# CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

**Version 2.0**

June 2019

# TABLE OF CONTENTS

Acknowledgments ... iii
Change Log ... iv
1. Introduction ... 1
1.1 Intended Audience ... 1
1.2 Document Organization ... 2
2. Background ... 4
2.1 Model Development Approach ... 4
3. Core Concepts ... 6
3.1 Maturity Models ... 6
3.2 Critical Infrastructure Objectives ... 6
3.3 Function ... 7
3.4 Assets ... 8
4. Model Architecture ... 9
4.1 Domains ... 9
4.2 Maturity Indicator Levels ... 11
4.2.1 Approach Progression ... 12
4.2.2 Management Progression ... 13
4.2.3 Summary of MIL Characteristics ... 15
4.3 Practice Reference Notation ... 15
5. Using the Model ... 17
5.1 Prepare to Use the Model ... 17
5.2 Prioritize and Scope ... 18
5.3 Orient ... 19
5.4 Create a Current Profile ... 19
5.5 Conduct a Risk Assessment ... 21
5.6 Create a Target Profile ... 21
5.7 Determine, Analyze, and Prioritize Gaps ... 22
5.8 Implement Action Plan ... 23
6. Model Domains ... 25
6.1 Risk Management (RISK) ... 25
6.2 Asset, Change, and Configuration Management (ASSET) ... 28
6.3 Identity and Access Management (ACCESS) ... 31
6.4 Threat and Vulnerability Management (THREAT) ... 34
6.5 Situational Awareness (SITUATION) ... 37
6.6 Event and Incident Response (RESPONSE) ... 40
6.7 Supply Chain and External Dependencies Management (DEPENDENCIES) ... 43
6.8 Workforce Management (WORKFORCE) ... 46
6.9 Cybersecurity Architecture (ARCHITECTURE) ... 50
6.10 Cybersecurity Program Management (PROGRAM) ... 54

# TABLE OF CONTENTS

APPENDIX A: Practice Guidance ..... 58
APPENDIX B: V1.1 to V2.0 Mapping ..... 59
APPENDIX C: References ..... 60
APPENDIX D: Glossary ..... 67
APPENDIX E: Acronyms ..... 84
NOTICES ..... 86

# LIST OF FIGURES

Figure 1: Model and Domain Elements ..... 10
Figure 2: Referencing an Individual Practice, Example: RISK-2a ..... 16
Figure 3: Recommended Approach for Using the Model ..... 17
Figure 4: Objective View Example ..... 20
Figure 5: Domain View Example ..... 20
Figure 6: C2M2 Inputs, Outputs, and Activities ..... 24

# LIST OF TABLES

Table 1: Recommended Document Sections per Stakeholder Role ..... 2
Table 2: Example of Approach Progression in the Cybersecurity Program Management Domain ..... 13
Table 3: Summary of Maturity Indicator Level Characteristics ..... 15

# ACKNOWLEDGMENTS

The U.S. Department of Energy (DOE) developed the Cybersecurity Capability Maturity Model (C2M2) from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0 by removing sector-specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the DOE, in partnership with the U.S. Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts.

The DOE acknowledges the dedication and technical expertise of all the organizations and individuals who participated in the development of ES-C2M2, as well as the organizations and individuals from different sectors who have provided the critiques, evaluations, and modifications in order to produce this new release of the C2M2.

### Program Lead

**Jeffrey Baumgartner**
Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

### Program Team

**Jeffrey Hood**, BCS, LLC
**Timothy Kocher**, Department of Energy
**Benjamin Steinberg**, Department of Energy
**Daniel Lagraffe**, Department of Energy

### Model Version 2 Architecture Team and Contributors

| | | |
|---|---|---|
| Brian David Benestelli, SEI | Dale Gonzalez, Axio | Jason Nations, OGE Energy |
| Kaitlin Brennan, EEI | Walt Grudzinski | Alexander Petrilli, SEI |
| Jason Christopher, Axio | Cynthia Hsu, NRECA | Jeff Pinckard, SEI |
| Linda Conrad, Exelon | Tamara Lance, Atmos Energy | Sara Ricci, NYPA |
| Pamela Curtis, Axio | Annabelle Lee, Nevermore Security | Christopher Taylor, Southern Co. |
| Patrick Donohoe, SEI | Jim Linn, AGA | Matt Trevors, SEI |
| Brendan T. Fitzpatrick, Axio | Samara Moore, Exelon | Jason Tugman |
| John Fry, Ernst & Young | Manny Moyosore | David White, Axio |
| Kegan Gerard, EEI | Julia Mullaney, SEI | |

# CHANGE LOG

| V1.1 | V2.0 |
| --- | --- |
| | |
| | |
| | |
| | |
| | |
| | |

# 1. INTRODUCTION

Repeated cyber intrusions into organizations of all types demonstrate the need for improved cybersecurity. Cyber threats continue to grow, and they represent one of the most serious operational risks facing modern organizations. National security and economic vitality depend on the reliable functioning of critical infrastructure and the sustained operation of organizations of all types in the face of such threats. The Cybersecurity Capability Maturity Model (C2M2) can help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience.

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

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

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

## 1.1 Intended Audience

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

[1] The C2M2 Toolkit may be obtained by sending a request to C2M2@doe.gov.

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

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

## 1.2 Document Organization

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

Stakeholders may benefit by focusing on specific sections of this document, as outlined in Table 1. Beyond these recommendations, all readers may benefit from understanding the entire document.

**Table 1: Recommended Document Sections per Stakeholder Role**

| Role | Recommended Document Sections |
|---|---|
| Decision makers | Chapters 1, 2, and 3 |
| Leaders or managers | Chapters 1, 2, 3, and 4 |
| Practitioners | Entire document |
| Facilitators | Entire document |

Chapter 2 provides background about the stakeholders who collaborated on the C2M2 and themes that characterized its development. Chapter 3 describes several core concepts that are important for interpreting the content and structure of the C2M2. Chapter 4 describes the architecture of the C2M2. Chapter 5 provides guidance on how to use the model. Chapter 6 contains the model itself—the model's objectives and practices, organized into domains. Appendix A provides guidance in interpreting the practices. Appendix B is a mapping showing how V1.1 practices correspond to V2.0 practices. Appendix C includes references that were either used in the development of this document or provide further information about the

[2] The sponsor of the self-evaluation should be a decision maker from the organization. For more information about the sponsor role, please refer to the C2M2 Facilitator Guide. The Facilitator Guide may be downloaded from http://energy.gov/node/795826.

[3] Subject matter experts (SMEs) for the self-evaluation should be leaders or practitioners. For more information about the SME role, please refer to the C2M2 Facilitator Guide. The Facilitator Guide may be downloaded from http://energy.gov/node/795826.

[4] For more information about the facilitator role, please refer to the C2M2 Facilitator Guide. The Facilitator Guide may be downloaded from http://energy.gov/node/795826.

practices identified within the model. Appendix D is the Glossary. Appendix E defines the acronyms used in this document.

# 2. BACKGROUND

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

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

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

## 2.1 Model Development Approach

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

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

[5] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[6] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

review of cyber threats to the subsector. Leveraging related works shortened the development schedule and helped to ensure that the model would be relevant and beneficial to the subsector.

- ***Descriptive, not prescriptive:*** This model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be abstract so that they can be interpreted for organizations of various structures, functions, and sizes.
- ***Fast-paced development:*** The new version focused on quickly developing a model that would provide value to the sector and be available for continued capability evaluation that strengthens the cybersecurity posture of the energy sector to meet the changing environment.

# 3. CORE CONCEPTS

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

## 3.1 Maturity Models

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

A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. Also, when a model is widely used in a particular industry (and assessment results are 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 "levels" along a scale. C2M2 uses a scale of maturity indicator levels (MILs) 0–3, which are described in Section 4.2. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

- Define its current state
- Determine its future, more mature state
- Identify the capabilities it must attain to reach that future state

## 3.2 Critical Infrastructure Objectives

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

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

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

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

## 3.3 Function

It is recommended that an organization use the model to evaluate a subset of its operations. In this model, the term *function* is used to refer to that subset. As stated earlier, the C2M2 focuses on the implementation and management of cybersecurity practices associated with the information, information technology (IT), and operations technology (OT) *assets* and the *environments* in which they operate. Selecting the function that will be the focus of a C2M2 evaluation determines the specific assets and people, which together constitute the function's operating environment, to be evaluated.

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

Some things to consider when defining the function are:

- its significance to the organization's mission
- its stakeholders
- its supporting assets
- whether the organization has identifiable ownership (i.e., authority) over its supporting assets

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

For example, an organization may select Plant Control and Monitoring systems as the function to evaluate. The organization might describe the function's criteria as follows:

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

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

- its supporting assets
  - *IT equipment that directly supports the function.*
  - *OT equipment that directly supports the function.*
  - *Information assets that directly support the function.*
  - *Finance and HQ receive reports directly from the system.*
  - *There are 3 stations that are staffed 24/7 with 4 people per shift for 4 shifts.*
  - *We have 2 vendors that can provide administrative support to the IT or OT systems via VPN.*
  - *The maintenance/engineering team has end-point connection access to the equipment but not the control room.*
  - *The ICS system is redundant and can be swapped in by the control room.*
  - *There is a backup site about 100 miles away, which is connected through VPN and backs up the software and data on the network daily. ICS data files are backed up during maintenance periods every 6 months.*

- whether the organization has identifiable ownership (i.e., authority) over its supporting assets
  - *It is mixed between the IT department (IT equipment/network) and the Plant (ICS and other OT equipment).*

Clearly identifying and defining the function makes providing definitive answers to the practices much easier. For example, the first practice in the Asset, Change, and Configuration Management (ASSET) domain is, "There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc." With a clearly defined function, the organization should be able to say, *We have a strong understanding of the hardware and software that are not just a part of the Plant Control and Monitoring system but are also important to the system.*

## 3.4 Assets

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

# 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 MIL.

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

## 4.1 Domains

Each of the model's 10 domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature cybersecurity risk management capability.

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

The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Risk Management domain comprises three objectives:

1. Manage Cybersecurity Risk
2. Establish Cybersecurity Risk Management Strategy
3. Management Practices

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 1 summarizes the elements of each domain.

