Raybuck, Edison Electric Institute
Mark Coffey, Eversource	Tamara Lance, Atmos Energy	Sara Ricci, New York Power Authority
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
Tim Corum, Knoxville Utilities Board	Jim Linn, American Gas Association / Downstream Natural Gas Information Sharing and Analysis Center	Brian Rudowski, Long Island Power Authority
Randy Crissman, New York Power Authority	Mujib Lodhi, Long Island Power Authority	David Sayles, Tri-State Generation and Transmission Association
Stephen Dake, Madison Gas and Electric	Helen Lorimor, Southern California Edison	Moin Shaikh, Long Island Power Authority
Michael Fish, Salt River Project	Jacob Maenner, Exelon	Curtis Stapleton, Enable Midstream Partners
Andrew Fitzgerald, Exelon	Carter Manucy, Florida Municipal Power Agency	Emma Stewart, National Rural Electric Cooperative Association
Chris Folta, Benton PUD	Shane Markley, Southwest Gas	Jon Stitzel, Ameren
Kegan Gerard, Southern California Edison	Paul Matthews, Dominion Energy	Chris Taylor, Southern Company
Charles Glidden, Oncor	Joshua Mauk, Omaha Public Power District	Michael Tomasiewicz, Omaha Public Power District
Patrick Glunz, Nebraska Public Power District	Dan Miller, Entergy	Gerardo Trevino, Electric Power Research Institute
Geoff Goolsbay, ONE Gas	Steve Miller, UGI Corporation	Tabice Ward, Xcel Energy
Matt Harper, Devon Energy	Robert Mims, Southern Company	Joy Weed, Southern California Edison
Nicholas Harrison, Salt River Project	Krishna Mistry, ConEdison	Spencer Wilcox, PNM Resources
Noelle Henrickson, Evergy	Nathan Mitchell, American Public Power Association	Mark Wixon, Black Hills Energy

Advisory Contributors

Joshua Axelrod, Amazon	David Howard, United States Department of Energy	Justin Pascale, Dragos
Jason Christopher, Dragos	Cynthia Hsu, United States Department of Energy	Brenden Pavlica, Ernst and Young
Robert Di Pietro, PwC	Al Kaufmann, Nevermore Security	Seth Pelletier, Dragos
Grayson Estes, Estes.io	Annabelle Lee, Nevermore Security	Maggy Powell, Amazon
Stu Goodwin, PwC	Samara Moore, Amazon	Mark Stacey, Dragos
Walter Grudzinski, PwC	Mobolaji Moyosore, Clear Channel Outdoor	Kai Thomsen, Dragos
Angela Haun, Oil and Natural Gas Information Sharing and Analysis Center		

Program Team and Contributors

Brian Benestelli, Carnegie Mellon University Software Engineering Institute - CERT Program	John Keenan, Idaho National Laboratory	Jared Smith, Idaho National Laboratory
Richard Caralli, Axio	Ismael Khokhar, ICF	Ron Savoury, MITRE
Eric Cardwell, Axio	Lindsay Kishter, Nexight Group	Patrick Siebenlist, Nexight Group
Michael Cohen, MITRE	Josie Long, MITRE	Paul Skare, Pacific Northwest National Laboratory
Pamela Curtis, Axio	Julia Mullaney, Carnegie Mellon University Software Engineering Institute - CERT Program	Beth Slaninka, Nexight Group
Jack Eisenhauer, Nexight Group	Bradley Nelson, Idaho National Laboratory	Morgan Smith, Nexight Group
Kathryn Fetzer, Idaho National Laboratory (INL)	Jason Pearlman, Nexight Group	Ryan Subers, Axio
Tricia Flinn, Carnegie Mellon University Software Engineering Institute - CERT Program	Alexander Petrilli, Carnegie Mellon University Software Engineering Institute - CERT Program	Darlene Thorsen, Pacific Northwest National Laboratory
John Fry, Axio	Jeanne Millet Petty, Appligent Document Solutions	Hillary Tran, MITRE

Program Team and Contributors (continued)

Doug Gardner, Carnegie Mellon University Software Engineering Institute - CERT Program	Jeff Pinkhard, Carnegie Mellon University Software Engineering Institute - CERT Program	David White, Axio
Clifford Glantz, Pacific Northwest National Laboratory	Rick Randall, MITRE	Virginia Wright, Idaho National Laboratory
Sri Nikhil Gourisetti, Pacific Northwest National Laboratory	Clark Robinson, United States Department of Energy	Chris Yates, MITRE
Jessica Hedges, Carnegie Mellon University Software Engineering Institute - CERT Program	Paul Ruggiero, Carnegie Mellon University Software Engineering Institute - CERT Program	Walter Yamben, National Energy Technology Laboratory
Gavin T Jurecko, 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

Since the initial release of Version 1.0 of the Cybersecurity Capability Maturity Model (C2M2) in 2012, both technology and threat actors have become more sophisticated, creating new attack vectors and introducing new risks. Also, new cybersecurity standards have been developed and existing standards have been improved. Several subsequent versions of the model have been developed and released since 2012. The C2M2, Version 2.1 incorporates guidance from energy sector cybersecurity practitioners to continue to address these challenges and improve alignment with internationally recognized cyber standards and best practices, including the NIST Special Publication 800-53 and the NIST Cybersecurity Framework (CSF) Version 1.1, released in April 2018.

Table 1: Summary of Changes

Update	Description of Update
Alignment with NIST Cybersecurity Framework	Version 2.1 of the model has been enhanced to improve alignment with the NIST Cybersecurity Framework.
Improvement of existing practices	Practices in Version 2.0 were reviewed through the United States Federal Register public comment process and by the C2M2 Working Group. Updates to model practices were made to improve clarity and ease of implementation. A few examples of the changes resulting from this review include: • rewording of practices for clarity and consistency • removal of practices to eliminate duplication • addition of practices to improve the comprehensiveness of cybersecurity activities addressed by the model • reordering of the objectives in the Workforce Management domain to improve clarity
Renaming of objectives	Domain names were added to the name of each management objective. Selected objectives were renamed to better describe their intent and the practices included within them.
Enhancements to introductory material	Introductory text explaining model concepts and providing the context for interpretation of each domain was updated to ease understanding and implementation of the model.