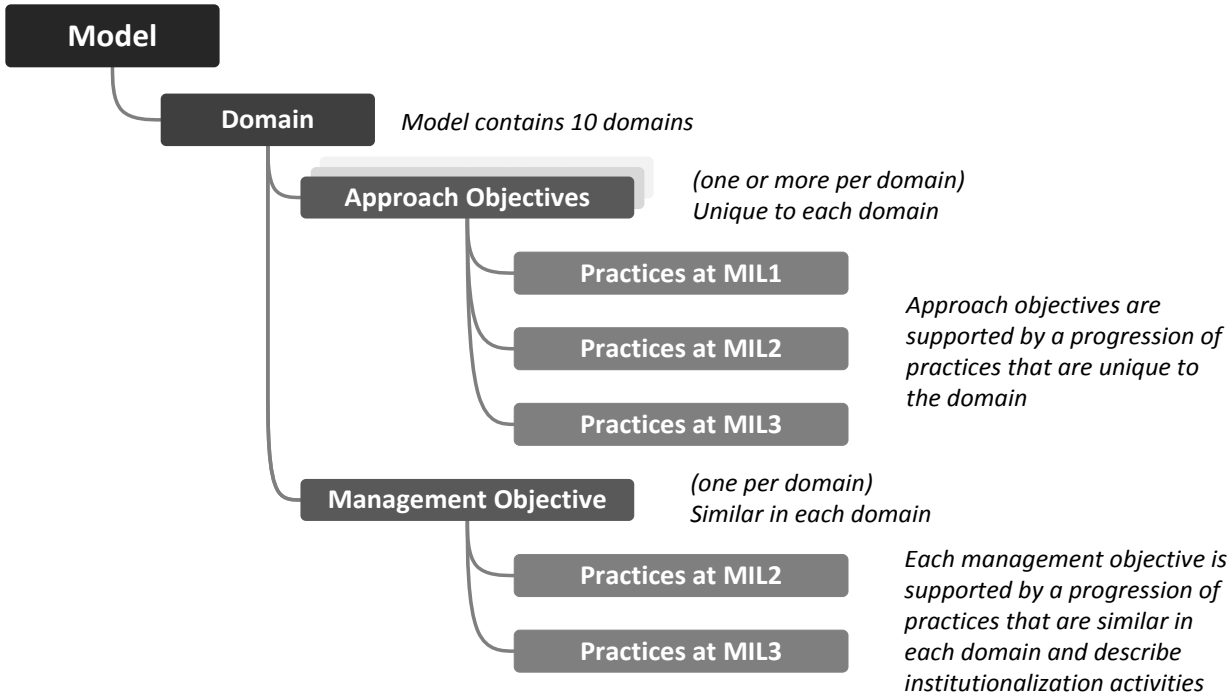


**Figure 1: Model and Domain Elements**

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 to reference that domain.

### Risk Management (RISK)

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

### 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.

### 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.

**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 (e.g., critical, IT, operational) and organizational objectives.

**Situational Awareness (SITUATION)**

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.

**Event and Incident Response (RESPONSE)**

Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents, commensurate with the risk to critical infrastructure and organizational objectives.

**Supply Chain and External Dependencies Management (DEPENDENCIES)**

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

**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 controls, processes, 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 the organization's strategic objectives and the risk to critical infrastructure.

## 4.2 Maturity Indicator Levels

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

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

- The maturity indicator levels apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings in different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
- The MILs are cumulative within each domain. To earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level(s). For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
- Establishing a target MIL for each domain is an effective strategy for using the model to guide cybersecurity program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Gap analysis activities and improvement efforts should then focus 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 against potential benefits. However, the model was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

### 4.2.1 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 this model, *ad hoc* (i.e., formed or used for a special purpose without policy or a plan for repetition) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much organizational guidance, such as a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice, when it is performed, the context of the problem being addressed, the methods, tools, and techniques used, and the priority given a particular instance of the practice. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, 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.

Table 1 provides an example of the approach progression in the Cybersecurity Program Management domain. At MIL1, a cybersecurity program strategy exists in any form. MIL2 adds more requirements to the strategy, including the need for defined objectives and alignment with the overall organization's strategy. Finally, in addition to requiring performance of all MIL1 and MIL2 practices, MIL3 warrants that the strategy be updated to reflect business changes, changes in the operating environment, and changes to the threat profile (developed in the Threat and Vulnerability Management domain).

**Table 2: Example of Approach Progression in the Cybersecurity Program Management Domain**

| | |
|---|---|
| MIL1 | a. The organization has a cybersecurity program strategy, which may be developed and/or managed in an ad hoc manner |
| MIL2 | a. The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities<br>b. The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure<br>c. The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities<br>d. The cybersecurity program strategy defines the structure and organization of the cybersecurity program<br>e. The cybersecurity program strategy identifies standards and/or guidelines intended to be followed by the program<br>f. The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program |
| MIL3 | g. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (THREAT-1d) |

### 4.2.2 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. A description of the management practices of each MIL can be found in the list below.

**Maturity Indicator Level 0 (MIL0)**

The model contains no practices for MIL0. Performance at MIL0 simply means that MIL1 in a given domain has not been achieved.

**Maturity Indicator Level 1 (MIL1)**

The model contains no management practices at MIL1.

**Maturity Indicator Level 2 (MIL2)**

Four management practices are present at MIL2, which represent an initial level of institutionalization of the activities within a domain.

1. **Practices are documented**. The practices in the domain are being performed according to a documented plan. The focus here should be on planning to ensure that the practices are intentionally designed (or selected) to serve the organization.
2. **Adequate resources are provided** to support the process (people, funding, and tools). Adequate resources are provided in the form of people, funding, and tools to ensure that the practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources. If all desired practices have been implemented as intended by the organization, then adequate resources have been provided.
3. **Personnel performing the practices have adequate skills and knowledge**. The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.
4. **Responsibility and authority for performing the practices are assigned to personnel**.

Overall, the practices at MIL2 are more complete than at MIL1 and are no longer performed irregularly or are not ad hoc in their implementation. As a result, the organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time.

**Maturity Indicator Level 3 (MIL3)**

At MIL3, the activities in a domain have been further institutionalized and are now being managed. Three management practices support this progression.

1. **Activities are guided by policies (or other organizational directives)**. Managed activities in a domain receive guidance or requirements from the organization in some form, typically in policies. Policies are an extension of the planning activities that are in place at MIL2.
2. **Performance objectives for domain activities are established and monitored to track achievement**.
3. **Documented practices for domain activities are standardized and improved across the enterprise.**

At MIL3, the practices in a domain are further stabilized and are guided by high-level organizational directives, such as policies. As a result, the organization should have additional confidence in its ability to sustain the performance of the practices over time and across the organization.

### 4.2.3 Summary of MIL Characteristics

Table 3 summarizes the characteristics of each MIL. At MIL2 and MIL3, the characteristic associated with the approach progression is distinguished from the characteristics associated with the management progression.

**Table 3: Summary of Maturity Indicator Level Characteristics**

| Level | Characteristics |
|---|---|
| **MIL0** | • Practices are not performed |
| **MIL1** | • Initial practices are performed but may be ad hoc |
| **MIL2** | *Management characteristics:*<br>• Practices are documented<br>• Adequate resources are provided to support the process<br>• Personnel performing the practices have adequate skills and knowledge<br>• Responsibility and authority for performing the practices are assigned<br>*Approach characteristic:*<br>• Practices are more complete or advanced than at MIL1 |
| **MIL3** | *Management characteristics:*<br>• Activities are guided by policies (or other organizational directives)<br>• Performance objectives for domain activities are established and monitored to track achievement<br>• Documented practices for domain activities are standardized and improved across the enterprise<br>*Approach characteristic:*<br>• Practices are more complete or advanced than at MIL2 |

## 4.3 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 abbreviation, a hyphen, the objective number, and the practice letter. Figure 2 shows an example from the second objective in the Risk Management domain. The objective's first practice, "There is a documented cybersecurity risk management strategy," would be referenced elsewhere in the model using the notation "RISK-2a."

### Example: RISK-2a

**Domain Abbreviation-Objective Number Practice Letter**

| 2. Establish Cybersecurity Risk Management Strategy | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. There is a documented cybersecurity risk management strategy<br>b. Organizational risk criteria (criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, risk tolerance, and risk response capabilities) are defined and available |
| **MIL3** | c. The risk management strategy defines risk response options for the organization<br>d. The risk management strategy is periodically updated to reflect the current threat environment<br>e. An organization-specific risk taxonomy (a catalogued collection of common risks that the organization is subject to and must manage) is documented and is used in risk management activities |

**Figure 2: Referencing an Individual Practice, Example: RISK-2a**

# 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 3 summarizes the recommended approach for using the model. An organization performs an evaluation against the model, uses that evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. The following sections discuss the preparation activities required to begin using the model and provide additional details on the activities in each step of this approach.

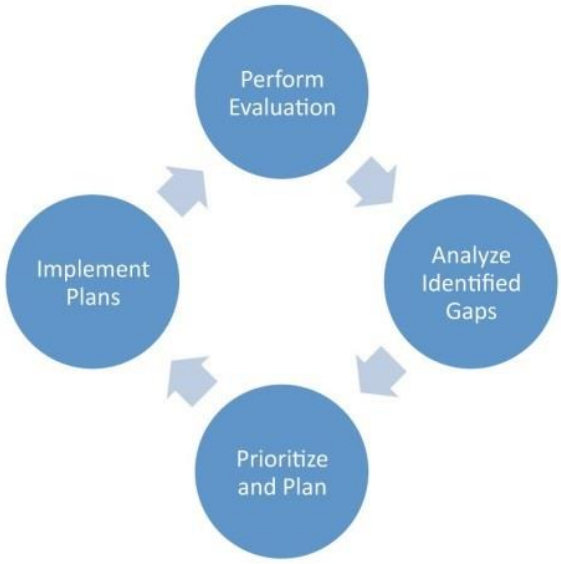


**Figure 3: Recommended Approach for Using the Model**

## 5.1 Prepare to Use the Model

A design goal of the model was to enable organizations to complete a self-evaluation for a single function in less than one day without extensive study or preparation. This goal is achieved in part because the model is supported by an evaluation survey and scoring mechanism and the evaluation survey itself is performed in a workshop setting, led by a facilitator who is familiar with the model content. An important component of successfully completing the self-evaluation in one day is the selection of an effective facilitator. Generally speaking, a C2M2 facilitator is someone who is not only familiar with the model and its supporting artifacts but also who is effective at helping a group of people understand their common objectives and assisting them in planning to achieve these objectives without taking a particular position in the discussion.

In addition to helping to execute the self-evaluation and interpret the results, the facilitator helps the organization establish a scope for the model application. Though the C2M2 and its supporting survey apply to an entire organization, the self-evaluation survey is typically applied to a single function to maintain focus. Recall that the term *function* refers to the subset of the operations of the organization that is being evaluated. The facilitator must work with the organization to determine the survey *scope*—the part of the organization's operations to which the model and survey will be applied and the groups supporting IT and OT activities. When defining scope, clarify the extent to which the scope includes both cyber and physical security (e.g., physical access to cyber infrastructure). Selecting and documenting the scope before completing the survey ensures that users of the survey results understand to which part of the organization the results apply.

More thorough guidance on using the model, selecting a facilitator, and scoping the evaluation can be found in the supporting *C2M2 Facilitator Guide*.[9]

## 5.2 Prioritize and Scope

| Inputs | Activities | Outputs |
|---|---|---|
| 1. Risk management strategy<br>2. Organizational objectives and priorities<br>3. Threat information<br>4. *C2M2* | 1. Organization determines the scope of operations that will use the *C2M2* to evaluate and potentially improve the organization's cybersecurity capabilities | 1. *Function list* |

Organizations begin a C2M2 self-evaluation by determining the function—the subset of the operations of the organization that will be evaluated. (Section 2.6 of the *C2M2 Facilitator Guide* provides guidance for scoping.) However, the C2M2 is flexible enough to be used for whatever scope an organization chooses for implementation, including systems or technology areas that cross organizational boundaries. There may even be some cases where the C2M2 function encompasses the entire organization, as is sometimes the case in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [NIST CSF].

[9] The *C2M2 Facilitator Guide* may be downloaded from http://energy.gov/node/795826.

## 5.3 Orient

| Inputs | Activities | Outputs |
|---|---|---|
| 1. *Function list*<br>2. Risk management strategy | 1. *Based on selected functions*, the organization identifies the in-scope:<br>– assets (e.g., people, information, technology, and facilities)<br>– regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines) | 1. In-scope systems and assets<br>2. In-scope requirements (i.e., regulatory, company, organizational)<br>3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines<br>4. Evaluation approach: *C2M2 self-evaluation* |

Once a function is determined, the organization identifies the information, technology, people, and facilities covered by the function, the applicable regulatory requirements, and any cybersecurity and risk management standards, tools, methods, and guidelines in use.