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. Help text was enhanced for many practices.
Updated self-evaluation tools	The C2M2 self-evaluation tools[1] were updated for clarity and consistency. Additional visualizations were added to the tools to improve the ease of interpretation of self-evaluation results. The ability to compare results from multiple self-evaluations was added as well as the ability to load results from self-evaluations completed in previous versions of the PDF- or HTML-based tools. Both tools maintain all data on users' local machines.
Expansion of the C2M2 product suite	Additional documents have been created to assist organizations in the facilitation of C2M2 self-evaluation workshops, including a Self-Evaluation Guide, a C2M2 Overview presentation, a C2M2 Workshop Kickoff presentation, an example threat profile, and user guides for the self-evaluation tools. In addition, a guidance document has been developed for C2M2 users who are seeking CMMC certification.

[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.

1. INTRODUCTION

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

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

The C2M2 is designed to guide the development of a new cybersecurity program or for use with a self-evaluation methodology to enable an organization to measure and improve an existing cybersecurity program. Two C2M2 self-evaluation tools are available for free to any organization. These include a PDF-based tool and an HTML-based tool. Both tools may be obtained by visiting the DOE's C2M2 webpage.[2] Both tools maintain all data on users' local machines. A self-evaluation using one of the tools can be completed in one day, but the model could also be adapted for a more rigorous self-evaluation effort.

The C2M2 provides descriptive rather than prescriptive guidance. The model content is presented at a high level of abstraction so that it can be applied by organizations of various types, structures, sizes, and industries. Broad use of the model by a sector can support benchmarking of the sector's cybersecurity capabilities. 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 was developed with asset owners and operators in the electricity, oil, and natural

[2] 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.

gas industries, and can be used by organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. 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
- **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 the model (planning and managing changes in the organization based on the model)
- **Facilitators** with responsibility for leading a self-evaluation of the organization based on the model and an evaluation tool and analyzing the self-evaluation results[3]

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: Introduces the model and details the model's purpose, intended audience, and the organization of the content within this document.
- 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: Provides definitions for terms used in C2M2.
- 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 and Facilitators: Entire document

[3] For more information about the facilitator role, refer to the *C2M2 Self-Evaluation Guide*. The *C2M2 Self-Evaluation Guide* may be downloaded from the C2M2 program website 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 industry, private- sector, and public-sector experts. The initiative to update the C2M2 to Version 2.0, and now Version 2.1, operated under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework as a public-private partnership and included the formation of a working group consisting of energy sector cybersecurity practitioners. The update initiative leveraged and built upon existing efforts, models, and cybersecurity best practices to advance the model and address new technologies, practices, and changes in the threat environment.

Since the previous releases, additional strategic guidance has been provided by the White House through Presidential Executive Orders 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[4] 13636 "Improving Critical Infrastructure Cybersecurity,"[5] and 14028 "Improving the Nation's Cybersecurity."[6] C2M2, Version 2.1 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 2.1 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.

2.1 Model Development Approach

C2M2, Version 2.1 builds upon initial development activities and is enhanced through the following approach:

- *Public–private partnership:* Numerous government and industry partners participated in the development of this version, bringing a broad range of knowledge, skills, and experience to the team. The initial version of the 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.

[4] https://trumpwhitehouse.archives.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure
[5] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-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 emerging cyber threats to the energy sector. Leveraging related works helped to ensure that the model would be relevant and beneficial to the sector.
- *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, model practices tend to be abstract so that they can be interpreted for organizations of various structures, functions, and sizes.

3. CORE CONCEPTS

This section 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 a scale defining levels of maturity. C2M2 uses a scale of maturity indicator levels (MILs) 0–3, which are described in Section 4.3. 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 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 3.2.1). *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 multiple 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.

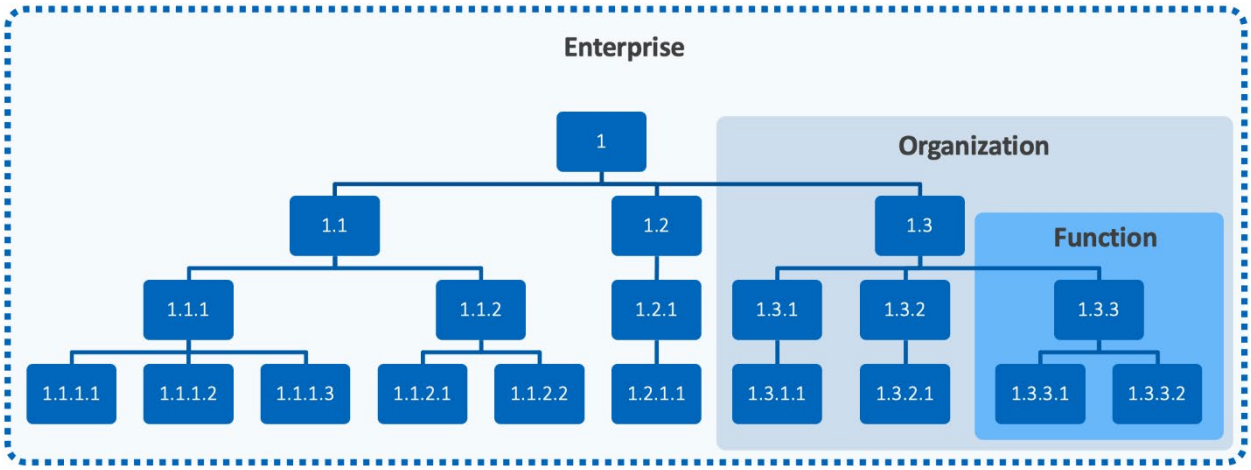

Figure 1: Example of the Structure of a Notional Entity

3.2.1 Function

In the model, the term *function* refers to the part of the organization that is being evaluated based on the model. It is common for an organization to use the model to evaluate a subset of its operations. The model broadly defines the function to allow organizations the greatest degree of flexibility in determining the scope of the self-evaluation that is appropriate for them. Functions can align with organizational boundaries, or they can align to a single product line or system. 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.

Selection of the function defines which IT, OT, and information assets will be in scope for the evaluation including interconnected or interdependent business and technology systems and the environment in which they operate. The function also defines the people who should participate in the self-evaluation. Specifically, appropriate participants should be included to ensure there is someone familiar with the way that the activities described in each of the C2M2 domains are implemented for the selected function.

Picking the right scope improves the accuracy of self-evaluation results. Selecting a scope that includes a part of the organization that manages cybersecurity homogenously avoids a situation where two different groups must combine two different responses into one. Care should be given to select a scope that provides a good balance between accuracy and time spent performing individual self-evaluations. A general rule for finding the right balance is to

identify the fewest number of self-evaluations that still provides an accurate picture of the organization's cybersecurity practices.

3.3 Assets

Many C2M2 practices refer to *assets*. For the purposes of the C2M2 model, the term *assets* includes all IT, OT, and information assets within the selected function, including interconnected or interdependent business and technology systems and the environment in which they operate. This may also include virtualized assets, regulated assets, cloud assets, and mobile assets. Additionally, this may include assets managed by a third party, software as a service, platform as a service, and infrastructure as a service, as well as public, private, or hybrid cloud assets.

3.3.1 IT Assets, OT Assets, and Information Assets

The C2M2 uses the following definitions when referring to IT assets, OT assets, and information assets:

- *IT assets:* 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 interdependent business and technology systems and the environment in which they operate.
- *OT assets:* OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.
- *Information assets:* Any communication or representation of knowledge such as facts, data, or opinions that is of value to the organization. Information Assets may be in any media or form, including digital or non-digital.

The following table provides examples of IT assets, OT assets, and Information assets.

Table 3: Examples of IT Assets, OT Assets, and Information Assets

Examples of IT Assets	Examples of OT Assets	Examples of Information Assets
▪ Workstations ▪ Switches, routers, and firewalls ▪ Servers ▪ Virtual machines ▪ Software ▪ Mobile computing devices ▪ Cloud assets	▪ Workstations ▪ Switches, routers, and firewalls ▪ Servers ▪ Virtual machines ▪ Software ▪ Mobile computing devices ▪ Cloud assets ▪ Programmable Logic Controllers ▪ Remote Terminal Units ▪ Industrial Control Systems (ICS) ▪ Safety Instrumented Systems ▪ Physical access control devices	▪ Business data ▪ Intellectual property ▪ Customer information ▪ Contracts ▪ Security logs ▪ Metadata ▪ Set points ▪ Operational data ▪ Financial records ▪ Security information and event management log files ▪ Historian data ▪ Configuration files

3.3.2 Additional Asset Subgroupings

In some cases, C2M2 practices refer to specific subgroupings of assets. These subgroupings focus on importance to the function and potential impact if accessed or misused by a threat actor. They may include any combination of IT, OT, and information assets. These subgroupings are defined as:

- *Assets that are important to the delivery of the function:* 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:* Assets that may be used in the pursuit of the tactics or goals of a threat actor that are of concern to the organization. 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. Examples of assets within the function that may be leveraged to accomplish a threat objective include:

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

A threat actor is any actor with the potential to adversely impact organizational operations or resources through IT, OT, or communications infrastructure. Threat objectives are the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage.

Threat actors may leverage multiple tactics or techniques, like those defined in MITRE ATT&CK [MITRE ATT&CK] or MITRE ATT&CK for Industrial Control Systems [MITRE ATT&CK for ICS]), to achieve their goals. Threat objectives may be described in an organization's threat profile and may change over time or in different situations. Threat objective examples include data manipulation, IP theft, damage to property, denial of control, loss of safety, or operational outage.

Note that an organization's inventory 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. 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.

- *All assets within the function:* All assets that operate or are used within the function. These assets may not be considered important to the delivery of the function and may not be likely to be leveraged to achieve a threat objective (for example, printers, radios, badge readers, or telephones).

The following figure is a visual depiction of how these subgroupings may be organized within a function.

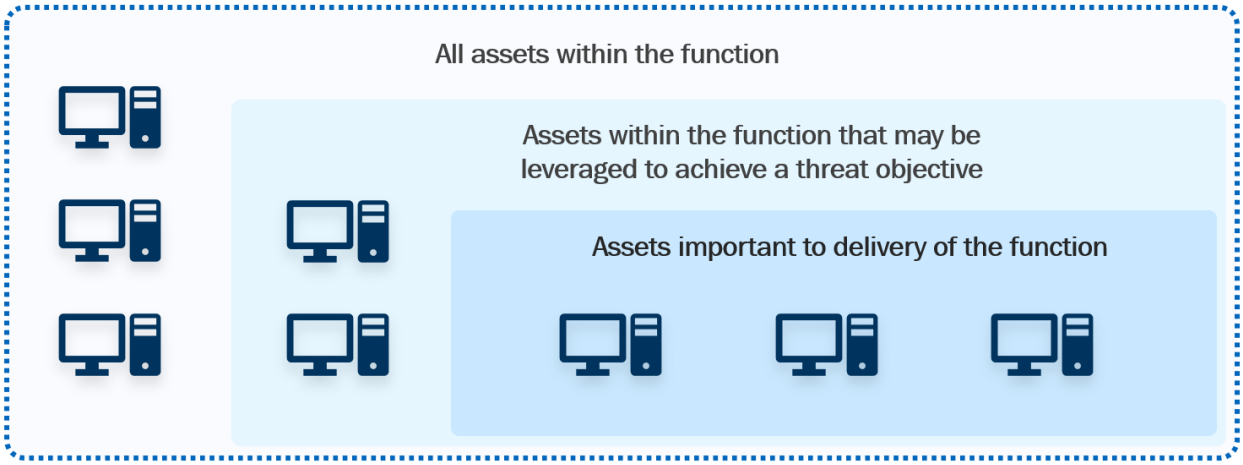

Figure 2: Groups of Assets

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 356 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 IT and OT Asset Configuration
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 3 summarizes the elements of each domain.