## 5.4 Create a Current Profile

| Inputs | Activities | Outputs |
|---|---|---|
| 1. *C2M2 self-evaluation*<br>2. In-scope systems and assets<br>3. In-scope regulatory requirements<br>4. In-scope cybersecurity and risk management standards, tools, methods, and guidelines | 1. *Conduct C2M2 self-evaluation workshop with appropriate attendees* | 1. *C2M2 Evaluation Scoring Report*<br>2. Current Implementation Tier |

The C2M2 is typically applied through a facilitated, one-day workshop that includes key individuals representing all in-scope assets and functions. Through open dialog and consensus, survey workshop participants answer questions in the evaluation survey about practices in each domain. Responses are chosen from a four-point scale: Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented. Using the toolkit, the C2M2 Evaluation Scoring Report is generated from the survey results. The Scoring Report can serve as a Current Profile. The report presents results in two views: the Objective view, which shows practice question responses by each domain and its objectives, and the Domain view, which shows responses by all domains and MILs. Figure 4 gives an example of results for the Risk Management domain in the Objective view, and Figure 5 gives an example of results in the

Domain view. [Note: Figures 4 and 5 will be updated after all model changes are finalized and a report can be generated from the new toolkit.]

Red sectors in a doughnut chart show a count of the number of questions that received survey responses of “Not Implemented” (dark red) or “Partially Implemented” (light red). The green sectors show the number of questions that received responses of “Largely Implemented” (light green) or “Fully Implemented” (dark green).

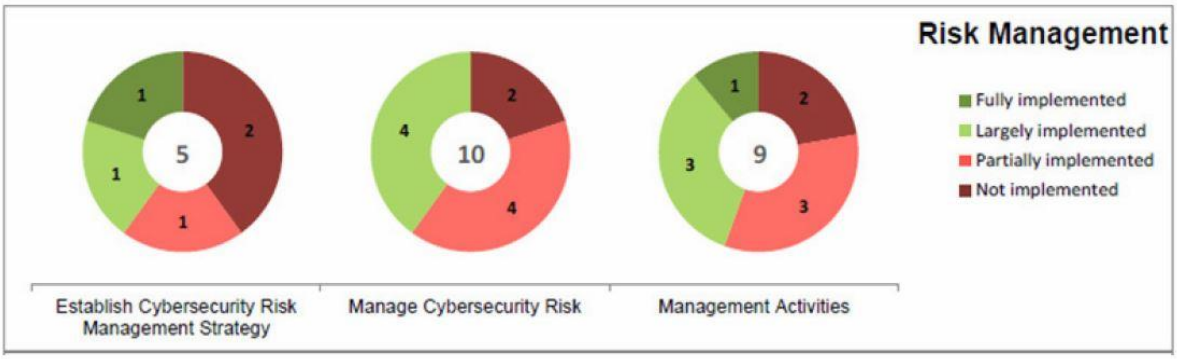


**Figure 4: Objective View Example**

In the Objective view, the number in the center of the doughnut indicates the number of questions for the objective named below the doughnut chart.

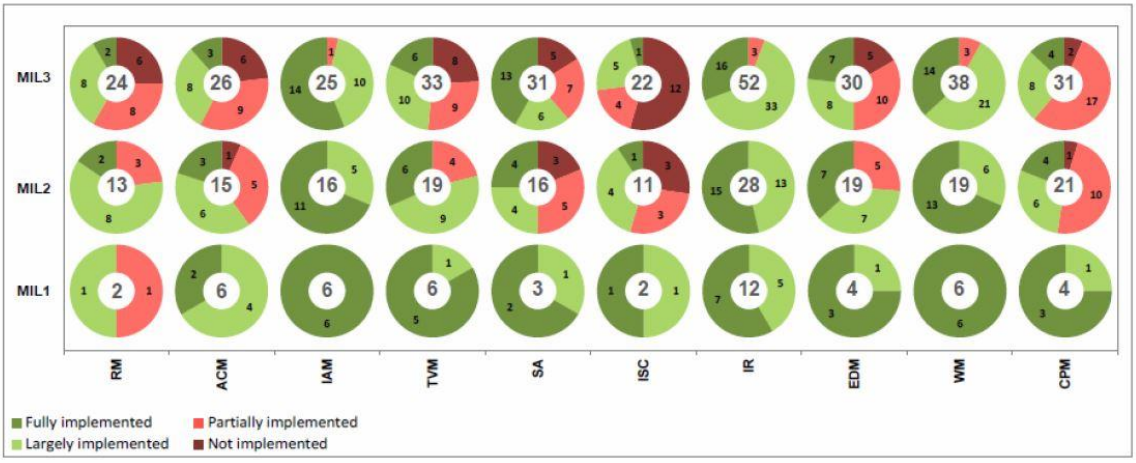


**Figure 5: Domain View Example**

In the Domain view, the number in the center of the doughnut indicates the cumulative number of questions that must be answered “Largely Implemented” or “Fully Implemented” to achieve that MIL for that domain.

A current NIST CSF Implementation Tier is not a direct output of a C2M2 workshop, but it can be arrived at with some further analysis. Information about how this can be done is shown in Table 12 of Appendix A of the *Energy Sector Cybersecurity Framework Implementation Guidance* [DOE Framework Implementation].

## 5.5 Conduct a Risk Assessment

| Inputs | Activities | Outputs |
|---|---|---|
| 1. *Function list*<br>2. Risk management strategy<br>3. Organization-defined risk assessment approach<br>4. In-scope regulatory requirements<br>5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines<br>6. *C2M2 Evaluation Scoring Report* | 1. Perform risk assessment *for each function in the function list* | 1. Risk assessment reports *for each of the functions* |

Ideally, organizations will use C2M2 as part of a continuous enterprise risk management process that includes risk assessments. Results of the risk assessment are used as input in all of the rest of the C2M2 implementation steps. Organizations can look to the NIST CSF [NIST CSF] and the *Electricity Subsector Cybersecurity Risk Management Process Guideline* [DOE RMP] for additional guidance for this activity [DOE 2012b].

## 5.6 Create a Target Profile

| Inputs | Activities | Outputs |
|---|---|---|
| 1. *C2M2 Evaluation Scoring Report*<br>2. Current Tier<br>3. Organizational objectives<br>4. Risk management strategy<br>5. Risk assessment reports | 1. Organization identifies *MIL and practice-specific* goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives | 1. *C2M2* Target Profile<br>2. Target Tier |

The C2M2 Evaluation Scoring Report highlights potential areas for improvement. For example, within any domain, practices that represent achievement of MIL1 are prerequisites to practices that allow achievement of MIL2. All practices must be present to achieve the next MIL. The

Evaluation Scoring Report may give some initial insights for the Target Profile by drawing attention to the absence of qualifying practices at the lower MILs. The report also includes a "Summary of Identified Gaps" table, which lists the survey questions that were answered either "Partially Implemented" or "Not Implemented," and is useful in setting a Target Profile.

The risk assessment can be used along with the Evaluation Scoring Report to identify target practices and MILs. Some practices may appear to be necessary based on the Domain view to reach the next MIL but may not make sense for the organization based on its risk profile. Each organization determines the target MIL and practices that make sense for each domain.

## 5.7 Determine, Analyze, and Prioritize Gaps

| Inputs | Activities | Outputs |
|---|---|---|
| 1. *C2M2 Evaluation Scoring Report*<br>2. Current Tier<br>3. *C2M2* Target Profile<br>4. Target Tier<br>5. Organizational objectives<br>6. Impact to critical infrastructure<br>7. Gaps and potential consequences<br>8. Organizational constraints<br>9. Risk management strategy<br>10. Risk assessment reports | 1. Analyze gaps between current state and Target Profile in organization's context<br>2. Evaluate potential consequences from gaps<br>3. Determine which gaps need attention<br>4. Identify actions to address gaps<br>5. Perform cost-benefit analysis (CBA) on actions<br>6. Prioritize actions (CBA and consequences)<br>7. Plan to implement prioritized actions | 1. Prioritized gaps and potential consequences<br>2. Prioritized implementation plan |

The C2M2 Self-Evaluation Scoring Report enables organizations to identify gaps between the Current Profile and the Target Profile. Section 4.3.2 of the *C2M2 Facilitator Guide* [DOE 2017] provides guidance on how to plan and prioritize the actions needed to address gaps and achieve the Target Profile. Prioritization should consider how gaps affect organizational objectives and the relative criticality of those objectives, the cost of implementing the target practices, and the availability of resources to implement the practices.

The organization should identify risks that could arise as a result of gaps that are not addressed and decide whether those gaps can be mitigated in other ways. The organization may choose to accept and manage such risks over time. The priority of unresolved gaps can also be reconsidered if C2M2 self-evaluations are conducted periodically.

## 5.8 Implement Action Plan

| Inputs | Activities | Outputs |
|---|---|---|
| 1. Prioritized implementation plan | 1. Implement actions by priority<br>2. Track progress against plan<br>3. Re-evaluate periodically or in response to major change | 1. Project tracking data |

The organization executes the implementation plan and tracks its progress over time, ensuring that gaps are closed and risks are monitored.

Figure 6 presents a detailed outline of the C2M2 process as described in this chapter.

**Figure 6: C2M2 Inputs, Outputs, and Activities**

| | Prioritize and Scope | Orient | Create a Current Profile | Conduct a Risk Assessment | Create a Target Profile | Determine, Analyze, and Prioritize Gaps | Implement Action Plan |
|---|---|---|---|---|---|---|---|
| INPUTS | 1. Risk management strategy<br>2. Organizational objectives and priorities<br>3. Threat information<br>4. C2M2 | 1. **Function list**<br>2. Risk management strategy | 1. **C2M2 self-evaluation**<br>2. In-scope systems and assets<br>3. In-scope regulatory requirements<br>4. In-scope cybersecurity and risk management standards, tools, methods, and guideline | 1. **Function list**<br>2. Risk management strategy<br>3. Organization-defined risk assessment approach<br>4. In-scope regulatory requirements<br>5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines<br>6. **C2M2 Evaluation Scoring Report** | 1. **C2M2 Evaluation Scoring Report**<br>2. Current Tier<br>3. Organizational objectives<br>4. Risk management strategy<br>5. Risk assessment reports | 1. **C2M2 Evaluation Scoring Report**<br>2. Current Tier<br>3. **C2M2** Target Profile<br>4. Target Tier<br>5. Organizational objectives<br>6. Impact to critical infrastructure<br>7. Gaps and potential consequences<br>8. Organizational constraints<br>9. Risk management strategy<br>10. Risk assessment reports | 1. Prioritized implementation plan |
| ACTIVITIES | 1. Organization determines the scope of operations that will use the **C2M2** to evaluate and potentially improve the organization's cybersecurity capabilities | **Based on selected functions**, the organization identifies the in-scope:<br>- assets (e.g., people, information, technology, and facilities)<br>- regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines) | 1. Conduct **C2M2 self-evaluation** workshop with appropriate attendees | 1. Perform risk assessment **for each function in the function list** | 1. Organization identifies **MIL and practice-specific** goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives | 1. Analyze gaps between current state and Target Profile in organization's context<br>2. Evaluate potential consequences from gaps<br>3. Determine which gaps need attention<br>4. Identify actions to address gaps<br>5. Perform cost-benefit analysis (CBA) on actions<br>6. Prioritize actions (CBA and consequences)<br>7. Plan to implement prioritized actions | 1. Implement actions by priority<br>2. Track progress against plan<br>3. Re-evaluate periodically or in response to major change |
| OUTPUTS | 1. **Function list** | 1. In-scope systems and assets<br>2. In-scope requirements (i.e., regulatory, company, organizational)<br>3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines<br>4. Evaluation approach: **C2M2 self-evaluation** | 1. **C2M2 Evaluation Scoring Report**<br>2. Current Implementation Tier | 1. Risk assessment reports **for each of the functions** | 1. **C2M2 Target Profile**<br>2. Target Tier | 1. Prioritized gaps and potential consequences<br>2. Prioritized implementation plan | 1. Project tracking data |

# 6. MODEL DOMAINS

## 6.1 Risk Management (RISK)

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

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

The Risk Management (RISK) domain comprises three objectives:

1. Manage Cybersecurity Risk
2. Establish Cybersecurity Risk Management Strategy
1. Management Activities

Managing cybersecurity 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 cybersecurity risk management strategy discussed above. With defined risk criteria, organizations can consistently respond to and monitor identified risks. A risk register—a list of identified risks and associated attributes—facilitates this process. Other domains in this model (Situational Awareness and Event and Incident Response; ) refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cybersecurity risk management program.