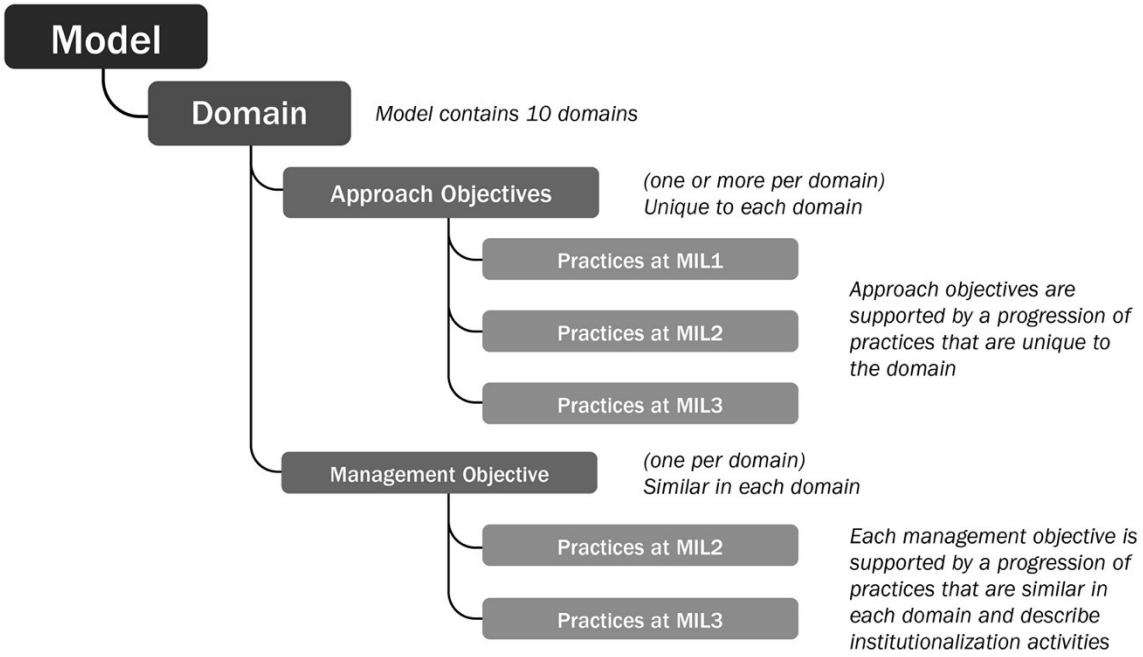

Figure 3: Model and Domain Elements

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 providing more context and introducing the practices. An example scenario is included in a sidebar. The purpose statement, introductory notes, and example are provided to help interpret 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, 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.

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—MIL0 through MIL3—are cumulative within each domain. To earn a MIL in a given domain, an organization must perform all practices in that level and in the preceding level. For example, an organization must perform all the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization must perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3. In the C2M2 self-evaluation tools, the practice is considered performed if a response of Fully Implemented or Largely Implemented is selected.
- 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 4: 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) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • 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, 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 to performance of the practice. High-quality outcomes may be achieved with experienced and talented personnel 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 may 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 defined in 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 within the function and is updated based on defined triggers.

Table 5: Example of Approach Progression in the ASSET Domain

1. Manage IT and OT Asset Inventory	
MIL1	a. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner
MIL2	b. The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective c. Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function d. Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective e. The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system, and firmware versions)
MIL3	f. The IT and OT asset inventory is complete (the inventory includes all assets within 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. 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 6: 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. Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel e. Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities f. The effectiveness of activities in the ASSET domain is evaluated and tracked

4.5 Enterprise-Focused Domains

As with all organizational functions and activities, a cybersecurity program operates in an enterprise context. The enterprise imposes requirements on the cybersecurity program in the form of mission, goals, and objectives, and in turn, provides some of the tools and capabilities that are needed for program success. Some enterprise functions, such as risk management, directly influence cybersecurity program decisions and actions, and require coordination to ensure shared goals can be achieved.

The C2M2 model is generally applied to a specific scope or organizational function. For example, an organization may decide to improve the cybersecurity posture of a particular line of business, or more directly, a key manufacturing process. Most C2M2 domains contain practices that can be operationalized in the context of this scope. However, three domains—Risk Management, Cybersecurity Architecture, and Cybersecurity Program Management—operate in an enterprise context in that they define practices that benefit all cybersecurity activities in the organization, regardless of the model scope.

Model users should recognize that these domains constitute enterprise programs that may be established and operate independently of the in-scope function. For this reason, the initial objective in each domain is focused on the establishment and maintenance of the related program, which addresses the:

- development of a strategy for the program
- governance over the program
- alignment of the program to the organization's mission and objectives
- coordination between the program and the strategy and objectives of related enterprise functions

Additionally, the initial objective in each domain includes practice references to align the domain's program strategy with other enterprise domains. For example, in the Risk

Management domain, the strategy for the cyber risk management program is established to support and align with the cybersecurity architecture program and cybersecurity program.

Each enterprise domain represents a set of practices that, when applied at a programmatic level, benefit and support the performance of the other C2M2 domains, as described below.

4.5.1 Cybersecurity Program Management

In this domain, a cybersecurity program is established to benefit and support the cybersecurity posture for all organizational functions and key assets. The program establishes strategy and structure for managing cybersecurity across the enterprise, provides for consistent application and integration of cybersecurity practices, and leverages cybersecurity resources and investments. Because the program operates at the enterprise level, it improves sponsorship from and involvement of senior leaders, streamlines resource requests, and benefits from consistent governance and oversight, particularly in the development and implementation of cybersecurity policies and directives. And, as an enterprise-wide function, it improves the effectiveness of the Risk Management and Cybersecurity Architecture domains that inherit the advantages of senior-level participation in the cybersecurity effort.

4.5.2 Risk Management

In this domain, the organization establishes a cyber risk management program that supports the risk management activities of other C2M2 domains, in alignment with the organization's enterprise risk management function. The Risk Management domain broadly defines a cybersecurity risk management lifecycle that addresses cyber risks that could affect the resiliency of key assets (as defined in the Asset, Change, and Configuration Management domain) and provides a universal and consistent method for analyzing and responding to these risks. From a C2M2 model perspective, the Risk Management domain provides the enterprise-wide process and practices to address risk that arises from known threats and vulnerabilities (Threat and Vulnerability Management), third-party relationships (Third-Party Risk Management), and weaknesses in the organization's systems and networks (Cybersecurity Architecture), or from any process that negatively affects the organization's cybersecurity posture.

4.5.3 Cybersecurity Architecture

The cybersecurity architecture represents the organization's plan for actualizing the cybersecurity objectives in the Cybersecurity Program Management strategy. It provides for the definition of cybersecurity requirements to protect key assets, and the design and engineering of tools, technologies, processes, and controls that improve and sustain the organization's cybersecurity posture. Because the cybersecurity architecture operates in the context of other enterprise systems, applications, and networks, it can take advantage of existing key resources and competencies while building additional capabilities that are required to address cybersecurity challenges. The enterprise orientation also provides first-hand awareness of and response to organizational changes that could affect the effectiveness of existing cybersecurity controls or identify gaps that create exploitable weaknesses and exposures that must be addressed as known organizational risks.

4.6 Considerations for the Cybersecurity Architecture Domain

To better understand the objectives and practices in the Cybersecurity Architecture domain, the fundamental definition and features of a cybersecurity architecture must be understood.