A cybersecurity risk management strategy is a high-level strategy that provides direction for analyzing and prioritizing cybersecurity risk and defines risk tolerance. The cybersecurity risk

**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 cybersecurity 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.

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.

management strategy includes a risk assessment methodology, risk monitoring strategy, and cybersecurity governance program. This includes defining the enterprise risk criteria (e.g., impact thresholds, risk response approaches) that guide the cybersecurity program discussed in the Cybersecurity Program Management domain later in this model. The cybersecurity risk management strategy should align with the enterprise risk management strategy to ensure that cybersecurity risk is managed in a manner that is consistent with the organization's mission and business objectives.

**Objectives and Practices**

### 1. Manage Cybersecurity Risk

| | |
|---|---|
| **MIL1** | a. Cybersecurity risks are identified and documented, at least in an ad hoc manner<br>b. Risks are mitigated, accepted, avoided, or transferred (i.e., risk responses are implemented), at least in an ad hoc manner |
| **MIL2** | c. Risk assessments are performed to identify risks according to organization-defined triggers (e.g., time elapsed, changes to infrastructure, changes to threat environment)<br>d. Risks are recorded in a risk register (a structured repository of identified risks)<br>e. Risks are analyzed to select and prioritize risk responses using defined risk criteria (RISK-2b)<br>f. Risks are tracked to ensure that risk responses are implemented and meet organizational objectives (PROGRAM-1b) |
| **MIL3** | g. Risk assessments include all assets and activities that are critical to the achievement of the organization's mission<br>h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy<br>i. A current cybersecurity architecture is used to inform risk analysis (ARCHITECTURE-1c)<br>j. The risk register includes all risks identified through cybersecurity risk assessments and is used to support risk management activities |

### 2. Establish Cybersecurity Risk Management Strategy

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. There is a documented cybersecurity risk management strategy<br>b. Organizational risk criteria (criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, risk tolerance, and risk response capabilities) are defined and available |
| **MIL3** | c. The risk management strategy defines risk response options for the organization<br>d. The risk management strategy is periodically updated to reflect the current threat environment<br>e. An organization-specific risk taxonomy (a catalogued collection of common risks that the organization is subject to and must manage) is documented and is used in risk management activities |

### 3. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the RISK domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain<br>c. Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the RISK domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the RISK domain<br>f. Performance objectives for activities in the RISK domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the RISK domain are standardized and improved across the enterprise |

## 6.2 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 this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.

The Asset, Change, and Configuration Management (ASSET) domain comprises four objectives:

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage Asset Configuration
4. Manage Changes to Assets
5. Management Activities

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

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

Managing changes to assets includes analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes. Change control

**Example: Asset Change and Configuration Management**

Anywhere Inc. has an asset database. Within that database, technology assets are identified and prioritized based on importance to the generation function. The database includes attributes that support cybersecurity operations, such as hardware and software versions, physical location, security requirements (business needs for the asset's confidentiality, integrity, and availability), asset owner, and version of applied configuration baseline.

Anywhere Inc. uses this information for cybersecurity 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.

applies to the entire asset lifecycle, including requirements definition, testing, deployment and maintenance, and retirement from operation.

**Objectives and Practices**

### 1. Manage IT and OT Asset Inventory

| | |
|---|---|
| **MIL1** | a. There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc |
| **MIL2** | b. Inventory attributes include information to support the cybersecurity program strategy (PROGRAM-1a) (e.g., locations, asset owners, applicable cybersecurity requirements, service dependencies, service level agreements, end of life dates, end of support dates, and conformance of assets to relevant industry standards)<br>c. Inventoried assets for the delivery of the function are prioritized based on formally defined criteria |
| **MIL3** | d. All IT and OT assets for the delivery of the function are inventoried<br>e. The asset inventory is current (as defined by the organization)<br>f. The asset inventory is used to identify cybersecurity risks (e.g., asset end of life or end of support, single points of failure) |

### 2. Manage Information Asset Inventory

| | |
|---|---|
| **MIL1** | a. There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data, log data); management of the inventory may be ad hoc |
| **MIL2** | b. Inventory attributes include information to support the cybersecurity program strategy (PROGRAM-1a) (e.g., storage locations, backup locations and frequencies, asset owners, applicable cybersecurity requirements, service dependencies, service level agreements)<br>c. Inventoried information assets are categorized based on a defined scheme |
| **MIL3** | d. There is an inventory for all information assets related to the delivery of the function<br>e. The asset inventory is current (as defined by the organization)<br>f. The asset inventory is used to identify cybersecurity risks (e.g., risk of disclosure, risk of destruction, risk of tampering) |

### 3. Manage Asset Configuration

| | |
|---|---|
| **MIL1** | a. Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly<br>b. Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment and restoration |
| **MIL2** | c. The design of configuration baselines includes cybersecurity objectives (PROGRAM-1b) |

### 3. Manage Asset Configuration (cont.)

| | |
|---|---|
| **MIL3** | d. Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles<br>e. Configuration baselines are reviewed and updated at an organization-defined frequency<br>f. Configuration baselines incorporate requirements from the applicable security zone (ARCHITECTURE-2b) (e.g., network appliance configurations are tailored to the traffic restrictions for the zone) |

### 4. Manage Changes to Assets

| | |
|---|---|
| **MIL1** | a. Changes to inventoried assets are evaluated before being implemented, at least in an ad hoc manner<br>b. Changes to inventoried assets are logged, at least in an ad hoc manner |
| **MIL2** | c. Changes to assets are tested prior to being deployed, whenever possible<br>d. Change management practices address the full lifecycle of assets (e.g., acquisition, deployment, operation, retirement) |
| **MIL3** | e. Changes to assets are tested for cybersecurity impact prior to being deployed<br>f. Change logs include information about modifications that impact the cybersecurity requirements of assets (confidentiality, integrity, availability) |

### 5. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the ASSET domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain<br>c. Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the ASSET domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the ASSET domain<br>f. Performance objectives for activities in the ASSET domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the ASSET domain are standardized and improved across the enterprise |

## 6.3 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 cyber assets relevant to the function, and automated access control systems (logical or physical) relevant to the function. Improper access management practices can lead to unauthorized use, disclosure, destruction, or modification, as well as unnecessary exposure to cybersecurity risks.

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

1. Establish and Maintain Identities
2. Control Access
3. Management Activities

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

**Example: Identity and Access Management**

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

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

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

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

Controlling access includes determining access requirements, granting access to assets based on those requirements, and revoking access when it is no longer required. Access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters. For example, the 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.

Access is granted only after considering risk to the function, and regular reviews of access are conducted.

**Objectives and Practices**

### 1. Establish and Maintain Identities

| | |
|---|---|
| MIL1 | a. Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) that require access to assets (note that this does not preclude shared identities)<br>b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys, lock combinations), at least in an ad hoc manner<br>c. Identities are deprovisioned, at least in an ad hoc manner, when no longer required |
| MIL2 | d. Identity repositories are reviewed and updated to ensure accuracy, at an organization-defined frequency<br>e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity<br>f. Identities are deprovisioned within organization-defined time thresholds when no longer required |
| MIL3 | g. Requirements for credentials are based on the organization's risk criteria (RISK-2b) (e.g., multifactor credentials for higher risk access) and cybersecurity architecture (e.g., credential requirements for accessing security zones (ARCHITECTURE-2b)) |

### 2. Control Access

| | |
|---|---|
| MIL1 | a. Access requirements (e.g., rules for which types of entities are allowed to access an asset, the limits of allowed access, constraints on remote access, and authentication parameters) are determined, at least in an ad hoc manner<br>b. Access is granted to identities based on the access requirements, at least in an ad hoc manner<br>c. Access is revoked when no longer required, at least in an ad hoc manner |
| MIL2 | d. Access requirements incorporate least privilege and separation of duties principles<br>e. Access requests are reviewed and approved by the asset owner<br>f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring |
| MIL3 | g. Access privileges are reviewed and updated to ensure conformance with access requirements, at an organization-defined frequency<br>h. Anomalous access attempts are monitored as indicators of cybersecurity events |

### 3. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the ACCESS domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain<br>c. Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the ACCESS domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the ACCESS domain<br>f. Performance objectives for activities in the ACCESS domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the ACCESS domain are standardized and improved across the enterprise |

# 6.4 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 (e.g., critical, IT, operational) and organizational objectives.*

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

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

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

1. Identify and Respond to Threats
2. Reduce Cybersecurity Vulnerabilities
3. Management Activities

**Example: Threat and Vulnerability Management**

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

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

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

Reducing cybersecurity vulnerabilities begins with collecting and analyzing vulnerability information. Vulnerability discovery may be performed using automatic scanning tools, network penetration tests, cybersecurity exercises, and audits. Vulnerability analysis should consider the vulnerability's local impact (the potential effect of the vulnerability on the exposed asset) as well as the importance of the exposed asset to the delivery of the function. Vulnerabilities may

be addressed by implementing mitigating controls, monitoring threat status, applying cybersecurity patches, or through other activities.

**Objectives and Practices**

### 1. Identify and Respond to Threats

| | |
|---|---|
| **MIL1** | a. Internal and external information sources to support threat management activities (e.g., NCCIC, appropriate ISACs, industry associations, vendors, federal briefings) are identified, at least in an ad hoc manner<br>b. Cybersecurity threat information is gathered and interpreted for the function, at least in an ad hoc manner<br>c. Threats that are relevant to the delivery of the function are addressed (e.g., implement mitigating controls, monitor threat status), at least in an ad hoc manner |
| **MIL2** | d. A threat profile for the function is established (e.g., characterization of potential threat actors, motives, intent, capabilities, and targets)<br>e. Threat information sources that collectively address all components of the threat profile are prioritized and monitored<br>f. Identified threats are analyzed and prioritized and are addressed accordingly<br>g. Cybersecurity threat information is provided to selected individuals and/or organizations |
| **MIL3** | h. The threat profile for the function is updated at an organization-defined frequency<br>i. Threats that pose ongoing risk to the function are referred to the risk management process for action (RISK-1e)<br>j. Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3h)<br>k. Threat information-sharing stakeholders are identified and engaged based on their relevance to the continued operation of the function (e.g., government, connected organizations, vendors, sector organizations, regulators, information sharing and analysis centers (ISACs), internal entities)<br>l. Secure, automated workflows are used to publish, consume, analyze, and act upon cyber threat information |

### 2. Reduce Cybersecurity Vulnerabilities

| | |
|---|---|
| **MIL1** | a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., NCCIC, appropriate ISACs, industry associations, vendors, federal briefings, internal assessments), at least in an ad hoc manner<br>b. Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner<br>c. Cybersecurity vulnerability assessments (e.g., end-of-life and end-of-support asset review, software-based scans, penetration tests) are performed, at least in an ad hoc manner<br>d. Cybersecurity vulnerabilities that are relevant to the delivery of the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches), at least in an ad hoc manner |

## 2. Reduce Cybersecurity Vulnerabilities (cont.)

| | |
|---|---|
| **MIL2** | e. Cybersecurity vulnerability information sources that collectively address all assets important to the function are monitored<br>f. Cybersecurity vulnerability assessments are performed at an organization-defined frequency<br>g. Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., the NIST Common Vulnerability Scoring System could be used for software vulnerabilities; internal guidelines could be used to prioritize other types of vulnerabilities) and are addressed accordingly<br>h. Operational impact to the function is evaluated prior to deploying patches<br>i. Information on any discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders |
| **MIL3** | j. Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function at an organization-defined frequency<br>k. Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function<br>l. Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management process for response (RISK-1e)<br>m. Ongoing risk monitoring includes review and confirmation of actions taken in response to cybersecurity vulnerabilities (e.g., deployment of patches or other activities) where appropriate |

## 3. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the THREAT domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain<br>c. Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the THREAT domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the THREAT domain<br>f. Performance objectives for activities in the THREAT domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the THREAT domain are standardized and improved across the enterprise |

## 6.5 Situational Awareness (SITUATION)

*Purpose: Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.*

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

The Situational Awareness (SITUATION) domain comprises four objectives:

1. Perform Logging
2. Perform Monitoring
3. Establish and Maintain Situational Awareness
4. Management Activities

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

Monitoring and analyzing data collected in logs and through other means enables the organization to understand the function's operational and cybersecurity status. Effectively communicating the operational and cybersecurity status to relevant decision makers is the essence of situational awareness (sometimes referred to as a *common operating picture*). While many situational awareness implementations

**Example: Situational Awareness**

Anywhere Inc. identified the assets that are essential to the delivery of the organization's functions. 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 include summarizing the current state of operations using a color-coded scale and posting it 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 helpdesk conducts malware scans on misbehaving laptops, and human resources sends out reminders about phishing. Senior management can review the situational awareness information and be prepared should extraordinary action—like shutting down the website—be required. At the highest state of alert, they change firewall rule sets to restrict nonessential protocols like video conferencing, delay all but emergency change requests, and put the cybersecurity incident response team on standby.

may include visualization tools (e.g., 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 important to the function wherever feasible, at least in an ad hoc manner |
| **MIL2** | b. Logging requirements are established and maintained for assets important to the function<br>c. Log data are being aggregated within the function |
| **MIL3** | d. Logging requirements are based on risk to the function (i.e., more rigorous logging for higher risk assets) |

### 2. Perform Monitoring

| | |
|---|---|
| **MIL1** | a. Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner<br>b. Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event, at least in an ad hoc manner |
| **MIL2** | c. Monitoring and analysis requirements are established and maintained for the function and address timely review of event data<br>d. Indicators of anomalous activity are established and maintained based on system logs, data flows, cybersecurity events, and system architecture and are monitored across the operational environment<br>e. Alarms and alerts are configured to support the identification of cybersecurity events (RESPONSE-1b)<br>f. Monitoring activities are aligned with the defined threat profile (THREAT-1d) |
| **MIL3** | g. Monitoring requirements are based on the risk to the function (i.e., more rigorous monitoring for higher risk assets)<br>h. Automated monitoring is performed across the operational environment to identify anomalous activity<br>i. Risk register (RISK-1d) content is used to identify indicators of anomalous activity<br>j. Indicators of anomalous activity are evaluated and updated at an organization-defined frequency |

### 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<br>b. Monitoring data are aggregated to provide an understanding of the operational state of the function<br>c. Relevant information from across the organization is available to enhance situational awareness |

### 3. Establish and Maintain Situational Awareness (cont.)

| | |
|---|---|
| **MIL3** | d. Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders (e.g., government, connected organizations, vendors, sector organizations, regulators, internal entities)<br>e. Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state of the function<br>f. Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness (THREAT-1g, THREAT-2i)<br>g. Procedures are in place to analyze and deconflict received cybersecurity information in support of situational awareness<br>h. Predefined states of operation are documented and invoked (through manual or automated processes) based on the analysis of aggregated data (THREAT-1k, RESPONSE-3k) |

### 4. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the SITUATION domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain<br>c. Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the SITUATION domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the SITUATION domain<br>f. Performance objectives for activities in the SITUATION domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the SITUATION domain are standardized and improved across the enterprise |

## 6.6 Event and Incident Response (RESPONSE)

*Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and 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 and/or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts.

The Event and Incident Response domain comprises four objectives:

1. Detect Cybersecurity Events
2. Analyze Cybersecurity Events and Declare Incidents
3. Respond to Cybersecurity Events and Incidents
4. Management Activities

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

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

Responding to cybersecurity incidents requires the organization to have a process to limit the impact of cybersecurity incidents to its functional and organizational units. The process should describe how the organization manages all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure). Conducting lessons-learned reviews as a

**Example: Event and Incident Response**

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.

part of cybersecurity event and incident response helps the organization eliminate the exploited vulnerability that led to the incident.

**Objectives and Practices**

### 1. Detect Cybersecurity Events

| | | |
|---|---|---|
| MIL1 | a. | Detected cybersecurity events are reported to a specified person or role and logged, at least in an ad hoc manner |
| MIL2 | b. | Criteria are established for cybersecurity event detection (e.g., what constitutes a cybersecurity event, where to look for cybersecurity events) |
| | c. | Cybersecurity events are centrally logged based on the established criteria |
| MIL3 | d. | Event information is correlated to support incident analysis by identifying patterns, trends, and other common features |
| | e. | Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RISK-1d) and threat profile (THREAT-1d) to help monitor for identified risks and detect known threats |
| | f. | Situational awareness for the function is monitored to support the identification of cybersecurity events (SITUATION-2i) |

### 2. Analyze Cybersecurity Events and Declare Incidents

| | | |
|---|---|---|
| MIL1 | a. | Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner |
| | b. | Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner |
| MIL2 | c. | Cybersecurity incident declaration criteria are formally established based on the potential impact to the function (RISK-1c) |
| | d. | Cybersecurity incident declaration criteria are updated at an organization defined frequency |
| | e. | Events are escalated based on established criteria |
| | f. | There is a repository where escalated cybersecurity events and incidents are logged and tracked to closure |
| | g. | Cybersecurity stakeholders (e.g., government, connected organizations, vendors, sector organizations, regulators, internal entities) are identified and notified of events and incidents based on organization-defined criteria (SITUATION-3d) |
| MIL3 | h. | Criteria for cybersecurity incident declaration are aligned with the organization's risk criteria (RISK-2b) |
| | i. | Cybersecurity incidents are correlated to support the discovery of patterns, trends, and other common features |

### 3. Respond to Cybersecurity Events and Incidents

| | | |
|---|---|---|
| MIL1 | a. | Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner |
| | b. | Responses to cybersecurity events and incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations |
| | c. | Cybersecurity events and incidents are reported to cybersecurity stakeholders, at least in an ad hoc manner |

### 3. Respond to Cybersecurity Events and Incidents (cont.)

| | |
|---|---|
| **MIL2** | d. Cybersecurity incident response plans that address all phases of the incident lifecycle (e.g., triage, escalation, handling, communication, coordination, and closure) are established and maintained<br>e. Cybersecurity event and incident response is executed according to defined plans and procedures<br>f. Cybersecurity event and incident response plan exercises are conducted at an organization-defined frequency |
| **MIL3** | g. Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed and corrective actions are taken, including updating incident response plans<br>h. Cybersecurity event and incident responses are coordinated with law enforcement and other external entities as appropriate, including support for evidence collection and preservation<br>i. Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., tabletops, simulated incidents)<br>j. Cybersecurity event and incident responses leverage and trigger predefined states of operation (SITUATION-3h) |

### 4. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the RESPONSE domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain<br>c. Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the RESPONSE domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the RESPONSE domain<br>f. Performance objectives for activities in the RESPONSE domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the RESPONSE domain are standardized and improved across the enterprise |

# 6.7 Supply Chain and External Dependencies Management (DEPENDENCIES)

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

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

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

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

The Supply Chain and External Dependencies Management (DEPENDENCIES) domain comprises three objectives:

1. Identify Dependencies
2. Manage Dependency Risk

**Example: Supply Chain and External Dependencies 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.

3. Management Activities

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

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

**Objectives and Practices**

### 1. Identify Dependencies

| | |
|---|---|
| **MIL1** | a. Important IT and OT supplier dependencies are identified (i.e., internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner<br>b. Important customer dependencies are identified (i.e., internal and external parties that are dependent on the delivery of the function, including operating partners), at least in an ad hoc manner |
| **MIL2** | c. Supplier dependencies are identified according to established criteria<br>d. Customer dependencies are identified according to established criteria<br>e. Single-source and other essential dependencies are identified<br>f. Dependencies are prioritized |
| **MIL3** | g. Dependency prioritization and identification are based on defined risk criteria (RISK-2b) |

### 2. Manage Dependency Risk

| | |
|---|---|
| **MIL1** | a. Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner<br>b. Cybersecurity requirements are considered when establishing relationships with suppliers and other third parties, at least in an ad hoc manner |
| **MIL2** | c. Identified cybersecurity dependency risks are entered into the risk register (RISK-1d)<br>d. Contracts and agreements with third parties incorporate sharing of cybersecurity threat information<br>e. Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate<br>f. Agreements with suppliers and other external entities include cybersecurity requirements<br>g. Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements<br>h. Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service<br>i. Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements |

## 2. Manage Dependency Risk (cont.)

| | |
|---|---|
| **MIL3** | j. Cybersecurity requirements are established for supplier dependencies based on defined risk criteria (RISK-2b)<br>k. Vendor selection criteria include consideration of end-of-life and end-of-support timelines<br>l. Vendor selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services<br>m. Information sources are monitored to identify and avoid supply chain risks (e.g., counterfeit or compromised software, hardware, and services)<br>n. Acceptance testing of procured assets includes testing for cybersecurity requirements |

## 3. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the DEPENDENCIES domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the DEPENDENCIES domain<br>c. Personnel performing activities in the DEPENDENCIES domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the DEPENDENCIES domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the DEPENDENCIES domain<br>f. Performance objectives for activities in the DEPENDENCIES domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the DEPENDENCIES domain are standardized and improved across the enterprise |

# 6.8 Workforce Management (WORKFORCE)

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

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

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

The Workforce Management (WORKFORCE) domain comprises five objectives:

1. Assign Cybersecurity Responsibilities
2. Develop Cybersecurity Workforce
3. Implement Workforce Controls
4. Increase Cybersecurity Awareness
5. Management Activities

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

Developing the cybersecurity workforce includes training and recruiting to address identified skill gaps. For example, hiring practices should ensure that recruiters and interviewers are aware of cybersecurity workforce needs. Also, personnel (and contractors) should receive

**Example: Workforce Management**

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

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

periodic security awareness training to reduce their vulnerability to social engineering and other threats. The effectiveness of training and awareness activities should be evaluated, and improvements should be made as needed.