4.6.1 Cybersecurity Architecture Defined

A cybersecurity architecture is a framework that defines the organization's system of tools, techniques, methods, and controls that ensure cyber threats can be prevented, detected, and corrected across all levels and layers of information and operational technologies (IT and OT). The cybersecurity architecture is a fundamental component of the organization's enterprise architecture which, in simple terms, defines, documents, and standardizes the IT and OT infrastructure that supports business needs, goals, and objectives. Because the cybersecurity architecture operates within the enterprise architecture, these frameworks must align and integrate, and the cybersecurity architecture must objectively ensure the operational consistency, reliability, and continuity of the enterprise architecture.

4.6.2 Cybersecurity Architecture Framework

In practice, a cybersecurity architecture is typically documented through a series of reference diagrams that establish a plan for and working definition of the organization's cybersecurity infrastructure and the way in which it aligns with and integrates to the IT and OT infrastructure.

Details of the cybersecurity architecture are often established as a series of requirements described in reference architectures. For example, a reference architecture for securing mobile computing (such as the use of phones and tablets) may establish the requirements, acceptable technologies, and controls for connecting devices to wireless routers, including acceptable encryption methodologies, and guidelines for segmentation of mobile network traffic into subnets that can be monitored with more granular policies and rulesets.

The cybersecurity architecture must be comprehensive and inclusive of all potential types of platforms (such as cloud, IoT, mobility, networks, endpoints, and external connections), systems (such as in-house applications and applications-as-a-service), data (stored, transmitted, and processed in-house or in the cloud), and operational technologies (such as field automation devices, industrial control systems, and physical security components).

4.6.3 Implementing the Cybersecurity Architecture

The cybersecurity architecture establishes the organization's plan for securing the IT and OT infrastructure and contributing to its resiliency when threatened or compromised. In operation, the cybersecurity architecture guides the selection of tools, techniques, methods, and controls to meet the organization's cybersecurity objectives. For example, a cybersecurity architecture may include a defense-in-depth strategy that reflects specific tools and technologies for perimeter defense (such as firewalls, intrusion prevention and detection, demilitarized zones (DMZs)), web traffic filtering (such as proxies, web filters, content filtering), and endpoint protection (such as antivirus, antimalware, data loss prevention).

The cybersecurity architecture also serves as a compliance reference as changes occur in the IT and OT infrastructure or as cybersecurity objectives change. These changes may result from many sources, including upgrading of technologies, sunsetting of old technologies, changes in business structure, new business initiatives, merger and acquisition activity, or regulatory changes. In addition, changes to the cybersecurity and IT and OT infrastructure may be informed by perceived threats and vulnerabilities, or events and incidents that the organization has experienced. Many organizations establish an architecture review board or similar group to provide collaborative discussion, consideration, and approval of proposed technology changes. For all proposed changes, the architecture review board examines the change or reconfiguration of existing technologies or addition of any new technology with reference to the cybersecurity and enterprise architectures to ensure proper interoperability, preservation of controls, continuity of operation, maintainability, and limited impact on user functionality.

4.6.4 Considering the Cybersecurity Architecture in C2M2

The objectives and practices in the Cybersecurity Architecture domain ensure that the organization establishes a strategy and plan that reflects their cybersecurity objectives, is implemented in alignment with the organization's enterprise architecture, and provides proper oversight as changes are proposed and made. The domain's practices also reflect foundational controls expected in a cybersecurity architecture (such as segmenting IT and OT networks) and proper coverage of infrastructure layers (IT and OT assets, networks, software, and data). Finally, support practices that establish mechanisms such as documentation, policy, and accountability are included to ensure the architecture is properly institutionalized as part of the organization's security culture.

4.7 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 an authoritative 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 list as indicating a minimum baseline or as an exhaustive list of what might be considered for implementation of a practice.

Example: ASSET-1e

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

Figure 4: Example List Included in Practice ASSET-1e

4.8 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 5 shows an example from the first objective in the Asset, Change, and Configuration Management domain. The objective's first practice, "IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner," 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. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner
MIL2	b. The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective c. Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function d. Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective e. The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system, and firmware versions)
MIL3	f. The IT and OT asset inventory is complete (the inventory includes all assets within 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. Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life

Figure 5: 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 6 summarizes a potential approach for using the model. An organization performs a self-evaluation against the model, uses that self-evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves the process is repeated. Each step in this approach is described in the following sections.

Figure 6: Potential Approach for Using the Model

5.1 Step 1: Perform a Self-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 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, increases shared situational awareness of relevant cybersecurity risks and concrete steps to mitigate them using the model practices, and

offers an opportunity to clarify roles and responsibilities. More thorough guidance on preparing to use the model, selecting a facilitator, and scoping the self-evaluation can be found in the supporting *C2M2 Self-Evaluation Guide*.[7]

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 7 includes a description for each self-evaluation response option.

Table 7: 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[8] 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. It is important to note that the self-evaluation report may include sensitive information and should be protected accordingly.

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

[7] The *C2M2 Self-Evaluation Guide* may be downloaded from the C2M2 program website https://www.energy.gov/C2M2.
[8] 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.

MIL rating for each domain in the model. This collection of desired capabilities is the organization's target profile.

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 a self-evaluation. An appropriate mix of organizational stakeholders should be included in the selection of 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 representing business, technology, and operational considerations from across the organization.

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 may help to 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 8: Inputs, Activities, and Outputs: Breakdown of Potential Approach

	Inputs	Activities	Outputs
1. Perform a Self-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. Develop a target profile 2. Analyze gaps 3. Evaluate potential consequences from gaps 4. 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 IT and OT Asset Configuration
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

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.

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 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.

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. IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner
MIL2	b. The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective c. Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function d. Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective e. The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system, and firmware versions)
MIL3	f. The IT and OT asset inventory is complete (the inventory includes all assets within 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. 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. Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner
MIL2	b. The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective c. Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function d. Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective e. The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements)
MIL3	f. The information asset inventory is complete (the inventory includes all assets within 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. Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements

3. Manage IT and OT 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 c. Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f) d. Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture
MIL3	e. Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles

4. Manage Changes to IT and OT Assets

MIL1	a. Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner b. Changes to assets are documented, at least in an ad hoc manner
MIL2	c. Documentation requirements for asset changes are established and maintained d. Changes to higher priority assets are tested prior to being deployed e. Changes and updates are implemented in a secure manner f. The capability to reverse changes is established and maintained for assets that are important to the delivery of the function g. Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)
MIL3	h. Changes to higher priority assets are tested for cybersecurity impact prior to being deployed i. Change logs include information about modifications that impact the cybersecurity requirements of assets

5. Management Activities for the ASSET domain

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. Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel e. Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities 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. This includes actors without intention to cause adverse impact (e.g., insider mistakes).

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.

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.

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 for the THREAT domain

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 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 or other mitigations i. Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders
MIL3	j. Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored k. Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function l. Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective m. Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications

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. Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner c. Threat objectives for the function are identified, at least in an ad hoc manner d. Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner
MIL2	e. A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets) f. Threat information sources that collectively address all components of the threat profile are prioritized and monitored g. Identified threats are analyzed and prioritized and are addressed accordingly h. Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs])
MIL3	i. The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events j. Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g) k. Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action

3 Management Activities for the THREAT domain

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. Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel e. Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities 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 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 for the RISK domain

The Risk Management domain is an enterprise focused domain. The activities described in enterprise focused domains are often performed as part of an enterprise-wide program and may be established and operate independently of the in-scope function. To account for this, the initial objective in each enterprise-focused domain is focused on the establishment and maintenance of the related program.

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.

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.

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. 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 in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture c. The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy d. Information from RISK domain activities is communicated to relevant stakeholders e. Governance for the cyber risk management program is established and maintained f. Senior management sponsorship for the cyber risk management program is visible and active
MIL3	g. The cyber risk management program aligns with the organization's mission and objectives h. The cyber risk management program is coordinated with the organization's enterprise-wide risk management program

2. Identify Cyber Risk

MIL1	a. Cyber risks are identified, at least in an ad hoc manner
MIL2	b. A defined method is used to identify cyber risks c. Stakeholders from appropriate operations and business areas participate in the identification of cyber risks d. Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level 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, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction i. Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified 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. Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks m. Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent 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 risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance) c. A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification) d. Defined methods are used to analyze higher priority 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 participate in the analysis of higher priority cyber risks f. Cyber risks are removed from the risk register or other artifact used to document and manage identified risks 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, external events, and information from other model domains

4. Respond to Cyber Risk

MIL1	a. Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address 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 for the RISK domain

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
MIL3	c. Up-to-date policies or other organizational directives define requirements for activities in the RISK domain d. Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel e. Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities 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 Identities and Manage Authentication
2. Control Logical Access
3. Control Physical Access
4. Management Activities for the ACCESS domain

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, their 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 Identities and Manage Authentication

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. Password strength and reuse restrictions are defined and enforced e. Identity repositories are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure f. Identities are deprovisioned within organization-defined time thresholds when no longer required g. The use of privileged credentials is limited to processes for which they are required h. Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)
MIL3	i. Multifactor authentication is required for all access, where feasible j. Identities are disabled after a defined period of inactivity, where feasible

2. Control Logical Access

MIL1	a. Logical access controls are implemented, at least in an ad hoc manner b. Logical access privileges are revoked when no longer needed, at least in an ad hoc manner
MIL2	c. Logical access requirements are established and maintained (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 the principle of separation of duties f. Logical access requests are reviewed and approved by the asset owner g. Logical access privileges that pose higher risk to the function receive 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 logical 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 privileges are 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 established and maintained (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 requirements incorporate the principle of separation of duties g. Physical access requests are reviewed and approved by the asset owner h. Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring
MIL3	i. Physical access privileges are reviewed and updated j. Physical access is monitored to identify potential cybersecurity events

4. Management Activities for the ACCESS domain

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. Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel e. Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities 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 for the SITUATION domain

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.

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.

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 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 that are important to the delivery of the function, at least in an ad hoc manner
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 IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective d. Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) e. Log data are being aggregated within the function
MIL3	f. More rigorous logging is performed for higher priority assets

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. Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, 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-2e)
MIL3	g. More rigorous monitoring is performed for higher priority assets h. Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity i. 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. Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness f. A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function g. 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

4. Management Activities for the SITUATION domain

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. Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel e. Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities 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 Incidents
4. Address Cybersecurity in Continuity of Operations
5. Management Activities for the RESPONSE domain

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. Identification of cybersecurity events and incidents may incorporate data from several sources including the outputs of activities performed in other domains, such as the outputs of Situational Awareness domain activities. Cybersecurity events may originate with or impact third parties necessitating coordination in response planning, execution, and communications.

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.

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

Responding to cybersecurity incidents requires the organization to have a process to limit the impact of cybersecurity incidents on 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. Incident response plans should be comprehensive of the types of incidents that may affect the organization (e.g., ransomware, denial of service, operational disruption). Incident response plans should also address potential incidents that may significantly impact the organization, such as major vulnerability disclosures and emerging technologies that would reduce the effectiveness of current cybersecurity controls (e.g., quantum computing). Conducting lessons-learned reviews as a part of cybersecurity event and incident response and continuity of operations helps the organization address the potential issues (e.g., vulnerabilities, control gaps, and process deficiencies) that led to the incident and prioritize future long-term improvement efforts.

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 the potential impacts of cybersecurity incidents and lessons learned from previous incidents. 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 documented, 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 documented 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 and the organization's threat profile (THREAT-2e) 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 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 documented and tracked to closure g. Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)
MIL3	h. Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b) i. Cybersecurity incidents are correlated to identify patterns, trends, and other common features across multiple incidents

3. Respond to Cybersecurity Incidents

MIL1	a. Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner b. Responses to cybersecurity 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 incident response is executed according to defined plans and procedures f. Cybersecurity incident response plans include a communications plan for internal and external stakeholders g. Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events h. Cybersecurity incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan
MIL3	i. Cybersecurity incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan j. Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation k. Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations l. Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g)

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. Continuity plans address potential impacts from cybersecurity incidents 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 that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets g. Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans h. Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel i. Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events j. Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data k. Data backups are logically or physically separated from source data l. Spares for selected IT and OT assets are available
	m. Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats n. Continuity plan exercises address higher priority risks o. The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly p. Continuity plans are periodically reviewed and updated

5. Management Activities for the RESPONSE domain

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. Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel e. Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities 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, quality assurance, and availability. The autonomy organizations often give to their individual business units further increases the risk, unless contracting and purchasing 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 for the THIRD-PARTIES domain

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 to determine the adequacy of requirements related to cyber risk, 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 that are important to the delivery of the function are identified, at least in an ad hoc manner
MIL2	c. A defined method is followed to identify risks arising from suppliers and other third parties d. 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) e. 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	f. 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 (for example, vulnerability notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties 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 for products 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. Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software l. Selection criteria for higher priority assets include evaluation of any associated third-party hosting environments and source data m. Acceptance testing of procured assets includes consideration of cybersecurity requirements

3. Management Activities for the THIRD-PARTIES domain

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. Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel e. Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities 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. Implement Workforce Controls
2. Increase Cybersecurity Awareness
3. Assign Cybersecurity Responsibilities
4. Develop Cybersecurity Workforce
5. Management Activities for the WORKFORCE domain

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.