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

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

**Objectives and Practices**

### 1. Assign Cybersecurity Responsibilities

| | |
|---|---|
| **MIL1** | a. Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner<br>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 (e.g., Internet service providers, security as a service providers, cloud service providers, IT/OT service providers)<br>d. Cybersecurity responsibilities are documented (e.g., in position descriptions, in performance criteria) |
| **MIL3** | e. Cybersecurity responsibilities and job requirements are reviewed and updated in accordance with organization-defined triggers (e.g., time elapsed, personnel changes, process changes)<br>f. Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning |

### 2. Develop Cybersecurity Workforce

| | |
|---|---|
| **MIL1** | a. Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner<br>b. Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs |

### 2. Develop Cybersecurity Workforce (cont.)

| | |
|---|---|
| **MIL2** | c. Training, recruiting, and retention efforts are aligned to address identified workforce gaps<br>d. Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training) |
| **MIL3** | e. The effectiveness of training programs is evaluated at an organization-defined frequency, and improvements are made as appropriate<br>f. Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities |

### 3. Implement Workforce Controls

| | |
|---|---|
| **MIL1** | a. Personnel vetting (e.g., background checks, drug tests) is performed, at least in an ad hoc manner, at hire for positions that have access to the assets required for delivery of the function<br>b. Personnel termination procedures address cybersecurity, at least in an ad hoc manner |
| **MIL2** | c. Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function<br>d. Personnel transfer procedures address cybersecurity |
| **MIL3** | e. Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk<br>f. A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures |

### 4. Increase Cybersecurity Awareness

| | |
|---|---|
| **MIL1** | a. Cybersecurity awareness activities occur, at least in an ad hoc manner |
| **MIL2** | b. Objectives for cybersecurity awareness activities are established and maintained (PROGRAM-1b)<br>c. Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-1d) |
| **MIL3** | d. Cybersecurity awareness activities are aligned with the predefined states of operation (SITUATION-3h)<br>e. The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency, and improvements are made as appropriate |

## 5. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the WORKFORCE domain<br>b. Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain<br>c. Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the WORKFORCE domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the WORKFORCE domain<br>f. Performance objectives for activities in the WORKFORCE domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the WORKFORCE domain are standardized and improved across the enterprise |

# 6.9 Cybersecurity Architecture (ARCHITECTURE)

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

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

The Cybersecurity Architecture (ARCHITECTURE) domain comprises five objectives:

1. Establish and Maintain Cybersecurity Architecture Strategy and Program
2. Implement Segmentation as an Element of the Cybersecurity Architecture
3. Implement Application Security as an Element of the Cybersecurity Architecture
4. Implement Data Security as an Element of the Cybersecurity Architecture
5. Management Activities

The cybersecurity architecture provides an overarching plan for how security is to be engineered in a way that transcends point solutions for individual assets such as identity management or access control. It enables reasoning about the security of critical applications and data in terms of known architectural tactics to, for example, detect, resist, react to, and recover from attacks. Such tactics include segmentation, choice of hosting solutions, cryptographic controls, and audit trails, and they can be allied with availability tactics such as monitoring, rollback, and redundancy. Aligned with an organization's enterprise architecture strategy and program,

**Example: Cybersecurity Architecture**

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

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

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

the cybersecurity architecture informs practices such as risk analysis and configuration of assets.

To be effective, the cybersecurity architecture must be sufficiently documented so that it can be communicated to stakeholders. It must also be governed to the extent that it is periodically reviewed and updated as necessary to address security concerns and align with the organization's cybersecurity program.

**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/or managed in an ad hoc manner |
| **MIL2** | b. | A strategy for cybersecurity architecture is established and maintained to support the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture |
| | c. | A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization |
| | d. | Governance for cybersecurity architecture is established and maintained that includes provisions for periodic architectural reviews and an exceptions process (e.g., an architecture review board) |
| | e. | The cybersecurity architecture incorporates confidentiality, integrity, and availability requirements for the function's assets |
| | f. | The cybersecurity architecture incorporates cybersecurity principles (e.g., least functionality, default deny, least privilege) |
| **MIL3** | g. | The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program |
| | h. | Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated according to organization-defined triggers (e.g., time elapsed, changes to systems, networks, or assets) |
| | i. | The cybersecurity architecture is guided by the information from the organization's risk taxonomy (RISK-2e) and threat profile (THREAT-1d) to support the implementation of protections against identified threats |

### 2. Implement Segmentation as an Element of the Cybersecurity Architecture

| | | |
|---|---|---|
| **MIL1** | a. | The organization's IT systems are separated from OT systems through segmentation, either through physical means (e.g., air gaps) or logical means (e.g., network configuration or appliances), at least in an ad hoc manner |
| **MIL2** | b. | Assets that are important to the delivery of the function are segmented into multiple security zones based on criteria defined in the cybersecurity architecture (e.g., risk analysis results, security requirements, remote access, functional requirements) |
| **MIL3** | c. | All assets are segmented into security zones based on criteria defined in the cybersecurity architecture |

### 3. Implement Application Security as an Element of the Cybersecurity Architecture

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Software developed in-house that is to be deployed on assets that are important to the delivery of the function is developed using secure software development practices<br>b. The selection of procured software (e.g., mobile applications, applications to be hosted on premises, software-as-a-service applications) to be deployed on assets that are important to the delivery of the function includes consideration of the vendor's secure software development practices (DEPENDENCIES-2e) |
| **MIL3** | d. The architecture review process evaluates the security of new and revised applications prior to deployment (ARCHITECTURE-1h)<br>c. Security testing (e.g., static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications based on identified risk according to organization-defined triggers (e.g., time elapsed, changes to applications, changes to threat environment) |

### 4. Implement Data Security as an Element of the Cybersecurity Architecture

| | |
|---|---|
| **MIL1** | a. Sensitive data (e.g., PII, PCI, PHI, CEII, IP, operations data) is protected at rest (e.g., encrypted, masked, password-protected, subject to access control lists) at least in an ad hoc manner<br>b. Sensitive data (e.g., PII, PCI, PHI, CEII, IP, operations data) is protected in transit (e.g., encrypted, masked, transmitted using protected mechanisms) at least in an ad hoc manner (ASSET-2c) |
| **MIL2** | c. Key management infrastructure (i.e., key generation, key storage, key destruction, key update, and key revocation) are established and maintained to support the protection of data-at-rest and data-in-transit<br>d. Cryptographic controls are established and maintained to support the protection of data-at-rest and data-in-transit as required in the cybersecurity architecture<br>e. The cybersecurity architecture includes controls (e.g., data loss prevention tools, physical data exfiltration controls) to manage the transmission of data within and between systems based on security requirements (ARCHITECTURE-1e) |
| **MIL3** | f. The cybersecurity architecture includes protections for all data-at-rest (i.e., on-premise and cloud-based file storage and databases) for selected data categories (ASSET-2c)<br>g. The cybersecurity architecture includes protections for all data-in-transit (e.g., within internal networks, across network boundaries, and external traffic, including cloud solutions) for selected data categories (ASSET-2c)<br>h. Data protections are tested (e.g., controls validation) according to organization-defined triggers (e.g., time elapsed, changes to system architecture, changes to threat environment)<br>i. The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and information (due to errors or malicious activity) |

## 5. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the ARCHITECTURE domain<br>b. Adequate resources (people, funding, and tools) are provided to activities in the ARCHITECTURE domain<br>c. Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities<br>d. Responsibility and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel |
| **MIL3** | e. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the ARCHITECTURE domain<br>f. Performance objectives for activities in the ARCHITECTURE domain are established and monitored to track achievement (PROGRAM-1b)<br>g. Documented practices for activities in the ARCHITECTURE domain are standardized and improved across the enterprise |

# 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 the organization's strategic objectives and the risk to critical infrastructure.*

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

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

1. Establish Cybersecurity Program Strategy
2. Sponsor Cybersecurity Program
3. Address Cybersecurity in Continuity of Operations
4. Management Activities

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

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

### Example: Cybersecurity Program Management

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

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

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

The cybersecurity program and continuity of operations planning activities should be aligned with one another. This alignment is important to ensure that continuity plans are suitable to sustain and restore operations following a cyber event. Ensuring that continuity plans address potential cyber incidents requires consideration of known cyber threats and identified categories of cyber risk. Continuity plan testing should include cyber incident scenarios to ensure that the plans will function as intended during such an incident.

**Objectives and Practices**

### 1. Establish Cybersecurity Program Strategy

| | |
|---|---|
| **MIL1** | a. The organization has a cybersecurity program strategy, which may be developed and/or managed in an ad hoc manner |
| **MIL2** | b. The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities<br>c. The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure<br>d. The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities<br>e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program<br>f. The cybersecurity program strategy identifies standards and/or guidelines intended to be followed by the program<br>g. The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program |
| **MIL3** | h. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (THREAT-1d) |

### 2. Sponsor Cybersecurity Program

| | |
|---|---|
| **MIL1** | a. Resources (people, funding, and tools) are provided, at least in an ad hoc manner, to establish the cybersecurity program<br>b. Senior management, with proper authority, provides support for the cybersecurity program, at least in an ad hoc manner |
| **MIL2** | c. The cybersecurity program is established according to the cybersecurity program strategy<br>d. Adequate resources (people, funding, and tools) are provided to operate a cybersecurity program aligned with the program strategy<br>e. Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities are regularly communicated by senior management)<br>f. Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies<br>g. Responsibility for the cybersecurity program is assigned to a role with requisite authority<br>h. Stakeholders for cybersecurity program management activities are identified and involved |

## 2. Sponsor Cybersecurity Program (cont.)

| | |
|---|---|
| **MIL3** | i. The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy<br>j. Cybersecurity activities are independently reviewed (i.e., by reviewers outside the cybersecurity program under direction from the organization's governing body) to ensure conformance with cybersecurity policies and procedures<br>k. The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate<br>l. The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies |

## 3. Address Cybersecurity in Continuity of Operations

| | |
|---|---|
| **MIL1** | a. Continuity plans are developed to sustain and restore operation of the function if a cyber event or incident occurs, at least in an ad hoc manner<br>b. Backups of IT, OT, and information assets are available and tested, at least in an ad hoc manner |
| **MIL 2** | c. An analysis of the impacts from potential cyber events informs the development of continuity plans<br>d. The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans<br>e. Continuity plans address IT, OT, and information assets important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets<br>f. Continuity plans are tested through evaluations and exercises (e.g., walkthroughs, tabletops, dependency testing, testing backups and spares) at an organization-defined frequency<br>g. Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets important to the delivery of the function are incorporated into continuity plans<br>h. Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management functions |
| **MIL 3** | i. Continuity plans are tested through evaluations and exercises at an organization-defined frequency and include current cyber threat scenarios<br>j. Continuity plans are aligned with the function's risk taxonomy (RISK-2e) and threat profile (THREAT-1d) to ensure coverage of identified risk categories and threats<br>k. The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly<br>l. Cybersecurity incident content within continuity plans is periodically reviewed and updated<br>m. Continuity plans are periodically reviewed and updated |

## 4. Management Activities

| | |
|---|---|
| **MIL1** | No practice at MIL1 |
| **MIL2** | a. Documented practices are established, followed, and maintained for activities in the PROGRAM domain<br>b. Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities<br>c. Responsibility and authority for the performance of activities in the PROGRAM domain are assigned to personnel |
| **MIL3** | d. Policies or other organizational directives are established and maintained that enact specific organizational requirements for the implementation of activities in the PROGRAM domain<br>e. Performance objectives for activities in the PROGRAM domain are established and monitored to track achievement<br>f. Documented practices for activities in the PROGRAM domain are standardized and improved across the enterprise |

# APPENDIX A: PRACTICE GUIDANCE

To be developed

# APPENDIX B: V1.1 TO V2.0 MAPPING

| V1.1 | V2.0 |
| --- | --- |

# APPENDIX C: REFERENCES

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

[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. 2011. *CERT resilience management model: A maturity model for managing operational resilience* (CERT-RMM Version 1.1). Boston, MA: Addison-Wesley.