Implementing workforce controls includes personnel vetting, personnel separation procedures, and acceptable use agreements. Additional controls may be appropriate for positions deemed to pose higher potential risk to the organization, such as those 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 additional measures may need to be 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. Personnel and contractors should receive periodic security awareness training to reduce their vulnerability to social engineering and other threats. 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 or unintentionally disclosing login credentials 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. The effectiveness of cybersecurity awareness activities should be evaluated periodically, and improvements should be made as needed.

Assigning cybersecurity responsibilities begins with identifying the key cybersecurity responsibilities necessary to support the organization's operational and risk management goals. Identified cybersecurity responsibilities can then be assigned to job roles and documented. Workforce planning helps ensure adequate resources are available to fulfill key cybersecurity workforce roles. 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, human resource professionals may react to cybersecurity skill deficiencies within the organization by prioritizing specific cybersecurity skills while performing recruiting and interviewing activities. Also, personnel (and contractors) should receive periodic security awareness training to reduce their vulnerability to social engineering and other threats. The effectiveness of training and awareness activities should be evaluated, and improvements should be made as needed.

Objectives and Practices

1. 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 at hire and periodically for positions that have access to assets that are important to the delivery of the function d. Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate e. Personnel 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

2. Increase Cybersecurity Awareness

MIL1	a. Cybersecurity awareness activities occur, at least in an ad hoc manner
MIL2	b. Cybersecurity awareness objectives are established and maintained c. Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e) d. Cybersecurity awareness activities are conducted periodically
MIL3	e. Cybersecurity awareness activities are tailored to job role f. Cybersecurity awareness activities address predefined states of operation (SITUATION-3g) g. 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

3. 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

4. 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. Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts d. Cybersecurity training is provided as a prerequisite to granting access to assets that are important to 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

5. Management Activities for the WORKFORCE domain

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. Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel e. Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities 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 for the ARCHITECTURE domain

The Cybersecurity Architecture domain is an enterprise focused domain. The activities described in enterprise focused domains are often performed as part of an enterprise-wide program and may be established and operate independently of the in-scope function. To account for this, the initial objective in each enterprise-focused domain is focused on the establishment and maintenance of the related program.

The cybersecurity architecture helps an organization plan the way security is to be engineered in a holistic and integrated manner. It facilitates a proactive and reasoned

Example: Cybersecurity Architecture

Anywhere Inc. has recognized that its current cybersecurity control environment is not sufficient to maintain its cybersecurity risk management objectives. Anywhere Inc. performs an assessment of its cybersecurity program and determines that many identified gaps stem from a lack of proactive planning and an uncoordinated approach to selection of cybersecurity improvement initiatives. To strengthen its cybersecurity posture, Anywhere Inc. has documented a target cybersecurity architecture. Anywhere Inc. plans to use the architecture as part of its cybersecurity project selection process and vendor proposal evaluation criteria.

The target cybersecurity architecture provides a blueprint for the cybersecurity risk management outcomes that Anywhere Inc. has determined it wants to achieve. Using an architecture-centric approach, Anywhere is able to identify the right tradeoffs to meet an acceptable level of risk tolerance. For example, the benefits of layered defenses (virtual private network (VPN), firewalls, and access controls) can be weighed against the costs of implementing and maintaining those controls.

In this way, Anywhere has better information about how potential cybersecurity improvement efforts impact its overall risk posture and the degree to which those efforts enable achievement of its operational and cybersecurity goals.

approach to planning for future security improvements for assets, systems, and the enterprise as a whole. Architectural controls may focus on several important cybersecurity capabilities for an enterprise such as detecting, resisting, reacting to, and recovering from attacks. Such tactics include segmentation, cryptographic controls, monitoring, and redundancy. Additionally, because a cybersecurity architecture is a forward-looking tool for planning, consideration should be given not only to current technology trends but also to potential future developments such as quantum computing and the associated risks it may pose to existing encryption systems. For the cybersecurity architecture to be effective, those responsible for it must be included in planning and decision-making processes when changes to the organization, IT systems, or OT systems are being considered. In this way, changes to the organization can be reviewed to address security concerns and to ensure the end result aligns with the organization's cybersecurity 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 in alignment with 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 process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process e. Senior management sponsorship for the cybersecurity architecture program is visible and active f. The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets g. Cybersecurity controls are selected and implemented to meet cybersecurity requirements
MIL3	h. The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program i. 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 j. The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e) k. The cybersecurity architecture addresses predefined states of operation (SITUATION-3g)

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

MIL1	a. Network protections are implemented, at least in an ad hoc manner b. 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	c. 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) d. Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements e. Network protections incorporate the principles of least privilege and least functionality f. Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) g. Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking)
	h. All assets are segmented into distinct security zones based on cybersecurity requirements i. Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication j. OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems 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. Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner b. Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner
MIL2	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 established and maintained 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 are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible i. Maintenance and capacity management activities are performed for all assets within the function j. The physical operating environment is controlled to protect the operation of assets within the function k. More rigorous cybersecurity controls are implemented for higher priority assets
MIL3	l. Configuration of and changes to firmware are controlled throughout the asset lifecycle m. Controls (such as allowlists, blocklists, and configuration settings) 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 is developed using secure software development practices b. The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices c. Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house
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 c. All data in transit is protected for selected data categories d. Cryptographic controls are implemented for data at rest and data in transit for selected data categories 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 for the ARCHITECTURE domain

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
	c. Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain d. Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel e. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities 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. Establish and Maintain Cybersecurity Program
3. Management Activities for the PROGRAM domain

The Cybersecurity Program Management domain is an enterprise-focused domain. The activities described in enterprise focused domains are often performed as part of an enterprise-wide program and may be established and operate independently of the in-scope function. To account for this, the initial objective in each enterprise-focused domain is focused on the establishment and maintenance of the related program.