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

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

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

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

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

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

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

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

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

[DHS Procurement]
U.S. Department of Homeland Security, Control Systems Security Program, National Cyber Security Division. 2009. *U.S. Department of Homeland Security: Cyber security procurement language for control systems.*

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

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

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

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

[HSPD-7]
U.S. Department of Homeland Security. n.d. *Homeland Security Presidential Directive – 7*. Retrieved May 30, 2019, from http://www.dhs.gov/homeland-security-presidential-directive-7#1

[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. [Home page]. Retrieved May 30, 2019, from https://www.nationalisacs.org/

[ISO/IEC 2:2004]
International Organization for Standardization. 2004. *Standardization and related activities -- General vocabulary* (ISO/IEC 2:2004).

[ISO 27005:2011]
International Organization for Standardization. 2011. *Information security risk management* (ISO 27005:2011)

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

[ISO/IEC 27001:2005]
International Organization for Standardization. 2008. *Information security management systems* (ISO/IEC CD 27001:2005).

[ISO/IEC 27002:2005]
International Organization for Standardization. 2008. *Code of practice for information security management* (ISO/IEC27002:2005).

[ISO 28001:2007]
International Organization for Standardization. n.d. *Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance* (ISO/ IEC20001:2007).

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

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

[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]
Radack, S. 2008. S*ecurity considerations in the information system development life cycle.* National Institute of Standards and Technology. Retrieved from http://www.itl.nist.gov/lab/bulletns/bltndec03.htm

[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 May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/draft

[NIST SP800-37]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2010. *Guide for applying the risk management framework to federal information systems* (NIST Special Publication 800-37). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

[NIST SP800-40]
Mell, P., Bergeron, T., & Henning, D. 2005. *Creating a patch management and vulnerability management program* (NIST Special Publication 800-40, version 2.0). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-40/version-20/archive/2005-11-16

[NIST SP800-50]
Wilson, M., & Hash, J. 2003. *Building an information technology security awareness and training program* (NIST Special Publication 800-50 ). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-50/final

[NIST SP800-53]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2009. *Recommended security controls for federal information systems and organizations* (NIST Special Publication 800-53, revision 3). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-3/archive/2010-05-01

[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]
Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, Jessica. 2008. *Security considerations in the system development life cycle* (NIST Special Publication 800-64, revision 2). National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

[NIST SP800-82]
Stouffer, K., Falco, J., & Scarfone, K. 2011. *Guide to industrial control systems (ICS) security* (NIST Special Publication 800-82). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final

[NIST SP800-83]
Mell, P., Kent, K., & Nusbaum, J. 2005. *Guide to malware incident prevention and handling* (NIST Special Publication 800-83). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-83/archive/2005-11-23

[NIST SP800-128]
National Institute of Standards and Technology. 2011. *Guide for security-focused configuration management of information systems* (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* (Special Publication 800-150). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-150/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 Vols. 1]
The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for smart grid cyber security: Vol. 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 cyber security: Vol. 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

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

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

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

[Situation Awareness in Dynamic Systems]
Endsley, M. 1995. "Toward a theory of situation awareness in dynamic systems." *Human Factors,* pp. 32-64.

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

[WH Trusted Identities in Cyberspace]
The White House. *National strategy for trusted identities in cyberspace.* 2011. Retrieved May 30, 2019, from https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf

# APPENDIX D: 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 (e.g., 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 this model, *ad hoc* (i.e., an ad hoc practice) 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 in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad hoc. However, because lessons learned are typically not captured at the organizational level, approaches and outcomes are difficult to repeat or improve across the organization. | C2M2 |
| advanced metering infrastructure (AMI) | Advanced Metering Infrastructure (AMI) refers to systems that measure, collect, and analyze energy usage, from advanced devices such as "smart" electricity meters, gas meters, and/or water meters, through various communication media on request or on a predefined schedule. | Adapted from SGMM v1.1 Glossary |
| anomalous/anomaly | 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 controls, processes, and other elements, commensurate with the risk to critical infrastructure and organizational objectives. | C2M2 |
| architecture | See *cybersecurity architecture.* | |
| assessment | See *risk assessment.* | |
| asset | Something of value to the organization. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function. | |

| Term | Definition | Source |
|---|---|---|
| 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, 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 |
| authentication | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT or ICS. | DOE Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline |
| authenticator | The means used to confirm the identity of a user, processor, or device (e.g., user password or token). | NIST 800-53 |
| 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 |
| business impact analysis | A mission impact analysis that prioritizes the impact associated with the compromise of an organization's information assets, based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. | Adapted from NIST SP800-30 |
| change control (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 |
| common operating picture | Activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains. | C2M2 |
| computer security incident | A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet. Also, see *incident.* | NIST 800-61 (computer security incident) |
| 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 |

| Term | Definition | Source |
|---|---|---|
| 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/or 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 |
| contingency plan | Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The contingency plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the continuity of operations plan or disaster recovery plan for major disruptions. | CNSSI 4009 |
| continuous monitoring | Maintaining ongoing awareness of the current cybersecurity state of the function throughout the operational environment by collecting, analyzing, alarming, presenting, and using OT system and cybersecurity information to identify anomalous activities, vulnerabilities, and threats to the function in order to support incident response and organizational risk management decisions. | Adapted from NIST 800-137 |
| controls | The management, operational, and technical methods, policies, and procedures—manual or automated—(i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information. | DOE RMP |
| critical infrastructure | Assets that provide the essential services that underpin American society. The Nation possesses numerous 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 (e.g., 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 | The ability to protect or defend the use of cyberspace from cyber attacks. Measures taken to protect a computer or computerized system (IT and OT) against unauthorized access or attack. | DOE RMP and Merriam-Webster.com |

| 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 *enterprise architecture* and *network architecture*. | C2M2 |
| cybersecurity event | Any observable occurrence in a system or network that is related to a cybersecurity requirement (confidentiality, integrity, or availability). See also *event*. | C2M2 |
| cybersecurity impact | The effect on the measures that are in place to protect from and defend against cyber attack. | C2M2 |
| cybersecurity incident | See *incident.* | |
| cybersecurity incident lifecycle | See *incident lifecycle.* | |
| cybersecurity plan | Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements. | DOE RMP |
| cybersecurity policy | A set of criteria for the provision of security services. | DOE RMP |
| cybersecurity program | A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or the function. A cybersecurity program may be implemented at either the organization or the function level, but a higher-level implementation and enterprise viewpoint may benefit the organization by integrating activities and leveraging resource investments across the entire enterprise. | 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 an IT and OT that are derived from organizational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, 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 |
| cybersecurity risk | The risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS. See *risk*. | DOE RMP |

| Term | Definition | Source |
|---|---|---|
| cybersecurity workforce management objectives | Performance targets for personnel with cybersecurity responsibilities that the organization sets to meet cybersecurity requirements. | Adapted from CERT RMM |
| defined practice | A practice that is planned (i.e., described, explained, made definite and clear, and standardized) and is executed in accordance with the plan. | Adapted from CERT RMM |
| dependency risk | Dependency risk is measured by the likelihood and severity of damage if an IT or OT system is compromised due to a supplier or other external 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 *upstream dependencies* and *supply chain risk.* | Adapted from NIST 7622, pg. 10 |
| deprovisioning | The process of revoking or removing an identity's access to organizational assets. See also *provisioning.* | CERT RMM |
| distribution | The delivery of energy to retail customers (e.g., homes, businesses, industry, government facilities). | Adapted from EIA Glossary |
| 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 |
| downstream activities | Business process most commonly used in the petroleum industry to describe postproduction processes (e.g., refining, transportation, and marketing of petroleum products). | API STD 689, Collection and Exchange of Reliability and Maintenance Data for Equipment, First Edition, July 2007 |
| downstream dependencies | External parties dependent on the delivery of the function, such as customers and some operating partners. | C2M2 |
| electricity sector information sharing and analysis center (E-ISAC) | The Electricity Sector Information Sharing and Analysis Center (E-ISAC) shares critical information with industry participants about infrastructure protection. The ES-ISAC serves the electricity sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, vulnerabilities, analyses, and warnings, together with interpretations, to help electricity sector participants take protective actions. See Information Sharing and Analysis Center (ISAC). | Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page |

| Term | Definition | Source |
|---|---|---|
| electricity subsector | A portion of the energy sector that includes the generation, transmission, and distribution of electricity. | ES-SPP |
| enterprise | The largest (i.e., highest-level) organizational entity to which the organization participating in the C2M2 survey belongs. For some participants, the organization taking the survey is the enterprise itself. See *organization.* | Adapted from SGMM v1.1 Glossary |
| enterprise architecture | The design and description of an enterprise's entire set of IT and OT: 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 *cybersecurity architecture* and *network architecture*. | DOE RMP (but changed ICS to OT) |
| entity | Something having separate or distinct existence. | Merriam-Webster.com |
| establish and maintain | The development and maintenance of the object of the practice (such as a program). For example, "Establish and maintain identities" means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements. | CERT RMM |
| event | Any observable occurrence in a system or network. Depending on their potential impact, some events need to be escalated for response. To ensure consistency, criteria for response should align with the organization's risk criteria. | NIST 800-61 |
| Event and Incident Response (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 | A subset of the operations of the organization that are being evaluated based on the C2M2 model. | C2M2 |
| generation | The process of producing electric energy by transforming other forms of energy; also, the amount of electric energy produced, expressed in kilowatt-hours. | EIA Glossary |
| 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 internally by an organization. See *standard*. | C2M2 |

| Term | Definition | Source |
|---|---|---|
| identity | The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. | 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 consequence to subsector functions. | C2M2 |
| incident | An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure and/or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts. See also *computer security incident* and *event.* | Adapted from CERT RMM |
| incident lifecycle | The stages of an incident from detection to closure. Collectively, the incident lifecycle includes the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents. Escalated events also follow the incident lifecycle, even if they are never formally declared to be incidents. | Adapted from CERT RMM |
| information assets | Information or data that is of value to the organization, including diverse information such as operational data, intellectual property, customer information, and contracts. | Adapted from CERT RMM |
| information sharing and analysis center (ISAC) | An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants on infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning. | Adapted from Electricity Sector Information Sharing and Analysis Center website home page |
| information technology (IT) | A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate. | DOE RMP |
| institutionalization | The extent to which a practice or activity is ingrained into the way an organization operates. 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. ("Incorporated into the ingrained way of doing business that an organization follows routinely as part of its corporate culture." – CERT RMM). See also *maturity indicator level.* | C2M2 |

| Term | Definition | Source |
|---|---|---|
| integrity | Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner. | DOE RMP & CERT RMM |
| 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/or functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary to achieving least privilege. Organizations also apply least privilege concepts to the design, development, implementation, and operations of IT and OT systems. | Adapted from NIST 800-53 |
| logging | Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace. Regular review and audit of logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness (e.g., through the detection of cybersecurity events or weaknesses). | C2M2 |
| logical control | A software, firmware, or hardware feature (i.e., 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" |
| Markets | Venues where participants buy and sell products and services. In the context of this model, markets refers to trading involving wholesale electricity. | FERC |
| maturity | The extent to which an organization has implemented and institutionalized the cybersecurity practices of the model. | C2M2 |

| Term | Definition | Source |
|---|---|---|
| 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) and holds a fifth level in reserve for use in future versions of the model. 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 core activities in the domain. | C2M2 |
| midstream activities | Business category involving the processing, storage, and transportation sectors of the petroleum industry. | API STD 689, Collection and Exchange of Reliability and Maintenance Data for Equipment, First Edition, July 2007 |
| 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 | Authentication using two or more factors to achieve authentication. Factors include (i) something you know (e.g., password/PIN), (ii) something you have (e.g., cryptographic identification device, token), (iii) something you are (e.g., biometric), or (iv) you are where you say you are (e.g., GPS token). See *authentication*. | Adapted from NIST 800-53 |
| network architecture | A framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection. See *enterprise architecture* and *cybersecurity architecture*. | Adapted from CNSSI 4009 (IA architecture) |
| objective(s) | *See domain objectives* and *organizational objectives*. | |

| Term | Definition | Source |
|---|---|---|
| operating picture | Real-time (or near-real-time) awareness of the operating state of a system or function. An operating picture is formed from data collected from various trusted information sources that may be internal or external to the system or function (e.g. temperature, weather events and warnings, cybersecurity alerts). The operating picture may or may not be presented graphically. It involves the collection, analysis (including fusion), and distribution of what is important to know to make decisions about the operation of the system.<br>A common operating picture (COP) is a single operating picture that is available to the stakeholders of the system or function so that all stakeholders can make decisions based on the same reported operating state. See common operating picture. | C2M2 |
| 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 *pre-defined states of operation*. | C2M2 |
| operational risk | The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. In the context of this model, our focus is on operational risk from cybersecurity threats. | Adapted from CERT RMM |
| operations technology (OT) | Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. | C2M2 |
| organization | An organization of any size, complexity, or positioning within an organizational structure that is charged with carrying out assigned mission and business processes and that uses IT and OT in support of those processes. In the context of the model, the organization is the entity using the model or that is under examination. | Adapted from DOE RMP |
| organizational objectives | Performance targets set by an organization. See *strategic objectives*. | Adapted from CERT RMM |
| periodic review/activity | A review or activity that occurs at specified, regular time intervals, where the organization-defined frequency is commensurate with risks to organizational objectives and critical infrastructure. | Adapted from SEI CMM Glossary |

| Term | Definition | Source |
|---|---|---|
| personal information | Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual. | NISTIR 7628 Vol. 3, 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 high-level overall plan embracing the general goals and acceptable procedures of an organization. | Merriam-Webster.com |
| position description | A set of responsibilities that describe a role or roles filled by an employee. Also known as a job description. | C2M2 |
| practice | An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organizational objectives. | C2M2 |
| predefined states of operation | Distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resiliency, reliability, and/or cybersecurity. For example, a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity. The high-security operating state may trade off efficiency and ease of use in favor of increased security by blocking remote access and requiring a higher level of authentication and authorization for certain commands until a return to the normal state of operation is deemed safe. | C2M2 |
| procedure | In this 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) |
| provisioning | The process of assigning or activating 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 |

| Term | Definition | Source |
|---|---|---|
| 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 |
| refining | The control or management of any operation by which the physical or chemical characteristics of oil or products are changed, but exclusive of the operations of passing oil through separators to remove gas, placing oil in settling tanks to remove basic sediment and water, dehydrating oil, and generally cleaning and purifying oil. | Natural Resources, Office of Conservation – General Operations, Louisiana Administrative Code, Title 43, Part XIX, March 2013 |
| 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. | DOE RMP |
| risk analysis | A risk management activity focused on understanding the condition and potential consequences of risk, prioritizing risks, and determining a path for addressing risks. 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, reputation), resources, other organizations, and the Nation, resulting from the operation of an IT and ICS. | 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. | ES-C2M2 |
| risk designation, as in "position risk designation" | An indication, such as high, medium, or low, of the position's potential for adverse impact to the efficiency, integrity, or availability of the organization's services. | Adapted from OPM |
| risk disposition | A statement of the organization's intention for addressing an operational risk. Typically limited to "accept," "transfer," "research," or "mitigate." | CERT RMM |
| risk management program | The program and supporting processes to manage cybersecurity 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 cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders. | C2M2 |

| Term | Definition | Source |
|---|---|---|
| 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 mitigation plan | A strategy for mitigating risk that seeks to minimize the risk to an acceptable level. | CERT RMM |
| risk parameter/risk parameter factors | Organization-specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk measurement criteria. | CERT RMM |
| risk register | A structured repository where identified risks are recorded to support risk management. | C2M2 |
| risk response | Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations. | DOE RMP |
| risk taxonomy | The collection and cataloging of common risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line-of-business if operational assets and services are affected by them. | Adapted from CERT RMM |
| role | A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. | CNSSI 4009 |
| 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 | 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 and/or roles; (ii) conducting information system support functions with different individuals (e.g., 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 |
|---|---|---|
| service level agreement (SLA) | Defines the specific responsibilities of the service provider, including the satisfaction of any relevant cybersecurity requirements, and sets the customer's expectations regarding the quality of service to be provided. | Adapted from CNSSI 4009 |
| situational awareness | A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modeling and simulation) to support automated and/or human decision making (for example, concerning OT system functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualization techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision making. | Adapted from SGMM Glossary |
| Situational Awareness (SITUATION) | The C2M2 domain with the purpose to establish and maintain activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP), commensurate with the risk to critical infrastructure and organizational objectives. | C2M2 |
| sponsorship | Enterprise-wide support of cybersecurity objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the cybersecurity program along with provision of resources. Senior management monitors the performance and execution of the cybersecurity program and is actively involved in the ongoing improvement of all aspects of the cybersecurity program. | C2M2 |
| stakeholder | An external organization or an internal or external person or group that has a vested interest in the organization or function (that is being evaluated using this model) and its practices. Stakeholders involved in performing a given practice (or who oversee, benefit from, or are dependent upon the quality with which the practice is performed) could include those from within the function, from across the organization, or from outside the organization. | 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 *guidelines*. | Adapted from ISO/IEC Guide 2:2004 |
| states of operation | See *pre-defined 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 | The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers.<br>The supply chain encompasses the full product lifecycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain. | NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA] |
| supply chain risk | *Supply chain risk* is measured by the likelihood and severity of damage if an IT or OT system is compromised by a supply chain attack, and takes into account the importance of the system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation.<br>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/ infrastructure, and/or disabling of mission-critical operations. See risks and supply chain. | Adapted from NIST 7622, pg. 7 & pg. 10 |
| Supply Chain and External Dependencies Management (DEPENDENCIES) | The C2M2 domain with the purpose to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives. | C2M2 |
| threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. | 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 (e.g., critical, IT, operational) and organizational objectives. | C2M2 |
| threat assessment | The process of evaluating the severity of threat to an IT and ICS or organization and describing the nature of the threat. | DOE RMP |
| 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 and OT of an organization and to the organization itself, delineating the feasible threats, describing the nature of the threats, and evaluating their severity. | C2M2 |
| threat source | An intent and method targeted at the intentional exploitation of a vulnerability or a situation, or a method that may accidentally exploit a vulnerability. | DOE RMP |

| Term | Definition | Source |
|---|---|---|
| traceability | The ability to determine whether or not a given attribute of the current state is valid (e.g., the current configuration of a system or the purported identity of a user) based on the evidence maintained in a historical record showing how the attribute was originally established and how it has changed over time. | C2M2 |
| transmission | The movement or transfer of electric energy over an interconnected group of lines and associated equipment between points of supply and points at which it is transformed for delivery to consumers or is delivered to other electric systems. Transmission is considered to end when the energy is transformed for distribution to the consumer. | EIA Glossary |
| upstream activities | Business category of the petroleum industry involving exploration and production (e.g., offshore oil/gas production facility, drilling rig, intervention vessel). | API STD 689, Collection and Exchange of Reliability and Maintenance Data for Equipment, First Edition, July 2007 |
| upstream dependencies | External parties on which the delivery of the function depends, including suppliers and some operating partners. | C2M2 |
| validate | Collect and evaluate evidence to confirm or establish the quality of something (e.g., information, a model, a product, a system, or component) with respect to its fitness for a particular purpose. | C2M2 |
| vulnerability | A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source. A *vulnerability* class is a grouping of common vulnerabilities. | Adapted from NISTIR 7628 Vol. 1, pp. 8 |
| vulnerability assessment | Systematic examination of an IT or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation. | DOE RMP |
| workforce lifecycle | For the purpose of this model, the *workforce lifecycle* comprises the distinct phases of workforce management that apply to personnel both internal and external to the organization. Specific cybersecurity implications and requirements are associated with each lifecycle phase. The workforce lifecycle includes recruiting, hiring, onboarding, skill assessments, training and certification, assignment to roles (deployment), professional growth and development, re-assignment and transfers, promotions and demotions, succession planning, and termination or retirement. The phases may not be in strict sequences, and some phases (like training, re-assignment, and promotions) may recur. | C2M2 |

| Term | Definition | Source |
|---|---|---|
| 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 |
| workforce management objectives | See *cybersecurity workforce management objectives.* | |

# APPENDIX E: ACRONYMS

| Acronym | Definition |
|---|---|
| C2M2 | Cybersecurity Capability Maturity Model |
| CERT®-RMM | CERT® Resilience Management Model |
| COP | common operating picture |
| COTS | commercial off-the-shelf |
| CVSS | Common Vulnerability Scoring System |
| DHS | Department of Homeland Security |
| DOE | Department of Energy |
| ES-C2M2 | Electricity Subsector Cybersecurity Capability Maturity Model |
| E-ISAC | Electricity Sector Information Sharing and Analysis Center |
| FIRST | Forum of Incident Response and Security Teams |
| FERC | Federal Energy Regulatory Commission |
| GWAC | GridWise Architecture Council |
| HR | human resources |
| IAM | identity and access management |
| ICS | industrial control system |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| ICSJWG | Industrial Control Systems Joint Working Group |
| IEC | International Electrotechnical Commission |
| ISAC | Information Sharing and Analysis Center |
| IT | information technology |
| MIL | maturity indicator level |
| NERC | North American Electric Reliability Corporation |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NIST | National Institute of Standards and Technology |
| OT | operations technology |
| RAWG | [European Union M/490] Reference Architecture Working Group |
| RPO | recovery point objective |
| RTO | recovery time objective |
| RMP | Electricity Subsector Cybersecurity Risk Management Process Guideline |

| | |
|---|---|
| SCADA | supervisory control and data acquisition |
| SEI | Software Engineering Institute |
| SGIP | Smart Grid Interoperability Panel |
| SLA | service level agreement |
| US-CERT | United States Computer Emergency Readiness Team |
| VoIP | Voice over Internet Protocol |

# NOTICES

This material is based on the Technical Report, "Electricity Subsector Cybersecurity Capability Maturity Model Version 1.0 (ES-C2M2)" © 2012 Carnegie Mellon University. This version of C2M2 is being released and maintained by the U.S. Department of Energy (DOE). The U.S. Government has, at minimum, unlimited rights to use, modify, reproduce, release, perform, display, or disclose this version the C2M2 or corresponding toolkits provided by DOE, as well as the right to authorize others, and hereby authorizes others, to do the same.

C2M2 was created with the funding and support of DOE under the Federal Government Contract Number FA8721-05-C-0003 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.

Capability Maturity Model® is a registered trademark of Carnegie Mellon University.