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.

Example: Cybersecurity Program Management

Anywhere Inc. decided to establish an enterprise cybersecurity program. To begin, Anywhere Inc. formed a cybersecurity governance board with leaders from business and operations functions. This 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 Anywhere Inc.'s 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 collaborate with the cybersecurity governance board to expand and document the cybersecurity program strategy for Anywhere Inc., ensuring that it aligns with the organization's business strategy and addresses its risk to critical infrastructure. After the strategy is approved by the Board of Directors, the new vice president will work with the cybersecurity governance board to implement the program by reorganizing some existing compartmentalized cybersecurity teams and recruiting additional team members to address skill gaps in the organization.

The new program will guide the Anywhere Inc. leadership team in integrating cybersecurity practices into functions across the enterprise including human resources, accounting, engineering, public relations and legal. For example, the new program will guide the human resources team in identifying points in the employee life cycle where cybersecurity practices should be implemented (such as, recruiting, vetting, onboarding, and separation).

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.

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 mission, 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, PCI DSS, ISO, DoD CMMC)
MIL3	h. The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile (THREAT-2e)

2. Establish and Maintain Cybersecurity Program

MIL1	a. Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner
MIL2	b. The cybersecurity program is established according to the cybersecurity program strategy c. Senior management sponsorship for the cybersecurity program is visible and active d. Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies e. Responsibility for the cybersecurity program is assigned to a role with sufficient authority f. Stakeholders for cybersecurity program management activities are identified and involved
MIL3	g. Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy h. Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes i. The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate j. 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 for the PROGRAM domain

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. Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel e. Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities f. The effectiveness of activities in the PROGRAM domain is evaluated and tracked

APPENDIX A: REFERENCES

The 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

[CMMC]
Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, and Futures, Inc. 2020. *Cybersecurity Maturity Model Certification (CMMC) Model Overview*. Retrieved March 31, 2022, from: https://www.acq.osd.mil/cmmc/documentation.html

[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

[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/screspons e/repository/rice_tenney_SCS_RMM_june-july_2007.pdf

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

[MITRE ATT&CK for ICS]
The MITRE Corporation. 2021. MITRE ATT&CK for Industrial Control Systems. Retrieved April 14, 2022, from https://collaborate.mitre.org/attackics/index.php/Main_Page

[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 SP800-30]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2012. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1.0). National Institute of Standards and Technology. Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[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. 2020. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Revision 5). Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/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

[NISTIR 8276)
Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. 2021. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (NISTIR 8276). National Institute of Standards and Technology. Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/nistir/8276/final

[PPD-21]
The White House. n.d. *Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience*. Retrieved May 30, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[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.

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. High-quality outcomes may be achieved with experienced and talented personnel, 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 may result in documented artifacts such as a documented asset inventory or a documented cybersecurity program strategy.	C2M2
all assets within the function	All assets that operate or are used within the function. These assets may not be considered important to the delivery of the function and may not be likely to be leveraged to achieve a threat objective (for example, printers, radios, badge readers, or telephones).	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.*	
assessment	See *risk assessment.*	

Term	Definition	Source
asset	For the purposes of the model, assets are IT and OT hardware and software assets, as well as information essential to operating the function. The definition also includes interconnected or interdependent business and technology systems and the environment in which they operate.	C2M2
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 that are 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 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 that are of concern to the organization. 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. A threat actor may leverage multiple tactics, like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems), to achieve their ultimate threat objectives (for example, extortion, data manipulation, IP theft, customer data theft, sabotage). 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 assets that if compromised, may allow lateral movement within an organization's network • assets with administrative rights that would enable privilege escalation • information assets such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed See also *threat objective*.	C2M2
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

Term	Definition	Source
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
capacity management	Planning adequate budget, equipment, and tools to meet current and future operational needs of the organization.	C2M2
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
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]

Term	Definition	Source
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 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
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

Term	Definition	Source
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 function to which the C2M2 is being applied. Some enterprises may consist of multiple organizations (e.g., a holding company with one or more operating companies). Other enterprises 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* and *function.*	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
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, implementation, and ongoing support of the object of the practice (such as a program). Development and implementation would typically result in documentation that captures important information about the activity. Ongoing support would typically result in periodic reviews and updates when events occur that may impact operations (such as major changes to IT and OT assets or change to the threat environment). 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 kept up to date including review, corrective actions, addressing changes in requirements, and improvements.	Adapted from CERT-RMM

Term	Definition	Source
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* refers to the part of the organization that is 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
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

Term	Definition	Source
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, intellectual property, customer information, 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 interdependent business and technology 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
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

Term	Definition	Source
logging	Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. 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)
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

Term	Definition	Source
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)	In the context of the model, OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. 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. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.	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
periodically and according to defined triggers	A review or activity that occurs at defined, regular time intervals and at the occurrence of defined events. The organization-defined frequency and threshold values are commensurate with risks to organizational objective 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
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

Term	Definition	Source
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
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

Term	Definition	Source
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
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
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

Term	Definition	Source
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 aid human comprehension and allow 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
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

Term	Definition	Source
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
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
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
threat	Any actor 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. This includes actors without intention to cause adverse impact (e.g., insider mistakes).	Adapted from DOE RMP
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	Threat objectives are the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage. Threat actors may leverage multiple tactics or techniques, like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems) to achieve their goals. Threat objective examples include data manipulation, intellectual property theft, damage to property, denial of control, loss of safety, and operational outage.	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

Term	Definition	Source
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
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.	Adapted from NISTIR 7628 Vol. 1, pp. 8
vulnerability assessment	Systematic examination of IT or OT assets or systems 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. This may include several types of assessments, such as a paper-based assessment, tool-based vulnerability scanning, and penetration tests.	DOE RMP
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
C2M2	Cybersecurity Capability Maturity Model
CCPA	California Consumer Privacy Act
CERT®-RMM	CERT® Resilience Management Model
CISA	Cybersecurity and Infrastructure Security Center
CMMC	Cybersecurity Maturity Model Certification
COTS	commercial off-the-shelf
CSF	NIST Framework for Improving Critical Infrastructure Cybersecurity
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DoD	Department of Defense
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
ISO	International Organization for Standardization
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
OT	operations technology
PCI DSS	Payment Card Industry Data Security Standards
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline
SCADA	supervisory control and data acquisition

Acronym	Definition
SEI	Software Engineering Institute
SLA	service level agreement
TTP	tactics, techniques, and procedures
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.